Digital Media and Society

Convenient Regulators of Society, Politics and Economics

DIMITRIOS VAGIANOS

KALLIPOS open academic editions

National Development Programme 2021-2025

DIMITRIOS VAGIANOS

Digital Media and Society

Convenient Regulators of Society, Politics and Economics

KALLIPOS
open academic editions

Digital Media and Society

Author

Dimitrios Vagianos

Contributors/Editors

Language editor: Anastasia Lampropoulou

Graphics editor: Faidra Stragali

Central Support Group

Language Check: Eleftheria Kanari

Graphics Check: Alexandra Theodoraki

Library Processing: Maria Kapnizou

KALLIPOS

National Technical University of Athens

Iroon Polytechneiou 9, 15780 Zografou

www.kallipos.gr

ISBN: 978-618-5726-25-6

Citation: Vagianos, D. (2024). *Digital Media and Society* [Undergraduate textbook]. Kallipos, Open Academic Editions. http://dx.doi.org/10.57713/kallipos-221

To my special wife and children for their eternal support
and
to my students for "being there".
Their contribution has been priceless…

Table of Contents

Table of Abbreviations

2FA	Two factor authentication
3D	Three Dimensions
A2C	Administration to Citizens
AAFPRS	American Academy of Facial Plastic and Reconstructive Surgery
AAP	American Academy of Pediatrics
ACLU	American Civil Liberties Union
AI	Artificial Intelligence
AKP	Justice and Development Party (Turkey)
ALS	Amyotrophic Lateral Sclerosis
AMA	Ask Me Anything (Reddit terminology)
API	Application Program Interfaces
AR	Augmented Reality
B2B	Business-to-Business
B2C	Business-to Consumer
BBC	British Broadcasting Corporation
BJP	Bharatiya Janata Party (India)
BLM	BlackLivesMatter
BRICS	Brazil, Russia, India, China, and South Africa
BYOD	Bring Your Own Device
C2B	Consumer-to-Business
C2C	Citizen to Citizen
C2C	Consumer-to-Consumer
CCA	Cyber Caliphate Army
CCP	Chinese Communist Party
CCPA	California Consumer Privacy Act
CCTA	Central Computer Telecommunications Agency

CDA	Communications Decency Act
CDC	Cult of the Dead Cow
CERT	Computer Emergency Response Team
CFO	Chief Financial Officer
CIA	Central Intelligence Agency
CMC	CMC Computer mediated Communication
CNN	Cable News Network
COMPROP	Computational Propaganda Research Project
COPA	Child Online Protection Act
COPPA	Children's Online Privacy Protection Act
CPA	Cost per Acquisition
CPC	Communist Party of China
CPC	Cost per Click
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Teams
CSO	Civil Society Organizations
CSS	Cascading Style Sheets
CTR	Cyber Team Rox
CX	customer experience
DCCC	Democratic Congressional Campaign Committee
DDoS	Distributed Denial of Service
DDoSA	Distributed Denial of Service Attacks
DEMOS project	Democratic Efficacy and the Varieties of Populism in Europe Project
DM	Digital Media
DMCA	Digital Millennium Copyright Act
DNC	Democratic National Committee
DNS	Domain Name System
DPI	Deep Packet Inspection
DWSN	Dark Web Social Network

ECB	European Central Bank
ECJ	European Court of Justice
EDI	Electronic Data Interchange
EDT	Electronic Disturbance Theater
EEAS	European External Action Service
ELAB	Anti-Extradition Law Amendment Bill
EMB	Electoral Management Bodies
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Network and Information Security Agency
EU	European Union
eVA Project	electronic Friendly Administration Project
EZLN	Zapatista Army of National Liberation (Ejército Zapatista de Liberación Nacional)
FBI	Federal Bureau of Investigation
FRA	Försvarets radioanstalt, National Defence Radio Establishment (Sweden)
FTC	Federal Trade Commission
G2B	Government to Business
G2C	Government to Citizens
G2G	Government to Government
GAFA	Google, Amazon, Facebook, Apple (four Big Tech companies)
GAP	Google Advertising Professional program
GCHQ	Government Communications Head Quarters
GDPR	General Data Protection Regulation
GDQ	GamesDoneQuick
GOP	Guardians of Peace
GPA	Grade Point Average
GPL	General Public License
GPRS	General Packet Radio Service
GPS	GPS Global Positioning system
GRU	Russian Military Intelligence Service

GSR	Global Science Research
HBCU	Historically Black Colleges and Universities
HCI	Human Computer Interaction
HDI	Human Development Index
HDTV	High-Definition TV
HTML	Hypertext Markup Language
IAB	Interactive Advertising Bureau
IAD	Internet Addiction Disorder
IAM	Identity and Access Management
IC	Invisible Children
ICA	Islamic Cyber Army
ICOESS	International Congress of Eurasian Social Sciences
ICT	Information and Communication Technologies
IGO	Intergovernmental Organizations
IMF	International Monetary Fund
IMSC	IMSC Integrated Media Systems Center
INVS	National Institute of Sleep and Vigilance
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IPM	Interactive Policy Making
IRBMS	Regional Institute for the Well-being of Medicine & Health Sport in Nord Pas de Calais
IRC	Internet Relay Chat
IS	Information Systems
IS	Islamic State
ISHD	Islamic State Hacking Division
ISIS	Islamic State o Iraq and Syria
ISP	Internet Service Provider
IT	Information Technology

iTEC	Innovative Technologies for an Engaging Classroom
ITIF	Information Technologies and Innovation Foundation
ITU	International Telecommunication Union
K-12 education	Primary and secondary levels of education
LAN	Local Area Network
LCD	Liquid Crystal Display
LGBTQ	Lesbian, Gay, Bisexual and Transgender and Queer
LRA	Lord's Resistance Army
LSE	London School of Economics
MENA	Middle East and North Africa
MEP	Member of European Parliament
MIPS	Millions Instructions per second
MIT	Massachusetts institute of Technology
MMORPGs	Massively Multiplayer Online Role-Playing Games
MN	Minessota
MOOC	Massive Open Online Courses
MP	Member of Parliament
MS	Member States
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NEGIS	Northeast Gang Information System
NGO	Non-Governmental Organizations
NHS	National Health System
NIST	National Institute of Standards and Technology
NRI	Networked Readiness Index
NSA	National Security Agency
NSPCC	National Society for the Prevention of Cruelty
NTIA	National Telecommunications & Information Administration
NYPD	New York Police Department

OECD	Organisation for Economic Co-operation and Development
OFDT	French Organization About Drugs and Addictions
OPM	Office of Personnel Management
OSINT	Open Source Intelligence
OTAN	Organisation du Traité de l'Atlantique Nord (NATO in French)
OVG	Online Video Games
OWS	Occupy Wall Street
P2P	Peer-to-peer
PDP	Personal Data Protection
PDSS	Personal Data Security System
PGA	Peoples Global Action
PGP	Pretty Good Privacy
PII	Personal identifiable information
POST	Parliamentary Office of Science and Technology
REST	Representational state transfer
RFID	Radio Frequency Identification
RIA	Rich Internet Applications
RMF	Rhodes Must Fall (campaign)
ROI	Return of Investment
RSS	Really Simple Syndication
RTVE	Radiotelevisión Española
SaaS	Software as a Service
SCA	Sons Caliphate Army
SCL	Strategic Communication Laboratories
SEA	Search Engine
SEM	Search Engine Marketing
SEO	Search Engine Optimization
SERP	Search Engine Results Page
SFA	Sales Force Automation

SM	Social Networking
SME	Small and Medium-sized Enterprises
SMS	Short Message Service
SMT	Social media technology
SNA	Social Network Analysis
SNS	Social Networking Sites
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SPE	Sony Pictures Entertainment
TIB	Presidency of Telecommunications and Communication (Turkey)
TOR	The Onion Router
TWEA	Trading with the Enemy Act
UC	University of California
UCC	United Cyber Caliphate
UK	United Kingdom
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
URL	Uniform Resource Locator
US	United states
USA	United States of America
VAP	Village Access Project
VPN	Virtual Private Network
WANK	Worms against Nuclear Killers
WAP	Wireless Access Protocol
WEF	World Economic Forum
WHO	According to the World Health Organization
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
WWF	World Wildlife Fund

www	World Wide Web
ZB	zettabyte

Prologue

The rapid development of digital communications, including radio, television, video services, mobile technology, and the Internet with social media, has caused multifaceted societal implications, including the News industry, local and international politics and Economics. These implications provided fertile ground for research in diverse scientific fields. Social Sciences may be the core of any scientific approach. However, due to the broad nature of the issue, the use of various scientific tools, requiring qualitative and quantitative specialization and expertise, is in many cases mandatory for integrated results.

Since scientists in many areas are potential researchers in this broad field, a general introduction to the topic has been found crucial by academics and institutions globally that can inspire further engagement in undergraduate or postgraduate students. This is why several universities across the globe have recently incorporated in their study programs courses that serve this exact purpose: to provide a platform for students to engage and critically analyze, from diverse perspectives, including technical ones, the issues surrounding the multifaceted relationships between digital media and society. Such academic efforts often require diverse sources to quickly and effectively provide the necessary background, especially when this must be accomplished within tight semestrial limits. Academics often engage students in assignment writing to stimulate personal research, leading to knowledge acquisition through navigation around the vast online sources that are dynamically updated.

However, in many cases, an integrated book that can provide initial awareness and operate as an educational basis for future involvement in the topic remains essential. Several books cover the topic from a specific, often narrow perspective that, omits some fruitful aspects.

This textbook attempts to cover, to a reasonable depth, the most important issues of the relations between digital media and Society. Teaching this broad topic for almost a decade to an international audience with diverse scientific backgrounds outlined its need and posed its prerequisites and specifications. At the same time, the individual supervision of hundreds of students' assignments with relevant and multivariate topics accumulated a broad knowledge of particular issues and incidents in the field that emerged during this time. This information repository has proven to be a valuable resource that needs to be made available to the academic community. Writing this book fulfilled this need.

The 15 chapters of this book aspire to offer a complete and organized collection of material that covers all prerequisite knowledge in the field, without going deeper than required at this level, but at the same time without omitting critical information and knowledge of the field through the lens of Social Sciences: Society, Politics and Economics. The introductory terms and notions are presented in the first two chapters, including the Information Society and the transition to the Networked Society. Subsequently, the transition from Web 1.0 to Web 2.0 is described, and social media, social networking sites and network media are introduced. Two chapters are dedicated to the Implications of social media in Politics, Education and the New Generation. In five chapters of the book, the Habermasian Public Sphere issues are investigated through the lens of digital media: the Digital Divide is initially defined, followed by an analysis of many critical areas, including Democracy in the Digital Age, e-Government, e-Business and e-Commerce. Subsequently, Social Movements and Activism in the Digital Age are outlined. The grey and dark zones of the Deep Web are also presented with extensive references to cybercrimes, cyber warfare and cyberterrorism. The essential issues of Privacy, Cybersecurity and surveillance in the Digital Age are also highlighted. Eventually, the implications of digital media in marketing are also highlighted.

The textbook "Digital media and Society: Convenient Regulators of Society, Politics and Economics aims to become an essential reading for undergraduate and postgraduate students of Social Sciences who generally

aim to explore and potentially seek motivation for more in-depth investigation of one (or more) of the following dynamically evolving areas: the realm of digital media, the Internet, social media, the Public Sphere, Mobile and Participatory culture, Internet Politics and Digital Marketing.

Dimitrios M. Vagianos

Electrical and Computer Engineer, PhD

Special Teaching Personnel

Department of International and European Studies

University of Macedonia

Chapter 1 An Introduction to Digital Media

Abstract

Chapter 1 introduces the reader to the transition from the traditional Media of the 20th century to the Digital Media (DM) of the present. Historical breakthroughs in Technology and social changes are indicated, which allowed for the transformation of the Media key elements and the surrounding "cybercultures" and led to digital media as they are today. These key elements include the medium of Digital Delivery, the devices for accessing DM Content, the audiences of DM, the producers with the distributors and the financiers of DM, the DM content itself, the owners and business of DM, the regulators and prevailing laws of Media, the relevant technologies, the inventors and innovators of the next generation of Media, the ethical framework and the new generation of consumers of DM content. The cybercultures include all the Networked, Electronic and Wired cultures of the last three decades. The vital social issues that are related to them are also presented: Globalization and Technocapitalism, the Digital Divide, E-Governance, Civil Society, the Governance of Cyberspace, the digital identities, Race/Class/Gender issues, the new dimensions of Space and Geography of the Internet, the risks and the Aesthetics of the New Media. At the end of the chapter, the topics of the following chapters are briefly described.

1.1 Introduction

Digital Media (DM) refers to the various systems of public communication, content creation and dissemination, as well as the computer-based technologies that facilitate and influence these processes. The term “public” includes all media producing, delivering, and packaging content and communications for public rather than private discourse or consumption. As such, it includes all the traditional mass communication media, including newspapers, magazines, books, radio, and television, that have undergone a digital change.

Digital media means any communication medium that operates using various encoded machine-readable data formats. Digital media can be created, viewed, distributed, modified, listened to, and preserved on a digital electronic device. Digital can be defined as any data represented by a series of digits, while media refers to methods of broadcasting or communicating this information. Together, digital media refers to mediums of digitized information broadcast to us through a screen and/or a speaker (wikipedia.com).

A term close to the notion of digital media is digital convergence, which refers to the convergence of all media types in a computer-based form, typically including wired or wireless connectivity to the internet or a local area network (LAN).

Although convergence is apparent, some diverse types of digital media devices exist. Digital convergence should not be confused with the Internet or the World Wide Web (www) itself. The truth is that a wide range of technologies compose the full spectrum of Media in the Digital Age that were initially launched as standalone technologies, such as wireless and mobile media, digital television, satellite radio, digital cameras, music players, etc. However, Internet technology gradually absorbed them under an umbrella of protocols, becoming the standard platform able to deliver most types of digital content.

It must be apparent to new generations that the digital media story did not start as the internet is taken for granted today. It took quite a while for the several types of media to go through the digitalization process and time-consuming standardization procedures to reach today’s state.

1.2 Information and Communication Technology (ICT)

Information and Communication Technology (ICT) is the aggregation of all professional fields linked to the research, design, development and control of telecommunications, computers and software. Information technology is used to store, manipulate, distribute or create information. The type of information or data is not crucial to this definition. Technology is any mechanism capable of processing this data.

Kathleen Guinee argued that “by information technology, we mean the tools we use to perform calculations, to store and manipulate text, and to communicate. Some of these twentieth-century tools include: the adding machine, slide rule, and calculator for performing calculations, the typewriter and word processor for processing text, and the telephone, radio, and television for communicating” (Guinee et al., 2003).

ICTs have been present for the last decades, and since then, the entire world’s society and economy have been organized based on them. Nowadays, everybody is surrounded by computers, vast amounts of information and several aspects of technology. This entails creating a new ideology and lifestyle different from previous generations. This new “digital generation” residing in the Information Age is actively involved in Information networks on a daily basis.

Information and communications technology (ICT) is often used as an extended synonym for information technology (IT). Still, it is a more specific term that stresses the role of unified communications and the integration of telecommunications (telephone lines and wireless signals), computers, software, middleware, storage and audio-visual systems that enable users to access, store, transmit, and manipulate information.

The term ICT became popular after it was used in a UK report by the government by Dennis Stevenson in 1997 and the revised National Curriculum for England, Wales and Northern Ireland in 2000. However, in 2012, the Royal Society recommended that the term ICT should no longer be used in British schools "as it has attracted too many negative connotations". Consequently, as of 2014, the National Curriculum was changed to use the word computing, reflecting the addition of computer programming to the curriculum.

1.3 The Transformation of Digital Media

Digital technologies have fundamentally altered the nature and function of media in society, reinventing age-old public communication practices and, at times circumventing traditional media and challenging its privileged role as gatekeepers of news and entertainment. According to John Pavlik (2008), the transformation of Media into the new digital state manifests itself over the following distinct dimensions (Pavlik, 2008):

- the digital distribution medium,
- the equipment used to access digital media content,
- consumers of digital media content,
- the producers of digital media content,
- the digital media content itself,
- the distributors of digital media,
- the digital media investors, entrepreneurs, and enterprises,
- the digital media legal and regulatory framework,
- digital media technological advances,
- the creators and innovators of the digital media next generation,
- the ethics of digital media,
- the next generation of digital media consumers.

Each sector will be summarily analyzed below.

1.3.1 The Medium

This dimension refers to the physical means and technologies that allow for transmitting and receiving the digitalized content. Remarkable technological advances have supported the delivery of digital content in the initial stages. Regarding TV broadcasting, advances included Digital TV audio and video in computerized formats with faster and error “free” frame rates, high-definition TV (HDTV) or Interactive TV features. Terrestrial communications played a role in developing fixed or wireless communication technologies along with satellites supporting content delivery through space. DSL and VDSL technologies exploited the existing copper wires infrastructure while fiber cables increased data rates’ transmission, offering the necessary broadband means for what followed.

1.3.2 The Devices

This refers to the devices that support producing and consuming digital content while allowing for interaction among users. Among these devices were desktop PCs, mobile access devices, video game consoles, DTV displays and smart TVs as their successors and generally all devices designed for viewing digital video or listening to digital audio. Devices for accessing or displaying digital content have gone and are consistently undergoing dramatic changes. According to Moore’s Law, the number of transistors in a computer doubles every 18 months, therefore, it is difficult to predict how the successors of smartphones or other smart devices

will be. Advances are reflected not only in processors but also in batteries and screens, all in less space and lower price. The integration of smartphones has made them the ultimate "all-inclusive" portable device that today supports the role of separate devices of the past. **Figure 1.1** shows the most popular devices used in 2014 to access social media services.

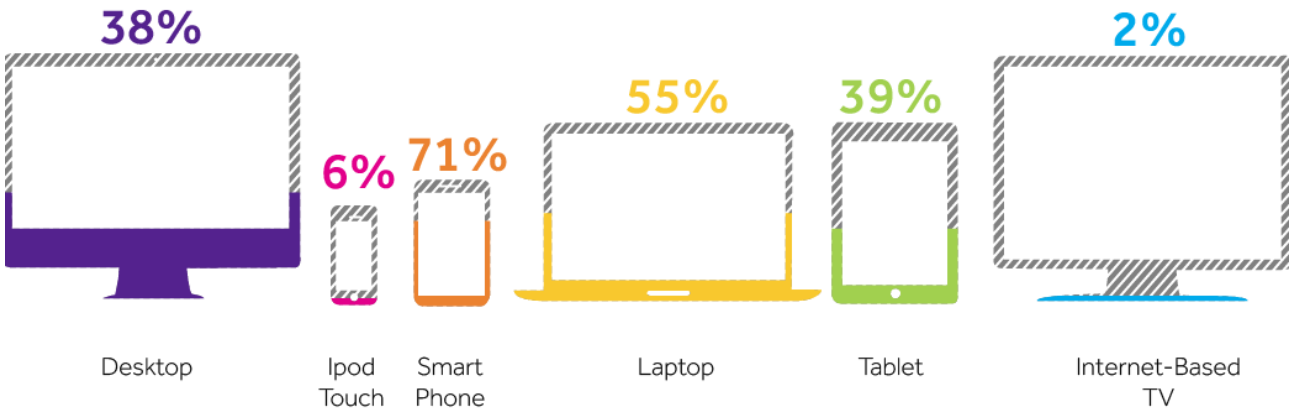


Figure 1.1 *Most popular devices to access social media in 2014 by Mammoth team (Source: Sensis, 2014).*

1.3.3 The Audiences

According to Pavlik (2008), the audience is an evolving concept. Passive receivers of the past have been substituted by active users who not only consume digital content but also produce it while interacting with that created by others. The discussion has now moved to whether Habermas' Public Sphere will take root in the interactive online arena. The German philosopher Juergen Habermas defined in the article *"Civil Society and the Political Public Sphere"* the Public Sphere as a "network for communicating information and points of view, gradually transforming into public opinion." Answering this question has been subject to investigation among scholars globally, and it seems that it requires time for a precise answer. Habermas describes these principles for an effective Public Sphere: accessibility, inclusiveness and privacy protection. All these issues will be analyzed in the following chapters of this book.

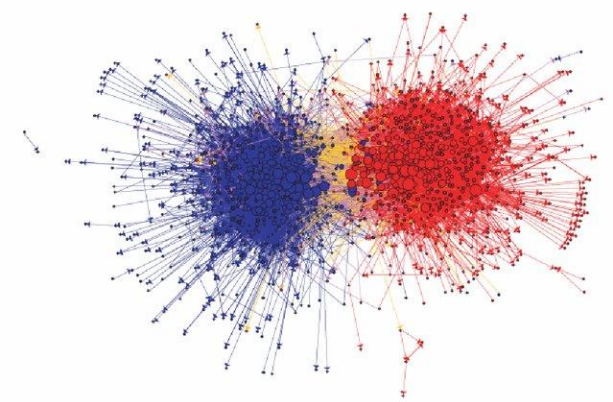


Figure 1.2 *US biased political system: Republicans vs. Democrats in the political blogosphere (Adamic and Glance, 2004).*

Contemporary active audiences can form interactive communities through discussion forums, the blogosphere and online social networks. **Figure 1.2** shows the US biased political system in the 2004 presidential elections, where blogs supporting Republicans and Democrats formed a social network with two clusters representing political discourse online between the two parties.

It is widely accepted that interactive communities generate, in many cases, more heat than light, but they also grapple intelligently and thoughtfully with the day's issues. They generate energy and influence that reach into the real world of politics and Media while they shape the daily agenda, the events and the decisions of the day (Pavlik, 2008).

1.3.4 The Producers

In the analog world, a relatively small number of increasingly large publishing companies, such as newspapers and magazines, came to control the means of print publication. On the contrary, in the digital age, there has been an exponential increase in the diversity of Sources of Media production, especially those dealing with text and graphics. Digital media content can still find its way onto national program networks; if not, it can reach the audience through other alternative distribution media like YouTube or Yahoo.

The international perspectives of digital media should be pointed out at this point. Digital content producers can now participate in the global flow of information and media programming. Moreover, the flow of information is not dominated anymore by advanced information societies while dramatic changes in journalism are taking place. Establishing credibility and believability between producer and audience, which is the only real value a journalist has, is now unavoidable.

On the other hand, there is no guide to online content, and users need to search on their own, a process that requires, at least in the initial stages, some digital literacy, which should not be assumed. Some also point out the conflicted "reporter-source relationship," a problem derived from Computer-mediated Communication (CMC) features.

1.3.5 The Content

Content is a core component of all media, regardless of their form. With the rise of digital technologies, media content is undergoing dramatic changes. The bibliography suggests four fundamental content forms according to typology criteria (Pavlik, 2008):

1. Content previously developed, tested and proven to have an audience, e.g. a newspaper distributed in digital form as a PDF document.
2. The content may include additional interactive features, e.g. the PDF document may now include hyperlinks.
3. Original content adhering to traditional design, e.g. HDTV: same narrative structure as traditional TV but more compelling experience, e.g. higher resolution, vivid colors, improved audio.
4. Original content designed for the digital domain from scratch, e.g. 360-degree spherical images, blogs, Wikipedia etc.

Digital content is dynamically evolving as a product of intense global research. For example, further experiments occur in the Integrated Media Systems Center (IMSC) at the University of Southern California, where some of the next generation of journalism technologies are developed. Multiple content forms may converge, e.g. Google News is an example of Form 2 & 4 convergence; automatic news tracking according to personal interest and previous search history through computer algorithms. Content forms 1, 2 and 3 are the most commonly produced by established media companies and organizations.

1.3.6 The Distributors

Since the beginning of modern mass communication, those who have controlled the means of media distribution have always had enormous power. According to Karl Marx, a ruling elite (government leaders, media owners) in every society controls the means of production and distribution of media. The ideas of this

ruling elite tend to dominate the society. Media distributors have often exerted significant influence over public opinion and reaped huge financial gains (Pavlik, 2008).

In the analog age, mass media dependent on expensive and limited means of production and distribution. Digital media tend to transform the system: Distributors of DM are growing rapidly and there needs to be more control over the means of their distribution. This itself is a potential fundamental shift in society.

In some cases, leading media distributors are the same as analog media distributors. However, in numerous other cases, new companies or nonprofit organizations have emerged as leading, if not dominant, players. Google is the foremost distributor and aggregator of digital media, including news, information, audio and video. iTunes has also emerged as a major distributor of digital music, movies and other multimedia.

These new and evolving digital media distributors are rewriting the media landscape and have helped the consumer move even closer to a system of entirely on demand media (Pavlik, 2008).

1.3.7 The Financers

According to Pavlik (2008), four business models took shape in the digital media age:

- Advertising supported digital media, e.g. Yahoo! Music that is free to the user but supported by online advertising, which enables a wide variety of tools that maximize advertising efficiency and allow for targeting.
- Sponsored digital media production. Moreover, a hybrid advertising and sponsored media technique is “Stealth advertising” where a product’s name is inserted into a TV program, movie, book or website.
- Premium on demand Media, e.g. media channels, movies’ rentals or sales.
- Transferring the cost of creating the digital media content to the end user. Producing quality content requires time, resources, ability and talent that often translate into a price, primarily micropayments that users cover.

A few major companies dominate the digital media landscape, in terms of finance. The six most prominent players in the digital age have been for quite a while, US companies: Viacom, News Corporation, TimeWarner, Walt Disney Pictures, CBC and General Electric (Pavlik, 2008).

Business models for media in the digital age are in flux due to uncertainties, unsettled technologies and changes in the audience or users. Only some media organizations have settled on a viable long-term strategy. Success stories may exist but only a limited number of cases have demonstrated that any model can be applied effectively across a broad spectrum of media properties (Pavlik, 2008).

1.3.8 Legal and Regulatory Framework

Whether digital or analog, media operate in a system constrained and governed by law and regulation. The basic laws were created during the analog age, and in many cases still operate and govern digital media. However, new law and regulations have been enacted in an effort to manage the digital system.

For many, it needs to be clarified who benefits nowadays from the new law and regulation of the digital age. Scholars contend that the main change is giving an advance to profit corporate players by providing greater control over their business interests. Only time will show the benefits of regulations and Law in the digital media age.

1.3.9 Technologies

Production and distribution technology costs have fallen, and the tools to create content have become more accessible and more portable (Pavlik, 2008). Significant digital technologies established the first levels of the transformation of the production and delivery of media content: digital Image formats (jpgs), digital video and audio formats (mp3, mpeg), GPS (Global Positioning System), production and distribution software, Search Engines etc.

1.3.10 Innovations

Barriers for innovators to entry are much lower in the digital age. Therefore, the opportunities for innovation are available to a much broader spectrum of the public. Innovation is central to the improvement of Media, and the Internet has offered fertile terrain for innovation, by offering collaborative spaces where members of communities can share their ideas and experiments in order to provide the best solution for each case. The Internet itself was developed using a collaborative model. Brilliant minds including academics, and simple home users, created virtual spaces in order to solve common problems collaboratively.

1.3.11 Ethics

Throughout history, the goal of every media producer has been to build and maintain public trust. Digital technologies have exacerbated some ethical problems and raised new ones. If the media loses the public's confidence, users can easily look elsewhere for information and entertainment. The bibliography suggests two types of ethical problems: the errors of omission and the errors of commission. The second case, presents a more profound issue that is prevalent in numerous present day social media platforms, characterized by proliferation of fake news, fraudulent user accounts and automated programs (bots) that manipulate information, thus undermining public trust and negatively impacting international relations.

1.3.12 The Next Generation

Nowadays, children are exposed to DM at a young age, resulting in both advantageous prospects and adverse consequences. Many concerns are pointed out related to Privacy, Online dangers like cyber stalking or grooming, social effects stemming from isolation, and Health disorders like Internet addiction etc. The future of DM relies on the upcoming generation, specifically children, who embrace emerging technologies but may lack the necessary expertise to employ them in a secure and efficient manner. In this highly delicate aspect of the digital media revolution, parents, teachers, media professionals and policy makers all bear the responsibility to help guide the next generation in wisely utilizing and producing media in the contemporary technological age.

1.4 Cyber Cultures

The term “Cyberspace” describes the world and domains generated by digital information and communications technologies (ICTs). The term refers to the social conditions brought about by the widespread use of computer networks for communication, entertainment, business and the set of Relations and Actions in Electronic Space. Cyberspace is treated by scholars not simply as a parallel universe but as an extension and augmentation of the everyday physical one.

Cyberculture is the electronic environment where various technologies and media forms converge, e.g. Internet and email, online chats, personal communication technologies, mobile entertainment and information technologies, social media etc. There is no one cyberculture; there are many that have been normalized and domesticated into our everyday lives, of which the Internet is the most common (Nayar, 2009).

The term “cybercultures” includes all the Networked, Electronic, Wired and wireless cultures of the last three decades.

Computers, digital technologies and communications systems play a significant role in today’s digital media world and the Internet networked cultures. While reducing cybercultures to the Internet cultures is tempting, the right approach invites a more broad-based perspective.

Any study of cybercultures must address all aspects of the so-called Information Society, which is intimately linked to globalization. The Information Society has been defined by Webster (2003) as an order where there is:

- Increasing convergence of telecommunications and computing in everyday life, production, consumption and politics.
- An increasing importance of knowledge production.
- An ever increasing number of people involved in information work.
- Networking of cities and spaces via flows of information through telecommunication networks.
- An increasing amount of information exchange in text, images and sound.

On the other hand, globalization is marked by the following features:

- The expansion of trade in terms of trading relationships and capital movements.
- The development of transnational and global communication networks.
- The diminished role of the nation-state even within its territorial space.
- The rise of transnational cultural, economic and political networks (e.g. Amnesty International, Greenpeace etc.).
- The increased presence of Western consumer products and cultural artifacts (the so-called “McDonaldization” of the world).

An illustration of globalization can be seen in the scenario where a shirt originating from Chinese cotton, was manufactured by workers in Thailand and subsequently transported by a French freighter, operated by a Spanish crew, before reaching its final destination, the US, a fifth country for retail purposes. Consequently, individuals from four different origins participated in the manufacturing operation before the shirt’s arrival in a fifth country for retail. As it may be obvious, the Internet is a major contributor to globalization, not only technologically but in other areas as well, like the cultural exchanges of art. For instance, students may enroll in online educational programs from anywhere worldwide and access new information on virtually any topic.

According to the literature, the features of popular cybercultures are convergence, remediation, consumption and interactivity. Moreover, some critical social issues related to Cybercultures are the following (Nayar, 2009):

- Globalized Transformation of Capitalism,
- Transition to the Posthuman Condition,
- the Digital Divide,
- E-government,
- Social Mobilization,
- Internet governance,
- Identity Expansion,
- Race features,
- Status Update,

- Gender issues,
- Alternate Spaces,
- Peril and Anticipation,
- Mediated Space,
- Art issues.

Each of the above will be presented more thoroughly in the following paragraphs.

1.4.1 Globalized Transformation of Capitalism

The advent of high-speed communications has been enabled by globalization. Therefore, capitalism has been substituted by technocapitalism, which refers to changes in capitalism associated with the emergence of new technology sectors, the power of corporations, and new forms of organization (39ikipedia.com). The new distributed nature of production, management and consumption demanded technological linkages and synchronous 24/7 communication which digital media has supported.

Globalization has evident material consequences: cybercultural forms, informational economy, and ICTs exist and function under these conditions. According to Castells (2001), managing information and financial flows is the key focus in globalized technocapitalism. The case of *Amazon.com* is the foremost example of the linkage between globalization, technology and commerce.

1.4.2 Transition to the Posthuman Condition

Virtual worlds enable users to transcend geography as well as their body. The body's limitations, such as diseases, degeneration or aging can be "overcome" through technological prosthesis. The result is the so-called augmented body, a situation many describe as "posthuman." With this perspective, subjectivity and identity are no longer rooted in the body in this posthuman condition: they are "dispersed throughout the cybernetic circuits" (Hayles, 1999). With this point of view in mind, research areas of cybercultures focus on the impact of computer technology and ICTs on real bodies social, cultural, economic and material conditions.

1.4.3 The Digital Divide

The term describes the uneven nature of access to and quality of Internet, electronic communication and cybercultures in general. A three-layer model is suggested for the digital divide (Norris, 2001):

- the global divide (divergence in Internet access between nations)
- the social divide (divergence in Internet access between social classes)
- the democratic divide (refers to the difference in the nature and quality of use of the internet and digital resources between users)

The digital divide refers to the gap between those who benefit from the digital age and those who do not. People without access to the internet and other information and communication technologies (ICTs) are put at a socio-economic disadvantage, as they are unable or less able to obtain digital information, shop online, participate democratically, or learn and offer skills.

1.4.4 E-government

Electronic government is the use of technological communications devices, such as computers and the Internet, to provide public services to citizens and other persons in a country or region. E-government offers new opportunities for more direct and convenient citizen access to government and for government provision

of services directly to citizens (wikipedia.com). The two key aims and principles in cases of e-governance are informational transparency and communication interactivity, referring to interactions between state agencies and citizens. E-government processes seek to increase transparency and enhance state citizen communication.

1.4.5 Social Mobilization

Digital technologies have been commonly understood to enhance civil society. Non-Governmental Organizations (NGOs), activists, experts and the general public now have greater access to information and greater chances of linking together to lobby. Social movements increasingly use the Internet as a communication medium, propaganda and political mobilization. Sometimes, such online political action might not have a material effect; cybercultural activism remains at the level of virtual and the resulting forms may be clicktivism or slacktivism.

1.4.6 Internet governance

Internet governance is the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet (wikipedia.com). Copyright Laws, Domain Names, National Security concerns are subject to this type of governance and regulations.

Governance concerns not simply the hardware of wires, terminals and routers, but also the consequence of modes of data transfer through codes or protocols. Governance concerns not only the physical components of technology, such as wires, terminals and routers but also the implications and effects of various methods of data transmission through codes and protocol. For example, the allocation of domain names and address space allocation are influenced by technical, economic and policy matters, and an example here is how a global Organization named ICANN has been introduced. The Internet Corporation for Assigned Names and Numbers (ICANN) manages the top-level development and architecture of the Internet domain name space. It authorizes domain name registrars, through which domain names may be registered and reassigned (icann.org).

1.4.7 Identity Expansion

In the real (offline) world, identity is a cumulative effect of negotiations, differences and discourses. In cyberspace, identity is malleable or unstable and the disconnect between the body and representation is infinite (Nayar, 2009).

Many might face obstacles in the real world posed by race, class, gender or sexuality when interacting others. On the contrary, cyberspace makes it possible to choose an identity that may have nothing to do with your life. Therefore, online identity can be expanded through additions from a variety of choices leading to a state of “fluid identity.”

1.4.8 Race features

It has been argued that cyberspace is a “raced” medium, where disembodiment, transcendence and fluid identities are privileges of the white race (Nakamura, 2002). The outsourcing of call center processes is an illustration of how businesses in the US are being supported by contracting companies in developing countries, (e.g. Asia) where costs are lower, despite the fact of having employees working during nighttime to accommodate the time difference.

1.4.9 Status Update

Even from the first stages of the transition to the digital age, there is a considerable demographic class, racial and national distinction between the wired and unwired. The hi-tech domain remains firmly in the hands of the techno-elite, who are predominantly white and male. “Status is augmented through techno-elitism” (Lake, 2013).

1.4.10 Gender issues

Today, many studies focus on issues related to cyberspace and women’s involvement. More specifically, research aims to investigated how women use ICTs for their empowerment, how the new IT environments portray them, how many have access to the ICTs world and what the role of women in the making of new technology is. Since there are issues of women representation in the digital realm, the main question is if cyberspace is as gendered as the real world. The movement of cyberfeminists seeks to feminize cyberspace by ensuring that the technology is appropriate for their use. Cyberfeminists seek to disturb power hierarchies by representing themselves in cyberspace.

1.4.11 Alternate Spaces

Cybercultures create alternate spaces and virtual universes that alter our experience of spatiality and location. For example, transnational activities have modified how that space is conceived online. The ideas of the nation state, which were firmly tied to matters of territoriality, have been altered. The physical environment involves structures and artifacts, while the electronic space consists of pictorial, aural and textual artifacts that enable and mediate social relations (Nayar, 2009). According to Manuel Castells (2001), the Internet possesses its own geography: the technical geography, the user geography and the economic geography.

1.4.12 Peril and Anticipation

Cybercultures generate their own forms of risk: Computer crashes, privacy invasions, financial fraud, stalking or cybersex addictions. It is generally accepted that while social media has offered great opportunities for socializing, there are also many emerging risks deriving from malicious use of the available tools. Cybercrimes, cyber warfare or cyber terrorism are among them. As Joost Van Loon (2002) suggested, “we live in a state of anticipating risk” and “risk is always potential, always waiting to happen or becoming real.”

1.4.13 Mediated Space

The mass media is a space of appearance (Silverstone, 2007). As such, the Internet serves an important social and political purpose. Mediapolis is the “mediated space” of appearance in which the world appears and through which we learn about the others. Computer mediated communication (CMC) supports this by projecting on the screen and the media the “constructed” world.

1.4.14 Art issues

Last but not least there is the aesthetics’ issue. Aesthetic Computing is the application of the theory and practice of art to the field of computing (Fishwick, 2006). It includes looking at the internal, mathematical structures of computing, the use of software to create art (software art), or the art of the interface (Nayar, 2009). Aesthetic computing focuses on specific areas, such as human computer interaction (HCI), visualization, location and design of the desktop or arrangement of the hardware. The interface of a computer can be regarded as a set of cultural signs (Nayar, 2009). A computer design can be considered a form of Art, which is

why the Apple's *Power Mac G4 Cube* has entered the New York's *Museum of Modern Art* and six other Apple products. The museum's collection also includes a 1984-vintage Macintosh and a QuickTake digital camera.

1.5 The Internet Culture

Manuel Castells (2001) describes four interrelated cultures of the Internet: the techno-meritocratic culture (the "techno-elites'" culture), the hackers' culture, the virtual communities' culture and the entrepreneurs' culture.

The fundamental concept of the techno-elites' culture is the Open-Source Software, which is software that is distributed with its source code, making it available for use, modification, and distribution with its original rights. Therefore, it is a collaborative product, where all have contributed to its development. The techno-elites' culture is rooted in the tradition of academia and science. The primary objective of this culture is to pursue discovery. Its value is judged by its peers in the community while its members legitimize their membership by demonstrating the relevance of their contributions to science and technology.

According to Castells, the hackers are not the typical anti-social saboteurs portrayed by the mass media. These are champions of freedom and open software. Their early role in the development of the Internet was to ensure that the Internet would keep embodying the spirit of freedom. They, therefore, worked from the early stages to protect its digital liberties. They are also motivated by creativity and innovation, which is allowed to flourish in the open environment and their independence from institutions.

The virtual communities' members use the Internet for community-building and social interaction. Individuals in this culture use the Internet for various reasons, such as seeking entertainment, relationships, hobbies or engaging in political discussions.

The entrepreneur culture of the Internet helped transform business practices. They try to attract venture capitalists to invest in their innovation or idea, and then try to disseminate it across the world. The entrepreneurs successfully raised massive amounts of capital to bring the Internet to the masses (commercialization of the Internet) but without (entirely) changing its character. Unlike their predecessors, the entrepreneurs are extremely money-driven (Castells, 2001).

According to the statements above, the culture of the Internet itself was indeed shaped by the culture of its inventors. In a way, they demise their own culture to the medium itself. Indeed, the culture of the Internet today is made up of a technocratic belief in the progress of humans through technology, enacted by communities of programmers thriving on free and open technological creativity, embedded in virtual networks aimed at reinventing society, and materialized by money-driven entrepreneurs into the workings of the new economy (Castells, 2001). Sociologically speaking, this phenomenon is unique in the history of technology and predisposes to the amazing implications of the Internet that will be analyzed in the following chapters of this book.

1.6 Conclusion

As an introduction, the initial stages of digital media were presented by outlining the various dimensions through which media underwent transformation in order to integrate into the digital realm. This process gave rise to a number of cybercultures that evolved and will continue to be domesticated in the digital age of humanity. Their descriptions in this chapter are introductory to the issues that will be presented in the next chapters.

For historical reasons, the multifaceted nature of digital technologies was highlighted, but due to of digital convergence, they were brought into a state of operating with the Internet as the delivery platform.

The next chapter will introduce the Information Society and the transition to the contemporary Network Society. In chapter 4, the initial Web 1.0 nature of the Internet will be presented, followed by the transition to the Web 2.0 age, where social media came into life along with online social networking. The phenomenon of virtual online communities will also be presented.

Subsequently, the Networked nature of contemporary digital media will be analyzed followed by the YouTube case study.

The crucial issue of the Digital Divide will be analyzed in Chapter 5, opening the discussion over digital media and their relation with politics. More specifically, the connection between them and Democracy will be analyzed in Chapter 6 and the connection of social media with Politics will be thoroughly presented in Chapter 7.

The Electronic Government aspects will be outlined in Chapter 8 followed by those of e-Commerce and e-Business in Chapter 9.

In Chapter 10, the phenomenon of Social Movements and online activism will be presented. The illegal or malicious use of the Internet will be described in Chapters 12 and 13, with Cybercrimes, Cyberwarfare and Cyberterrorism being presented there. The terms Deep and Dark Web will also be defined.

The Privacy, Cybersecurity and Surveillance issues in the Digital Age will be highlighted in Chapter 13.

In Chapter 14, the impact of digital media on Education and the new generation will be presented, and finally, the implication of digital media in Marketing will be given in Chapter 15.

References

Adamic L. A., and Glance N., (2005). "The political blogosphere and the 2004 US election: divided they blog." *LinkKDD '05: Proceedings of the 3rd international workshop on Link discovery*, New York, United States: Association for Computing Machinery.

Castels M., (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

Fishwick P.A., (2006). *Aesthetic Computing.* MIT Press.

Flew T., (2008). *New Media: An introduction.* Melbourne: Oxford University Press (3rd. Ed.).

Guinee, K., Eagleton, M. B., & Hall, T. E. (2003). Adolescents' Internet search strategies: Drawing upon familiar cognitive paradigms when accessing electronic information sources. *Journal of Educational Computing Research, 29(3)*, 363-374.

Hayles K., (1999). "How We Became Posthuman," *Virtual Bodies in Cybernetics, Literature, and Informatics*. Chicago: The University of Chicago Press.

Jenkins H., (2006). *Convergence Culture*, New York: New York University Press.

Lake, R. W. (1999). Postmodern urbanism?, *Urban geography*, *20*(5), 393-395.

Martin A., and Rader H., (2003). *Information and IT literacy: Enable learning in the 21st century*. Facet Publishing.

Nakamura L., (2002). *Cybertypes: Race, Ethnicity, and Identity on the Internet.* Routledge, 1st Edition.

Nayar P. K., (2009). *An introduction to New Media and Cybercultures*. Willey-Blackwell.

Norris P., (2001). *The Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge University Press.

Pavlik J. V., (2008). *Media in the Digital Age*. New York: Columbia University Press.

Silverstone R., (2007). Media and Morality: On the Rise of the Mediapolis. Cambridge and Malden. European Journal of Communication - EUR J COMMUN. 22. 511-513. 10.1177/02673231070220040804

Stevenson D., (1997). "Information and communications technology in UK schools: An independent inquiry." London: Independent ICT in Schools Commission.

Thompson J.B., (1995). *The Media and Modernity: A Social Theory of the Media*. Polity Press.

Turner F., (2006). *From counterculture to cyberculture*. The University of Chicago Press Ltd.

Van Loon J., (2002). *Risk and Technological Culture: Towards a Sociology of Virulence*. Routledge, 1st Edition.

Webster F., (2014). *Theories of the Information Society*. Routledge, 4th Edition.

Chapter 2 From the Information Society to the Network Society

Abstract

In Chapter 2, the features of the Information Society are described. The prevailing social, economic, cultural and technological factors that promoted the rise of the so-called Network Society are presented in the way this is defined by Manuel Castells and Van Dijk. The main features of this new social morphology of societies, whose key social structures and activities are organized around electronically processed information networks, are presented. The Information Society is projected as a societal state where all social entities increasingly organize their relationships in media networks, gradually replacing or complementing the social networks of face-to-face communication. The aforementioned social states are juxtaposed with the main features of globalization in an attempt to critically interpret their mutual influence and coexistence in the dynamic realm of constantly evolving technology. Finally, the digital identities crafted by individuals in the Digital Age are analyzed.

2.1 The Information Society

Early analyses of the term "*Information Society*" started between 1962 and 1970 in the US. In 1962, Fritz Machlup talked about the "Distribution of Knowledge in the US," while Marc Porat outlined the term "*The Information Economy*" in 1970. From the late 1970s to the 1990s, analyses looked further afield as ICTs were deployed extensively in rich or developed countries, Now, analyses focus on the potential and promise of the internet, leading to the current widespread interest in the global information society.

Fritz Machlup was the first to categorize Knowledge and Information tasks separately from normal industrial and social activities. He then, identified five sectors of Knowledge and Information that could be measured and assigned economic value: education, communication media, information machines, information services and information activities. This categorization enabled Machlup to claim that in 1958, 29% of the US Gross National Product came from these "Knowledge" industries.

Peter Drucker argued in his book "The Age of Discontinuity" (1968) that in the postwar period, "the base of our economy shifted from manual to knowledge work" and that "[the] center of gravity of our social expenditure shifted from goods to knowledge." He claimed that "the impact of cheap, reliable, fast and universally available information" would be as great as the impact of electricity. Knowledge Economy is the use of knowledge to produce values (tangible or intangible). Knowledge Technology, on the other hand, helps transform a part of human knowledge into machines, such as artificial intelligence (AI).

The term "Post-industrial Society" introduced by Daniel Bell (1973), is a closely related concept to Information Society. According to sociology, it is the stage of society's development where the service sector generates more wealth than the economy's manufacturing sector. In a post-industrial society:

- The economy undergoes a transition from the production of goods to the provision of services.
- Knowledge becomes a valued form of capital.
- Producing ideas is the leading way to grow the economy.
- Through processes of globalization (analyzed later in the chapter) and automation, the value and importance of manual labor to the economy decline, while those of scientists, creative-industry professionals, and IT professionals grow considerably.

An information society is one where information creation, distribution, use, integration and manipulation are significant economic, political, and cultural activities. The information society aims to gain a competitive advantage internationally, by using information technology (IT) creatively and productively. The knowledge economy is its economic counterpart, whereby wealth is created through the economic exploitation of understanding. People who have the means to partake in this form of society are sometimes called digital citizens (Wikipedia.com).

The growth of economic information can be quantified in 3 different ways, according to the society's technological capacity to store, communicate and compute information. As to present a view of the growth of Information in Society in recent years, here are some interesting details (Hilbert & López, 2011):

- The world's Technological storage capacity in 1986 was less than a CD-ROM per person. In 2007, it increased to 60 CD-ROMs per person. This means that the amount of information stored globally grew from 2.6 exabytes in 1986 to 309 exabytes by 2007.
- In 2007, the world's Technological capacity to receive information over one-way communication channels was 174 newspapers per person daily. This means that humankind received 1.9 zettabytes of optimally compressed information through its one-way communication broadcasting channels.
- In 1986, the world's technological capacity to exchange information over two-way communication channels was 0.02 newspapers per person per day, which was doubled by

1993. In 2000 it became 0.2 newspapers per person per day and reached six newspapers per person per day in 2007. This means that humankind telecommunicated 65 exabytes of optimally compressed information through its two-way telecommunication channels.

- In 1986, the world's Technological capacity to compute information was 300 million Instructions per second (MIPS). In 2007, it reached 6,400,000 million MIPS. This indicated a sustained annual growth rate of 60% for two decades.

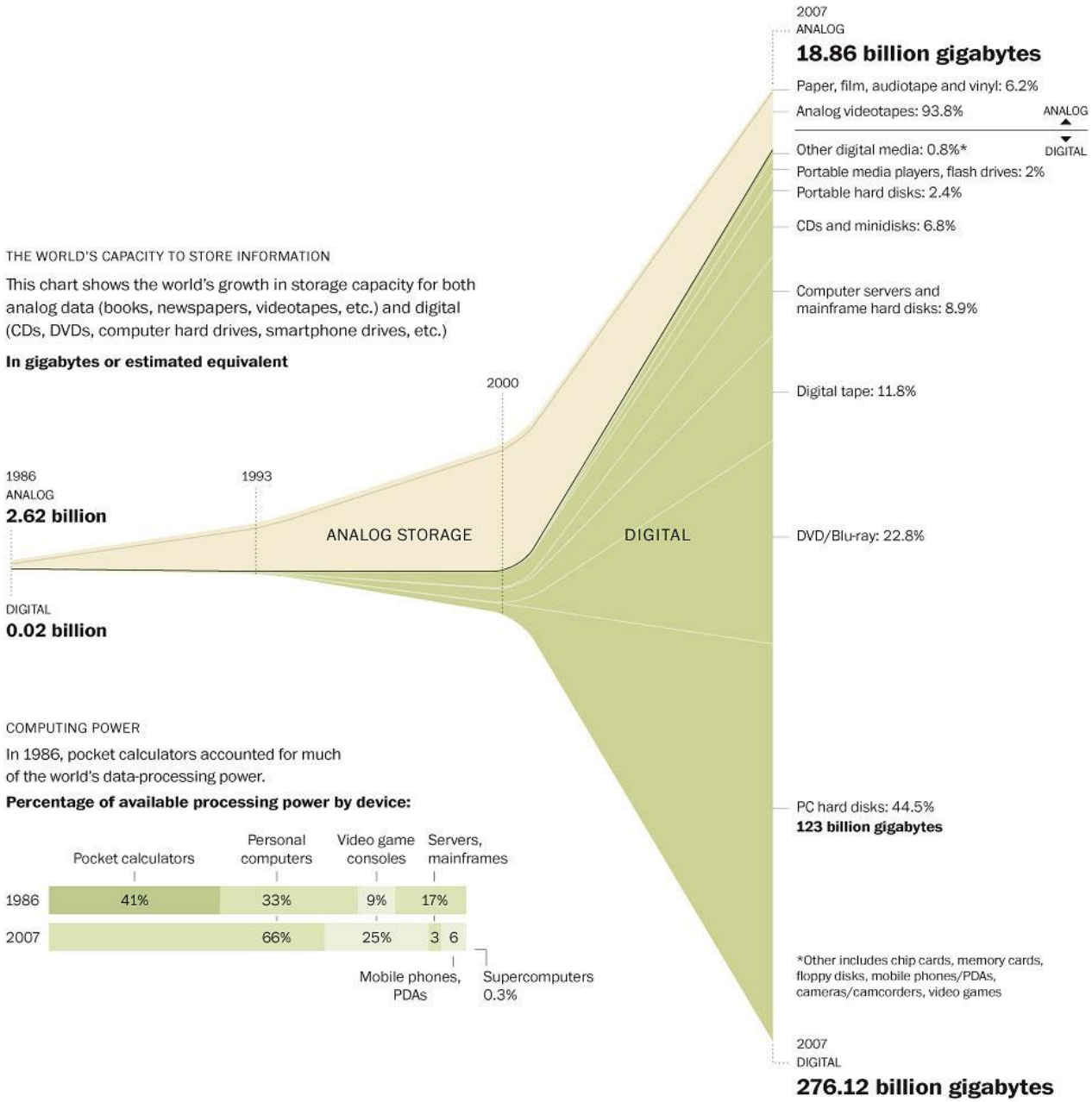


Figure 2.1 *Global Information storage Capacity in optimally compressed bytes (source: Hilbert & Lopez, 2011).*

Figure 2.1 demonstrates visually how digital information has exploded over the past two decades (Washington Post, 2011). The underlying data came from a study by Martin Hilbert and Priscila Lopez of the University of Southern California entitled "The World's Technological Capacity to Store, Communicate, and Compute Information." The total storage capacity in the global datasphere is expected to increase from 6.7 zettabytes (ZB) in 2020 to around 16 zettabytes in 2025.

As stated in the previous chapter, in 2003, Webster defined the Information Society as an order of increasing convergence of telecommunications and computing, allowing for networking via information flows. In this current state, the process of generating knowledge has transformed significantly as an increasing number of individuals engage in information-oriented tasks, exchanging information, via text, images, sound or video. Subsequent to that time, significant transformations have taken place, introducing the age of the Network Society.

2.2 The Rise of the Network Society

Reid Hoffman, an entrepreneur whose venture capital investments include *Aurora*, *Blockstream*, *Coda,* and *Convoy,* had once wondered if humankind could see the networks around. He pointed out that "when you truly see networks around, it changes how you plan and strategize. You move differently" (LinkedIn, 2014).

In this way, Hoffman underlined the necessity of exploiting the power of networks in contemporary societies. He mentioned two examples to support his arguments. First, there is the case of job hunting. In the Information Age, the method to find a job was to look for it thoroughly in job listings. The Network Age approach requires a different strategy: to look for people with connections to companies, trace the best path from these connections to people who can share helpful intelligence and therefore ask for an introduction to those people. This way of thinking is not impersonal and uses the influence that important actors of the game may have. Another example he used was the case of investing. The Information Age approach requires forming an investment theory and searching for a startup that fits this theory. It would be helpful to purchase some ad space in the Yellow Pages so talented entrepreneurs can find you. the Network Age paradigm suggests an alternative approach for handling the situation. It entails prioritizing the role of being a valuable ally within one's network and cultivating strong relationships characterized by a mutual beneficial exchange of information. Additionally, it is crucial to position oneself strategically at various pivotal points in the network as this will inevitably lead to connections with entrepreneurs and investment opportunities (LinkedIn, 2014).

Essentially, this logic implies an entire literacy behind the scenes. A decade ago, John Battelle stressed the importance of search literacy. Back then, people skilled at using Google to find information had an edge over those who had yet to acquire this aptitude. In the Information Age, if somebody cannot make sense of an increasingly information-rich world through effective search capabilities, they are bound to be culturally marginalized. Similarly, the Network Age requires some network literacy in order for somebody to gain competitive advantages.

Today, those who can conceptualize and understand networks have an edge in today's fast-paced and hyper-competitive landscape. Hoffman has suggested three levels of network literacy (LinkedIn, 2014):

- **Basic level**: using network technology,
- **Advanced level**: establishing a digital identity (analyzed later), in fact, a network identity,
- **Master level**: utilizing network intelligence.

At the basic level, users become members of online social networks like Facebook or LinkedIn. They realize that social networking sites are not just announcements but a place to strengthen personal relationships. Therefore, phrases and keywords are used with deliberately, to maximize their discoverability. At this level, they start to understand that the networks are an excellent place to craft their network identity by tailoring their profile to maximize chances of being discovered by the people or groups they want. According to Hoffman, this is the initial stage of thinking in a network-literate way.

In the Advanced Level, it is the time for users to establish their network identity. Their presence is highly annotated with readily apparent links to colleagues, mentors, institutions, and other entities that have helped shape the contours of this identity. In the Networked Age, the professional identity expands beyond job titles

and the employing company. Users begin to understand that their identities are not limited on their individual profiles. They encompass their connections, their perceptions others have for them, the knowledge of others and so forth. Users at this level are increasingly adopting this way of thinking. Moreover, they understand that their identity is multivariate, distributed, and partially out of control. And it is their network that helps shape their identity accordingly by understanding that increasing one's network literacy means also understanding other people's network identities.

The master level is the level that presupposes utilizing network intelligence. Here, users know that information proliferates faster in the Networked Age than in the Information Age. Their networks are their first reads because pipelines have been consciously built up with people that reliably deliver information which is highly significant and relevant to them. The "dark net" of critical-edge information, which hasn't made it into newspapers and blogs, is just a few keystrokes away. Users are also aware of who the news breakers are, the thought leaders, the critics, and sceptics, and they are familiar with their preferred sources and biases. To be truly network literate is to always be thinking of how one can add value to the networks he is a part of, and to make it a priority to turn connections into relationships, and relationships into alliances.

Fritjof Capra wrote in 2002 that "the network is a pattern that is common to all life. Wherever we see life, we see networks." For Manuel Castells (2001), "networks have become the basic units of modern society." He also claimed that: "networks constitute the new social morphology of our societies, whose key social structures and activities are organized around electronically processed information networks."

Network Society is an expression coined in 1981 related to the social, political, economic and cultural changes caused by the spread of networked, digital information and communications technologies. A network society is a society whose social structure is made of networks powered by microelectronics-based ICTs. The diffusion of networking logic substantially modifies the operation and outcomes of processes of production, experience, power and culture.

Van Dijk (2012) defined network society as "a form of society increasingly organizing its relationships in media networks gradually replacing or complementing the social networks of face-to-face communication." For Van Dijk, information forms the substance of contemporary society, while networks shape its organizational forms and infrastructures. He also argued that modern society is in the process of becoming a network society. For him, interpersonal, organizational and mass communication come together on the internet. Networks, as basic units of modern societies can be individuals, groups, organizations or communities, while people become linked to one another and can have access to information and communication with one another constantly.

In his book "The Rise of the Network Society," Castells wrote (1996) that "the network society goes further than the Information Society" and "it is not only technology that defines the network society. It is also cultural, economic and political factors." For Castells, the availability of proper technology is a necessary but insufficient condition for transforming social structure. It was only under the needs of a mature industrial society that this could happen (Castells, 1997).

Scholars suggest that networks became the most efficient organizational forms due to three significant features of networks that benefitted from the new technological environment: flexibility, scalability and survivability. Flexibility means that networks can reconfigure according to changing environments, keeping their goals while changing their components. Scalability is for being able to expand or shrink in size with little disruption, while survivability stands for having no center, being able to operate in a wide range of configurations, and resist attacks to their nodes and codes.

According to Castells (2001), the Network Society is the technological paradigm of the Information Age. Similarly, he named the technological paradigm of the network Society "*Informationalism.*" Informationalism manifests itself in the added importance of knowledge, information and communication in the globalized

world, where human labor is increasingly involved in producing immaterial goods (Hardt and Negri, 2000). It refers to a technological paradigm that replaces and subsumes the previous paradigm of industrialism (Castells, 1996). The rise of informationalism as the new paradigm does not suggest that industrialism disappears as a material fact but only suggests that industrialism loses centrality in discourses of technology. Informationalism presupposes industrialism, as energy and its associated technologies are still fundamental to all processes.

2.3 Globalization

Globalization is a term used to describe how trade and technology have eliminated the fragmentation of the world and put it in a more interdependent state. According to the World Health Organization (WHO), it manifests itself over two inter-related issues:

- The facilitation of fast cross boarder exchanges of goods, services, finance, people and ideas through the liberalization of borders
- The changes in institutions and policies at national and international levels that facilitate or promote such flows.

Scholars put the starting point of globalization in the times of Columbus' discovery of the New World in 1492. However, people travelled across the globe many ages before, exchanging their ideas, products, and customs along the way. The Silk Road, an ancient network of trade routes across China, Central Asia, and the Mediterranean used between 50 BCE and 250 CE, is a good example. Greek culture spread across Africa, Europe and Asia under the rule of Alexander the Great. This is why there are dozens of cities named after Alexander in several countries, such as Egypt, Turkey, Iran, and Pakistan. Moreover, the Olympics began in ancient Greece and continue today, with people from all across the globe competing together in a wide array of sports and games. Christian missionaries from Europe also added to globalization by migrating from one country to another to convert people abroad to a new spiritual way of living.

Unquestionably, globalization went further in the Age of Exploration. Technology played an important role in the maritime trade routes that flourished between old and newly discovered continents. New ship designs assisted by the magnetic compass supported explorers to establish a new reality where goods and ideas, could travel fluently.

In the Age of Revolution, the ideas about liberty, equality, and fraternity spread very quickly from America to Europe and France, as well as to Latin America and beyond. The invention of factories, railways, steamboats, cars, and planes played a crucial role in facilitating globalization until it was superseded by the Information Revolution.

The Information Age boosted globalization. Advances in computer and communications technology launched a new era. Global news networks contributed to the spread of knowledge, while worldwide news is reported almost instantly through continual updates to online news outlets. Modern communications satellites meant the 1964 Summer Olympics in Tokyo could be watched in the United States for the first time.

Due to its scale and virtues, the Internet has played a pivotal role in expanding globalization even more. Developed in the '60s as a decentralized network of networks, it managed to join together hundreds of millions of computing and communication devices of varying types running various programs. The World Wide Web's magnificent application allowed someone in Greece to read about a breaking news story in the US in almost real time.

To a degree, the Internet's networking features, open architecture and spirit of digital liberties eliminated territorial borders, and promote an international spirit of communication. News, cultures, or ideas

can spread instantly and at almost zero cost. No matter the Digital Divide, a great part of the planet's population is still involved in this huge information exchange that supports a variety of human life.

The Internet has also altered the structure of mass media. Most of the news networks were local or national prior to the Internet revolution, and only a few companies could broadcast in other countries. Right after the new millennium, social media came to add more networking features to humanity's new game. People could form communities regardless of the place or time of Internet access. Social movements born in the northern hemisphere could very easily find supporters in the South, even become donators by making online transactions. The protestors in the Arab Spring had an excellent tool for instant coordination, spreading ideas across many Arab countries.

Additionally, this digital revolution massively impacted economies across the world as they became more information-based and more interdependent. Multinational corporations operate now more than ever on a global scale, with satellite offices and branches in numerous locations. This means international companies can stay open virtually 24 hours a day and service customers no matter where they are located.

The examples listed above show that the notions of Information Age, Network Society and Globalization are very tightly connected. In fact, one is boosting the other in an endless dynamically evolving state with unpredictable future implications.

2.4 Digital Identities

The digital identity is an important element of the digital age. It has reached its contemporary state after the rise of the Network Society, as described in the paragraphs above. In the context of "Computer mediated discourse analysis," digital identity is referred to as being constructed through interaction, fluidity, and openness to revision (Seargeant & Tagg, 2015). Research on the topic of online identities, has argued that online identity can be easily altered or abandoned, as it is seen as a mere facade or mask. Furthermore, individuals are not expected to have any connection or similarity between their online and offline identities.

Now, there is a perceived shift from anonymously partaking in online forums to excessive self-expression via social media, and furthermore, not only language but also images and sometimes sounds have become the primary resources for online "identity work." In times of Internet Relay Chat, high emphasis was placed on nicknames to catch other participants' attention. Nowadays, social media sites, such as Facebook, Snapchat or Instagram, provide new ways for online users to present themselves, and make self-presentation far more dynamic and complex than those in older media, from creating user profiles to regularly updating status, messages and photographs (Lee, 2014).

Individuals can now portray themselves online in potentially more varied ways than in offline realities, which leads to the concept of "e-personality" to be "a virtual whole that is greater than its parts and that, despite not being real, is full of life and vitality" (Aboujaoude, 2011). Of course, one could easily argue that the "virtual whole" is indeed real regarding the consequences of online interaction, and this is why a lot of authors refer to the online/offline dimension of identity as a continuum rather than a polarity (Page, 2014; Vásquez, 2014).

Jochen Peter and his colleagues take a more educational approach to inventing and performing identity online and initially define social networking sites (through which individuals can facilitate identity construction) as "web-based services" that allow individuals to:

- Construct a public or semi-public profile within a bounded system.
- Articulate a list of other users with whom they share a connection.
- View and traverse their list of connections and those made by others within the system" (Peter et al., 2009).

Furthermore, they introduce five features of how individuals, especially adolescents, construct their digital identities on social networking sites. First, identity constructions occur "along a continuum of implicit and explicit identity claims" (Zhao et al., 2008). Implicit identity claims refer to the self as a social actor and its connection to peers, e.g. through uploading party pictures. Explicit identity claims portray the self as an individual actor, mainly through narrative descriptions. Second, identity construction on social media websites is partly a social identity construction, which refers to profiles as place markers within a social group, in which group attributes are internalized, and identity related information is used to reinforce or improve one's standing in a group. In the context of the relational self, insider jokes are quite important to reaffirm one's position within the group (Peter et al., 2009). A third feature is the dominance of social popularity claims (especially among adolescents), involving the "presentation of themselves as individuals worth having friendships with.", According to Peter et al. (2009), a fourth feature involves self-verification through positive or negative feedback given according to the authenticity of the portrayed online identity. Because of the roots of online social contacts in face-to-face relationships, negative feedback is often elicited by the presentation of over-idealized or inauthentic identities. A final feature of the construction of identity involves considerations about how to express a particular lifestyle and especially adolescents use their consumption preferences and tastes for "cultural products, such as films, music, and books, to locate their identities in a cultural space" (Peter et al., 2009).

As already stated above, many contacts and relationships on social media have their base in face-to-face relations which requires at least a minimum amount of consistency regarding an individual's offline and online identity. But by promising different contexts and anonymity to some extent, social media makes it challenging to resist pretending to be "thinner, more popular, and more successful than we really are" (Aboujaoude, 2011). It allows us to reinvent portions of ourselves we do not like and "of course identities in social media are not just about who we are, but also who we want to be to others, and how others see us or expect us to be" (Lee, 2014).

In the Network Society, it seems like all online activity is treated with distrust, and no individual's identity is taken "to be what it seems" (Page, 2014). On the other hand, it is not "that online representation is inherently inauthentic as compared with offline representation." Recent studies have shown that people don't give up their notions of authenticity while interacting online (Page, 2014). Still, there is an issue regarding "collapsed contexts", which can be described as the overlapping of segments of an individual's audience that are normally kept separate in offline contexts, such as the friends of Facebook consisting not only of the peer group, but also of the co-workers, and people from church. Since one is acting differently according to the general social context they are in, it is a huge communicative challenge to manage collapsed contexts (Page, 2014).

In expressing one's identity, users are provided with a variety of options to draw upon a wide range of multimodal resources. social media users are not limited to presenting themselves through the written word, e.g. in the description box of the profile but one can present oneself through a combination of images, videos, written and spoken language. But, whether subscribers on Facebook or Instagram "consciously and intentionally reinvent their biographies in part or in whole, presenting to the large virtual audience a new version of themselves, one that may in some cases bear little resemblance to the 'real me'" (Aboujaoude, 2011), or unintentionally adapt due to comparison, and the pressure to conformism. There are two options for the subscribers described by different authors of this matter. Elias Aboujaoude states that there is either an incorporation of the idealized "e-personality" into the offline self, which could lead to liberation, "allowing the person to transcend debilitating shyness, let go of stultifying inhibitions, and forge connections and friendships that would be impossible otherwise." Mark Leavy further describes the ambivalent character of the use of social media as follows: "While the Internet encourages dreams of wealth, health, and happiness, all of which can seem but a mouse click away, it also feeds self-distortion and delusion, by which I [M. Leary]

mean the ability to enhance or perfect oneself online simply by grossly misrepresenting one's identity." And if this is not incorporated to live up to this misrepresentation, sometimes it leads to believe in this misrepresentation of oneself, which then correlates with the godlike manner one can create for himself in cyberspace with an "explosion of narcissism and self-centeredness" (Aboujaoude, 2011).

2.5 Conclusion

Up to this point in this book, the historical as well as the theoretical background has been completed, which is considered essential for a deeper analysis of the multifaceted aspects of digital media. What will follow falls within the general concept of the Information Society integrated recently into the globalized Network Society: the world of Web 2.0 and social media. The opportunities and the risks that will be introduced will be deployed in the Digital World introduced so far, a vast scientific field where sociological, political and economic research is conducted. Regardless of the scientific standpoint, it is undeniable that the digitally enhanced existence of humanity is a permanent fixture and will serve as an ongoing source of inspiration for creators of digital media in the future.

References

Aboujaoude E., (2011). *Virtually You The Dangerous Powers of the E Personality*. New York: W.W Norton & Company, Inc.

Bell D. (1973). *The coming of post-industrial society: a venture in social forecasting*. Heinemann Educational Publishers.

Borcuch A., Piłat-Borcuch M. and Świerczyńska-Kaczor U., (2012). "The Influence of the Internet on Globalization Process." *Journal of Economics and Business Research*, pp. 118-129.

Capra F., (2002). *The Hidden Connections*. Doubleday, US.

Castells M., (1996). *The Rise of the Network Society*. Cambridge, MA: Blackwell.

Castells M., (1997). T*he Rise of the Network Society: The Information Age: Economy, Society, and Culture.* Willey-Blackwell, Volume I.

Castells M., (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press.

Drucker P., (1968). *The Age of Discontinuity*. Routledge, 2nd edition (January 30, 1992).

Hardt M., and Negri A., (2000). *Empire*. Harvard University Press.

Hilbert M., and López P., (2011). "The World's Technological Capacity to Store, Communicate, and Compute Information." *Science*, 332(6025), pp. 60–65. https://www.science.org/doi/10.1126/science.1200970

Hiltz S.R., and M. Turoff, (1993). *The Network Nation.* The MIT Press, Revised Edition. Lee C., 2014. "Language Choice and Self Presentation in Social Media: The Case of University Students in Hong Kong." in Seargeant, F./ Tagg, C. (eds.), *The Language of Social Media Identity and Community on the Internet.* New York 2014, pp. 91-111.

LinkedIn.com, (2014). "The Information Age to the Networked Age: Are You Network Literate?" Available at: https://www.linkedin.com/pulse/20140604152945-1213-the-information-age-to-the-networked-age-are-you-network-literate [Accessed 11 February 2018].

Machlup F., (1962). *Distribution of Knowledge in the US*. Princeton University Press.

Page R., (2014). "Hoaxes, Hacking and Humour: Analyzing impersonated identity on social network sites", Seargeant, F./ Tagg, C. (eds.), *The Language of Social Media Identity and Community on the Internet.* New York 2014, pp. 46-64.

Peter J., Valkenburg P.M., and Fluckiger C., (2009). "Adolescents and Social Network Sites: Identity, Friendships and Privacy." in Livingstone, S. and Haddon, L. (eds.), *Kids Online Opportunities and Risks for Children,* Bristol 2009, pp. 83-95.

Philip Seargeant P, and Tagg C., (2015). "The Language of Social Media: Identity and Community on the Internet." *Applied Linguistics*, Volume 36, Issue 5, December 2015, pp. 651–654, https://doi.org/10.1093/applin/amv008

Porat M.U., (1970). "The Information Economy: Definition and Measurement." Washington: The Office: For sale by the Supt. of Docs., US Govt. Print. Off.

Scholte J.A., (2000). *Globalization: A Critical Introduction*. Basingstoke and the New York: Palgrave, 2000.

Süss D., (2006). "Mediensozialisation zwischen gesellschaftlicher Entwicklung und Identitätskonstruktion," in Rehberg, K S. (ed.), *Soziale Ungleichheit, Kulturelle Unterschiede: Verhandlungen des32*. Kongresses der Deutschen Gesellschaft für Soziologie in München (Frankfurt a.M 2006) 3370-3380.

Thompson J. B., (1995). *The Media and Modernity: A Social Theory of the Media*. Polity Press.

Van Dijk Jan A.G.M., (2012). *The Network Society*. SAGE Publications Ltd, Third Edition.

Varnelis K., (2012). *Networked Publics*. The MIT Press; Reprint edition.

Vásquez C., (2014). "Usually not one to complain but…': Constructing Identities in User Generated Online Reviews," in Seargeant, F./ Tagg, C. (eds.), *The Language of Social Media Identity and Community on the Internet,* New York 2014, pp. 65-90.

Wampfler P., (2014). *Generation Social Media Wie digitale Kommunikation Leben, Beziehungen und Lernen Jugendlicher verändert.* Göttingen: Vandenhoek & Ruprecht GmbH.

Webster F., (2003). *Theories of the Information Society*. Routledge, 4th Edition.

Zhao S., Grasmuck S., and Martin J., (2008). "Identity Construction on Facebook: Digital Empowerment in Anchored Relationships." Computers in Human Behavior. https://doi.org/10.1016/j.chb.2008.02.012

Chapter 3 From Web 1.0 to Web 2.0
Social Media, Social Networking and Virtual Communities

Abstract

In this chapter, the terms Web 1.0 and Web 2.0 are explained, along with the processes behind this transition from the ordinary Web sites of the '90s, where people were limited to the passive viewing of content to, the technologies that allow users to interact and collaborate in an online dialogue as creators of user-generated content. social media is presented as Internet-based applications that build on the ideological and technological foundations of Web 2.0 that allow the creation and exchange of digital content. Contemporary social media platforms across the globe are presented, with Facebook, X (known as Twitter, up until the 24th July 2023) and Instagram being among the most popular. Most of these social media applications are envisaged as tools for implementing Digital Social Networking, and therefore the basic principles of the Social Networking Analysis (SNA) are figured. By applying these techniques, it is demonstrated how influence analysis and community detection can be made. It is also underlined how linkage data, combined with content Data Mining techniques, provide unprecedented opportunities for data analytics in the context of digitally implemented social networks. This context's essential policy, financial and social are also presented. Eventually, the formation of Virtual Communities on the Internet is highlighted. Their evolution from the Web 1.0 to the Web 2.0 state is presented, pointing out the main characteristics of each phase. Their genesis, causes and relationships between their members are presented, mainly focusing on their core attributes and the participatory culture of their members that lies behind.

3.1 Introduction

At the beginning of the century, new Internet applications were introduced, bringing the Internet user to the foreground by turning him from a passive consumer into an engaging and creative user, while contributing to creating online social networks whose operation dynamically promoted users' participatory culture. The new technological phase that the Internet has entered has been characterized by the term Web 2.0 or "Participatory Internet" or "Social Internet," signaling the change from the previous state of Web 1.0. The OECD recognized this trend and the growing role of social networks in modern democracies, proposing the name "Web 2.0 Participation and Information Model" for the new online participation model. social media have been the product of this transition, with online social networking being a side-effect of this new era. Its features and trends will be described in the following paragraphs.

3.2 From Web 1.0 to Web 2.0

The term Web 2.0 was first coined in 2004 during a conference organized by O'Reilly Media and MediaLive International, where ideas for upgrading the World Wide Web were proposed. In the early stages, the initial function of the Internet was limited to applications such as email messaging between its users. The development of the first web browsers allowed browsing the newborn World Wide Web, a vast collection of websites with content on various topics. These features outlined the so-called Web 1.0, where users could exchange messages via one way communication channels and download and passively watch published web page content.

Social evolution, as well as technology developments, led to the gradual highlighting of social networking, which led to the creation of services whose main feature was to put users at the center of the scene by making them content creators themselves and giving them the opportunity to participate, develop and design the new form of the web. The Web 2.0 term was coined to describe the second generation of internet services, which focuses on user's ability to share information and collaborate online. In this new context, the user is not simply considered a spectator, a customer, or a consumer, but someone who actively participates in the configurating and managing of web content. In the new digital realm, users communicate without geographical restrictions, technical expertise and computing equipment. The initial passive audience gradually evolved to a new status where the concepts of interactivity, collaboration and contribution played a leading role in this technological and social revolution. In this way, a social dimension was added to all previously developed Internet functions I.

Although the term Web 2.0 gives the impression that it is a new Web version, after all, it is not a new protocol or a new technology but refers to changes in the way Internet users would utilize existing technologies and the new guidelines by which IT designers would develop the new applications.

3.2.1 Definition and Features

According to the creator of the participatory internet Tim O'Reilly, Web 2.0 is a set of economic, social and technological factors that together form the core of the next generation Internet—a more mature means of communication that is open to all, is characterized by the participation of its users and the networking spirit (O'Reilly, 2005). Some of the features of Web 2.0 are listed below (Best, 2006; Greenmeier & Gaudin, 2007; Graham, 2005):

- The internet and all interconnected devices should be a global platform for reusable services and data, which derive mainly from the users and, in most cases, are exchanged freely.
- The only necessary tool should be a web browser running a Web 2.0 application regardless of the type of the accessing device, which could be a PC, a tablet or a mobile telephone, and

regardless of the operating system. The only prerequisite should preferably be a broadband Internet connection.

- Use of a "light" technology in terms of protocols, programming languages, user interfaces, and a trend for simplicity in their programming design.
- Open-source software.
- Multimedia and interactive user interfaces (Rich Internet Applications – RIA), dynamic content and websites that only update the changing part of the content (Ajax technology).
- Continuous and immediate software and content updates according to the customizable needs of the users.
- Adoption of a decentralization culture regarding data, services and standards.
- Open communication channels, feedback, information dissemination and publishing users' knowledge or opinions on various issues.
- Semantic content categorization features for more accessible information retrieval.
- Two-way user communication with peers, organizations or businesses and the ability to influence decision-making processes.

In the years that followed, there has been an increasing use of those Web 2.0 tools that allowed the users to create and handle the content they created: the User Generated Content. The term “social media” refers to these tools and they are considered the pre-eminent applications of the participatory Internet. They are tools of mass collaboration that empowered Internet users globally and allowed them to actively participate and collaborate in real time for the production, consumption and dissemination of information and knowledge circulated over the Internet. In other words, the Web 2.0 tools do nothing but enhance the awareness and exploitation of all the internet capabilities and of the initial conception of the internet as a platform primarily conceived to serve its own users. The main features of social media communication are the following (Χρήστου & Βαρουχάκη, 2008):

- **Sociability**: Social media facilitates creating online communities that communicate easily and efficiently with each other on issues of common interest.
- **Participation**: Social media encourages input from anyone interested in participating in them, shortening the distance between media and the public.
- **Accessibility**: Most social media do not create barriers to public participation and feedback. They encourage criticism, critical spirit and commentary, and also the circulation of information itself.
- **Compromise**: While traditional media operates based on one-way information transmission to the public, social media content has the form of public debate and two-way communication.
- **Connectivity**: Most social media is developed based on their ability to connect with other media while supporting the coexistence of many different media into one website.

The content produced by Web Applications 2.0 users significantly impacts on the profile, the expectations and generally the Internet users’ attitudes. These applications, as they were introduced back then, are presented in detail in the next paragraph.

3.2.2 Web 2.0 Applications

Web 2.0 includes applications, services, tools, and functions characterized by innovations and facilities that users desired and implemented when technology was ready to provide them. Once implemented, they were widely accepted and disseminated. Some of the main categories of Web 2.0 tools are:

Blogs

Blogs are websites that contain personal views, information, posts, links to other addresses, photos, etc. The entries are sorted in chronological order and start with the opinion or comment of the author on a topic, e.g. politics, science, or issues of the daily agenda. Their popularity derives from offering readers the option to comment on posts, thus opening a public debate with potential recipients, all visitors to a particular blog. Because of this popularity, the socialization feeling between participants and their impact on the physical (offline) world, many characterize them as an unprecedented social phenomenon. According to Rodzvilla and Blood (2002), blogs have been multimedia and user-friendly sites, which, through their chronology structure and their archiving capabilities, operate as individual and interconnected web filters, creating a new online public sphere that sets the web back to the public's disposal.

Micro-blogging

These are social platforms that allow contact and interaction with other members. The term "micro-blogs" focuses on a user who must publish their status within 140 characters of text, without images or other multimedia, making it much easier to convey a message than preparing a post for a classic blog. Micro-blogging platforms are very attractive to users who wish to express themselves often with anything they consider worthwhile to report. Through micro-blogs, one can send short messages with thoughts, activities, questions, or anything else that will be received by those who have chosen to "follow" them.

Social Networks

Social networks are considered (Boyd & Ellison, 2007) the appropriately configured platforms, set in the form of a web page for the end user, so that they enable the simple creation of profiles and interactions with other users through "social connections" within an electronic community, thus forming social structures. The connection of a user profile initiates some platform mechanisms such as updating the display of messages, photos etc. (Andrus, 2005). Theoretically, the possibilities of interaction are infinite and are defined by the nature of each social networking platform.

Social networks can be divided into two categories:

- Vertical social networks that involve members with shared interests and common goals.
- Horizontal social networks that consist of members with different interests, usually aiming to communicate, get to know each other and interact.

Wikis

Wikis (Richardson, 2006) are websites with content configured by users, in contrast to ordinary web pages, which can be modified only by their owner-administrator. The previous version is still available, no matter if a user modifies something on the wiki page, its Wikis are a means of collaborative work on a subject. They enable community members to contribute equally to the production of a collaborative project posted on a website. Every user who participates sets their personal knowledge at the disposal of the public. Wikis, even within organizations or services, facilitate informing employees of what is happening in business and can even act as progress reference pages.

RSS (Really Simple Syndication)

RSS is an XML content-based sharing template that was an innovative way of accessing content on the internet. It has been a digital technology that allowed internet users to become subscribers of a central website (RSS reader) through which they could receive news and updates from other websites of their choice (Sikos, 2011). Therefore, RSS technology was essentially about creating hyperlinks from the main website to other websites (RSS feeds), while allowed interactive communication between different Web 2.0 applications. In order to be able to get information about the new content of websites in which users were interested, they should have

either a news aggregator or a news reader. By selecting an RSS Feed for a specific issue of interest, they can be constantly updated on their favorite blogs or websites through the digital reader they have chosen, without checking the websites that they are interested in constantly. An important advantage of RSS technologies is that recipients of the distributed content can only be those users who have chosen to receive updates from these specific websites. RSS Feeds also increase the readability and accessibility of a website as it is an easy way to search for information on the internet. They are also good feeders for search engines as long as they keep up to date with new Web content, allow their users to forward their content to friends, relatives, or colleagues and favor the creation of links to other websites.

Mash-ups

The term refers to combining and using data and applications from different websites in one. The mash-ups are implemented through "open" application programming interfaces and aim to improve the websites' functionality.

Tagging

Tagging is a method of categorizing information on the internet. Any content, such as a new blog post, may accept multiple categorizations making it appear in several categories (Getting, 2007). This essentially leads to a new way of Web browsing that differs from the classic linear mode of Web 1.0. Tagging is ubiquitous on websites with user generated content. Users increasingly use tagging for content search, storage and exchange of information. In general, tagging moves on two main axes (Smith, 2008):

- In the storage and classification of content created by the user.
- In searches of content created by other users.

Users categorize the content topics of a website or a blog, giving them a meaning (a word or a phrase). This information is then categorized based on this meaning. Tagging works with bottom-up logic, with users categorizing the content with keywords, which then are used as search keys in internet search engines. In essence, tags are free expression tags that are freely chosen by users and not according to a default vocabulary.

Tagging creates value for users because it allows them to create online content for categorizing important information using their own words or meanings. The words that users use to categorize a webpage and its content are an easy and short way that other users can use to search for content or information on the Internet.

The tagging process is not only used for registration and content classification, but also for the circulation and exchange of this content on the internet. The websites that provide users with tagging capabilities also allow them to share with other users the personal classifications they create as well as personal Internet search methods.

Also, many of the websites use RSS technologies to notify their interested users of changes and developments that are happening. In addition, some websites, usually social networking sites, provide users with other functions, such as information retrieval, commentary, and API technologies (Application Program Interfaces) that allow for interoperability with various blogs or other websites. Although the tagging process is a simple technique, essentially a way of categorizing information, it also has a strong social dimension as website users find common ground interests and create online communities with each other.

Podcasting

The term refers to a method of creating audio files available in the network so that the supporting software recognizes new files and downloads them automatically (Richardson, 2006). No portable player is required to play podcasts. Every new podcast is referred to as an "episode," while many episodes together have the form

of a series and are referred to as a "channel." Podcasts are usually automatically downloaded to mobile audio players or personal computers and provide feeds with updates of new publications.

In addition to the above types of Web 2.0 applications, many lesser-known ones have also claimed and received their share of the participatory Internet, laying their role and affecting how it works and is used today.

3.2.3 Web 2.0 Technologies

The following is a summary of the most important technologies that implement Web 2.0 and its applications (O'Reilly, 2005; MacManus & Porter, 2005):

- Rich and interactive user interfaces (Rich Internet Applications-RIA) that incorporate technologies such as Flash, JavaScript and Ajax, which represent the trend of Web 2.0 for sharing Internet resources. When uploading a webpage, only data that changes is updated while the user is there or returns to it.
- Use of CSS (Cascading Style Sheets) to separate the information data from the formatting data on a webpage. That, beyond from economy to network resources (bandwidth), offers flexibility in the way data is presented as the user sees the data depending on the CSS they have: the same data depending on the CSS can be displayed on a computer screen, directly to a printer, to a mobile device with limited graphic display capacities etc.
- Use of RSS feeds or other related technology with the abovementioned advantages.
- Simple and lightweight REST network protocols (Representational state transfer) and SOAP (Simple Object Access Protocol) that use simple HTTP commands to retrieve data from servers (servers??), reducing the latency of telecommunication systems.
- Use of semantic data and microformats to describe data contained in the websites. This way, data are categorized and their search becomes easier and more efficient.
- Use of open-source software such as Linux, Apache Web server, MySQL as database, and PHP, Pearl, Python as programming languages.
- SOA (Service Oriented Architecture) architectures that allow sharing and reusing services and applications from different software programs as well as SaaS (Software as a Service), where applications are installed on a central network server so that users can access them through a browser, regardless of location and access time.

3.2.4 The Impact of Web 2.0

In the age of Web 1.0, Internet users gained access to Web data and applications that allowed them to communicate. Web 2.0, as an evolution of Web 1.0, brought users into the spotlight and shaped the new context of the Internet according to their demand for better, more accessible, and more effective communication while also contributing to the modification of services and functions based on how they wished to use the Internet from that point on. Tim O'Reilly (2006) once said that Web 2.0 was one economic revolution in the computer industry motivated by the need to use the Internet as a complete working platform and to understand the necessary rules that need to be applied for a widely accepted platform. The goal he had set from the beginning of this journey was to build applications that would utilize the network in order to evolve dynamically during their use. When programs and devices were connected to the Internet, applications would no longer be simple implementations but dynamic services.

The emerging situation had some beneficial consequences for the users, the main ones of which are listed below (MacManus & Porter, 2005; Hinchcliffe, 2007):

1. **Upgrade communication between users:** Applications have been created that have enabled direct communication by text, voice and image at minimal cost, making it easier and more massive. In

blogs, for instance, everyone could post thoughts and opinions, with all internet users as potential recipients. At the same time, those interested in them could always contact their creator through comments in the blog structure itself. The spread of social networking sites has already made them the dominant way of communicating and socializing with younger populations and beyond.

2. **Creating collaborative environments, opportunities for contribution and democratization:** With wikis, blogs and forums, users exchange views, collaborate and contribute to achieving a common purpose regardless of geographical location, social and racial features. During this process, they are forming online communities dealing with issues of common interest. The abolition of traditional barriers and the two-way communication between users, organizations, and businesses, gave from the early stages a sense of a social revolution. Through Web 2.0 applications, users' opinions are published, and depending on how much they converge, they acquire such importance that companies, organizations as well as political actors are forced to consider them (Gotved, 2002).
3. **Uncontrolled objective information:** Users can be better informed by taking advantage of news, information and views published outside conventional communication channels and posted by Internet users through blogs, wikis, and forums. The publication on news blogs or related multimedia content of their production and the public debate that can take place there through commentary offers a perspective of objective information control. This way the online community offers knowledge and experience, while users trust it more and more. It is knowledge of scientific, practical, and social issues, freely available. Many websites can perform an important social role and replace traditional forms of social care.
4. **Adaptation of applications to the user's needs:** "Light" technology has been applied in terms of protocols (REST) and open-source applications, which many times evolved based on the needs and the user's contribution. Also, in the programming and functional applications' design, simplicity (e.g. PHP language instead of C++ or Java, applications based on Ajax technology) and configurability of webpages was the norm, according to the users' preferences, while, as already reported, search for information through tagging was made easier. All this offered the users a better, more direct and more meaningful internet experience. A significant consequence was also the replacement of many traditional applications, such as open code operating systems and office suites e.g. Linux, Android, Gmail, and Google Docs, yielding significant cost benefits.
5. **Disclosure of creativity and opportunities for promotion:** Applications were developed, which, combined with the increased bandwidth that telecommunications providers globally, offered and the available storage facilities, technologically enabled the users to disclose their skills via multimedia content. This way they could allow access to their content to a broad audience highlighting some of their talents.
6. **Citizen service**: Handling citizens' cases by services or organizations via the internet and the potentiality of registering citizens' data in a common data form (e.g. with mash ups technology) is benefitting them since the daily public service transactions are facilitated.
7. **Improving the position of users/consumers in commercial transactions:** Users can choose products from a global market, find out more information about them from other users' comments and compare prices. This process upgrades the position of users/consumers towards companies (Sigala, 2008), which are now forced to treat them more responsibly.

3.2.5 The Risk of Web 2.0

From the above, it is indisputable that the technological innovations introduced by Web 2.0 significantly impacted upgrading the role and life of citizens in modern society. However, these possibilities come with some objective difficulties and problems that must be resolved, in order to achieve the most efficient use of these technologies. Regarding Web 2.0 applications, users' personal information should be safeguarded and

made clear as to who will use it and why. In order to ensure the highest level of security for Web 2.0 applications, an appropriate legal framework must exist. As blogs or microblogging services can be a steppingstone for complaints and grievances due to a dissatisfaction of entries or comments, this may lead to a deviation from a meaningful social dialogue and a fruitful exchange of views. Initially, an administrator can of supervise information, citizens' behavior, content or at least the comments made. However, given the tremendous rise of popularity in Web 2.0 applications and the vast amount of information all over the Internet, it is practically impossible to coordinate the public debate, turn it into fruitful dialogue and prevent malicious use of the new media. Ultimately it is up to the discretion of each reader to cross-reference the information published and evaluate its validity by developing through accumulated online experience the appropriate criteria for this purpose. Gradually, automated techniques have been embodied in platforms to control malicious behavior while tools have been developed and set to the users' disposal providing more security shields.

An important issue here is "electronic exclusion," which refers to the benefits of new technologies that cannot reach all citizens, but only those with access to them. The issue is referred to as the "Digital Divide" and refers to social and economic inequalities that prevent a large part of the global population from having equal access to new services. Different global organizations are working together to address the problem of the digital divide, and there are ongoing efforts worldwide to reduce this gap. This will be discussed further in the following section.

3.3 Social Media

In the late 1990s, as broadband internet became more popular, websites that allowed users to create and upload content began to appear. The first social networking site is the "SixDegrees.com" and appeared in 1997. From 2002 onward, many social media sites were launched. Some enjoyed a surge of popularity, such as Friendster. Others developed niche communities, such as MySpace, which appealed to teenage music fans.

By the late 2000s, social media had gained widespread acceptance and some services gained huge numbers of users. In November 2012, Facebook announced 1 billion users worldwide, while X (known as Twitter up until the 24th July 2023) had an estimated 517 million users in July 2012.

Several factors have contributed to this rapid growth in social media participation. These include technological factors such as increased broadband availability, the improvement of software tools, and the development of more powerful computers and mobile devices. Critical social factors were responsible for the rapid uptake of social media by younger age groups. In contrast, an important economic factor was the increasing affordability of computers and software as well as the growing commercial interest in social media sites.

3.3.1 Definition

Social media refers to the wide range of Internet-based and mobile services that allow users to participate in online exchanges, contribute user-created content, or join online communities. The kinds of Internet services commonly associated with social media that stem precisely from the Web 2.0 principles, include most of the services described in the Web 2.0 paragraph and are the following:

- **Blogs.** As previously presented, their name is short for "weblog," and they are online journals the pages of which are usually displayed in reverse chronological order. Blogs can be hosted for free on websites like *WordPress*, *Tumblr* and *Blogger*.
- **Wikis.** A wiki is a collective website where participants can modify any page or create a new page using a Web browser. One well-known example is Wikipedia, a free online encyclopedia that uses wiki technology.

- **Social bookmarking.** Social bookmarking sites allow users to organize and share links to websites, some examples include *Reddit*, *StumbleUpon* and *Digg*.
- **Social networking sites.** These have been defined as web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. Facebook and LinkedIn are among the most widely used platforms. **Status-update services.** Also known as microblogging services, status-update services, such as X, allow people to share short updates about people or events and to see updates created by others.
- **Virtual world content.** These sites offer game-like virtual environments in which users interact. One representative example is the imaginary world constructed in *Second Life*, in which users create avatars (a virtual representation of the user) that interacted with others.
- **Media-sharing sites.** These sites allow users to post videos or photographs. Popular examples include *YouTube*, *Pinterest*, and *Instagram*.

These categories overlap to some degree. *X* (formerly known as *Twitter)*, for example, is a social networking site and a status-update service. Likewise, users of the social networking site *Facebook* can share photographs, and users of the media-sharing site *Pinterest* can follow others.

The emergence of the concept of social media can be traced back to the time that Tim O'Reilly introduced the term "Web 2.0" in 2005 (Tim O'Reilly, 2005). While O'Reilly claimed that "Web 2.0" denotes the changes described above, it is the collective intelligence of users that co-created the value of platforms such as Google, Amazon, Wikipedia or Facebook, in a "community of connected users." The term was created mainly to identify the need for new economic strategies for internet companies after the "*dot-com*" crisis, where the burst of financial bubbles caused their collapse. In a paper published five years after the introduction of the term "Web 2.0," Tim O'Reilly described the new age as "a new return of the Web after the fall of "the dot-com," and underlined the attempt "to restore confidence in an industry that lost its way after the dot-com crash."

Michael Mandiberg (2012) argues that the notion of " social media " is based on multiple concepts:

- the user-generated corporate media content,
- the convergence culture, oriented towards the media industry (Jenkins, 2006),
- the computer-oriented programming (Tim O'Reilly, 2005).

Social media's ideology lies on the idea of allowing many users to access the internet to share, collaborate and update web content. Users can engage, collaborate, and share with others in real time without time or geography constraints. O'Reilly referred to the new internet as a participation channel and a consumer-based environment with ubiquitous coverage.

Social connections are the source of social media. However, not every social media platform or application facilitates face-to-face interaction between users. For instance, Amazon is primarily an information tool rather than a communication tool because it primarily offers information about goods. On the other hand, Facebook has built-in communication features such as messages, comment walls and forums that are broadly used.

Therefore, an interpretation of the social theory behind "social media" can be analyzed in three dimensions corresponding to three social information processes: cognition, communication, and cooperation.

To understand the designation "social" for this type of media, the term "Socialization" should be comprehended. Socialization is a term utilized by sociologists, social analysts, anthropologists, political researchers, and educationalists to allude to the deeply rooted procedure of acquiring and spreading standards, traditions, qualities, and belief systems, furnishing a person with the abilities and propensities vital

for taking their very own interest inside society. Socialization "the methods by which social interaction and social congruity are attained" (Huges & Kroehler, 2007; Macionis & Gerber, 2010). Therefore, this type of media allows for the deployment of all these human inherited virtues in a virtual world, which the social media users themselves construct.

3.3.2 Social Media versus Traditional Media

The etymology of the word “media” is a good starting point for this comparison. It comes from Latin, and it means “middle layer.” Therefore, the function of media, according to its classical definition, is to mediate between two layers, between an individual and the world (Pariser, 2011). Mainstream media’s role is to inform the public about what is happening worldwide. However, social media eliminates the intermediaries. Thanks to this disintermediation, people are no longer obliged to consume the source of information that is offered. They can choose from unlimited sources or create contents to offer to others as well. There is no need for the mediating role of broadcasts or newspapers. Nonetheless, in his book *The Filter Bubble: What the Internet is Hiding from You*, Eli Pariser argues that in reality intermediators are not eliminated on social media, but are just different and more difficult to notice (Pariser, 2011).

With attributes that can affect how people interact online, social media open new ways for collaboration and discussion. One of these is persistence, meaning that a great deal of content posted on social media sites may remain there permanently by default. Other characteristics are replicability, indicating that content can be copied and shared, and searchability, pointing out that content can be found easily using online search tools. The characteristic of accessibility is also important: social media can be used anywhere, at any time, where an internet connection is available. These attributes shape the dynamics of social interaction online. For example, the “invisibility” of the reader raises questions about the context, appropriateness and even the comprehensibility of a communication. Moreover, just as it is difficult to know who might be reading content posted on a social media site, the identity, and motives of those who post content are not always clear.

All in all, users can find social media news on demand choosing the most valuable source that fits their needs and beliefs. Media elites or authoritarian regimes usually control traditional media, and they have been supporting one-way communication for transmitting content to an audience that can only receive it passively for years. The consequences of that state of information delivery have already been known for years, as it is equally known that there were no feedback capabilities. In the social media world, the flow of information is not dominated anymore by advanced information societies, and dramatic changes in journalism have been introduced. Any point or opinion will find a way of broadcasting and reach an audience that has preferred to view it, away from censoring or biasing processes. This can have positive results but the chances for fake information remains in the foreground. All in all, social media offers great opportunities for accessing vast amounts of information; however, they require a highly critical attitude against the validity of news and its sources.

Regarding the intermediation issue of the usual media, social media has imposed another reality that has to do with new personalization. Unlike on broadcast media, people can receive personalized contents on the internet. At first, this served as a huge advantage, easing the work of consumers, who do not have to spend time on browsing anymore, as the internet offers them exactly what they need. Google CEO Eric Schmidt believed that what customers want from Google is to “tell them what they should be doing next” (Pariser, 2011), arguing that this personalization technique offers better service quality. Over time, personalizing algorithms have been developed, providing companies with better services and significant incomes. For instance, Amazon earns billions of dollars in merchandise by predicting what consumers are interested in the most and putting it in the front of the virtual store. Netflix’s income comes up to 60% from the personalized

guesses it can make concerning consumers' movie preferences. At the time of writing the book, Pariser (2011) stated that Netflix had the capability to accurately forecast a customer's preference for a movie with a precision of half a star.

Tailored media content can create filter bubbles, where people only see news and information that aligns with their preferences. This can reinforce their beliefs and is a risky phenomenon, especially since social media is now the main source of news for younger people. For instance, teenagers consider social media as a verification tool, if Facebook or any other platform they are using confirms their beliefs, they accept it as the truth (Niclewicz, 2017).

While broadcast media offers a wider, mainly universal overview of the world and what is happening in it, social media, due to personalization, puts a strong emphasis on the consumers' interests creating an individualized reality with news that corresponds to the reader's political, cultural, or social preferences, while maintaining the illusion of it being objective. This deception of social media by personalized content can be the root of multiple other problems.

From another perspective, although social media offers a variety of beneficial features, it can lead to fragmentation and polarization. Broadcast media has somehow united people in the sense that it offers information about the most relevant issues of society. When individuals watch the evening news, they feel a sense of unease due to the repetitive global events, which contributes to a shared understanding of common situations. However, these individuals have not actively chosen to seek out this information, as its dissemination is controlled by external organizations. Meanwhile, personalized content demolishes this feeling of solidarity and distances people from each other by making them focus on one particular problem mirroring their individual beliefs, reducing the number of shared experiences. The Echo chambers filter out all the information that somebody may not be interested in or does not fit into their worldview. The gap is enlarging, which makes communication between people with completely different mindsets more and more complex, sometimes even impossible. Although asynchronous and costless communication channels are provided, it depends on the user if opinion diversity will flourish or not. Users may end up living in their filter bubble where very little, or no information can enter from outside, hearing their echoes on at a higher volume.

Additionally, there is a shift from reason-centered to emotion-centered discussions, principles and arguments. The former is represented by mainstream media, the latter by social media (Niclewicz, 2017). There is an inclination to be objective and detached in mainstream media while sometimes totally delusive. On the other hand, on the internet, where everyone can upload content because there is no formal style and writing rules regarding the topics, the essence or the rhetoric of the texts, emotions become dominant. Moreover, combining polarization and appealing to emotions can lead to extensive radicalization. Being moderate is not really in fashion on the internet these days. This explains why extreme parties are more prevalent on online platforms.

The differences between these two media types can be huge and so can be the implications to society. Although many years have elapsed since they were first introduced, the consequences are still under investigation, a difficult task, given that the processes are dynamic, and these media types continuously develop. Traditional media continues to exist, but some of their attributes tend to be altered due to the convergence of modes that constantly blur the borders between them and the social media.

3.3.3 Social Media and Civil Society

Due to their nature, social media have unavoidably been connected with societal processes and Politics. Citizens use social media to communicate, influence decision-makers, and hold parliaments and governments accountable. In the United Kingdom, *They Work for You*, a UK Citizens Online Democracy affiliate, helps users keep up to date with parliamentary committees, votes, speeches, and proceedings. This site combines its

content with that of the *Hansard Society,* and encourages users to make their contribution to improving the information provided, both quantitatively and qualitatively.

In the past, in Canada, sites such as *www.TweetCommons.com* and *www.politwitter.ca* allowed users to track the Twitter accounts of Canadian politicians in one place. These sites also evaluated their activity on Twitter and rank political topics according to the frequency with which Twitter users comment on them. Moreover, like *They Work for You*, they partially relied on users' contributions to compile relevant information in one centralized and user-friendly place.

In addition to facilitating public monitoring of political actors and institutions, social media is used to raise awareness of specific causes and to gain support. For example, in 2007, a Facebook group led by Michael Geist, a professor of Law at the University of Ottawa, spoke out against *Bill C-61* (An Act to amend the Copyright Act) during the second session of the 39th Parliament. This Facebook group reached more than 90,000 members. Professor Geist was convinced that the online campaign contributed to the government's decision to hold public consultations on copyright law in 2009.

Social media is used to inform the public about the work and values of parliaments to build public confidence and interest in parliamentary governance. The UK Parliament uses social media extensively to engage the public. It currently has a YouTube channel, a Flickr account, an X account, a FriendFeed account and a Facebook page, all of which feature frequent news about MPs and the activities of parliamentary committees and Houses of Parliament.

In addition, the Parliament Labs blog chronicles the evolution of the UK Parliament website and its use of social media. Finally, members of the House of Lords keep a blog called *Lords of the Blog*. Administered by the *Hansard Society*, the blog aims to inform the public about the House of Lords' work and to raise interest in it.

Parliaments also use social media to engage citizens in public policy debates. For example, the UK Parliament is currently experimenting with online consultations that allow people to answer specific questions on a subject for consideration by a particular committee. Participants can view and respond to other participants' remarks, allowing for discussions among citizens, as well as between citizens and their representatives.

Similarly, governments have adopted social media as a tool to inform and engage the public. In Canada, several federal departments and agencies have opened X accounts and created Facebook pages to improve service delivery and disseminate information to the public. For example, Health Canada is now using X to announce product recalls. Human Resources and Skills Development Canada also uses it to inform the public, particularly immigrants, about Canadian employment opportunities and requirements.

Governments also use social media to solicit input from citizens in the workplace, establish a framework for policy development, and encourage public debate on policy issues. The US government's website, *Regulations.gov*, allows individuals to comment on regulations under study in more than 300 public bodies. In this case, users can also respond to comments from other participants. On the other hand, in Canada, the government's recent public consultation on copyright law reform shows how social media can facilitate an exchange of views between citizens and decision-makers on issues related to copyright law and public policies. In this case, internet users were invited to participate in online forums and web-based public meetings, as well as to comment on other participants' contributions of on the consultation website.

3.3.4 Some Social Media Sites: Facebook, X, and LinkedIn

In the following chapters, the most popular social media sites will be presented and analyzed through the lens of the topic outlined each time. At this point, an introduction can be made for three of them: Facebook, X, and LinkedIn.

3.3.4.1 Facebook

Facebook, originally *the Facebook,* is a social media platform created on the initiative of four Harvard University students: Mark Zuckerberg, Andrew McCollum, Dustin Moskovitz and Chris Hugues. The aim of *the Facebook* was to connect all Harvard students through an online community.

Nowadays, Facebook is the leading social media platform, spread and used worldwide, with more than 2.2 billion monthly users. In 2003, M. Zuckerberg developed a program named *FaceMash* to hack Harvard's informatic system to get personal photos of the students. This program was the base of a bigger project for Zuckerberg: to connect all Harvard students, with individual profiles, where they could download pictures, send messages to fellowships, and share events.

On February 4, 2004, an online platform known as *thefacebook.com* was available and spread on Harvard's campus. Its success was huge; thus, *the Facebook* became open to other universities in the US, like Yale and Columbia, to spread its popularity.

However, a few days later, the Winckleross brothers, two fellows of Zuckerberg, accused him of plagiarism; they argued that he had stolen from them the idea of *the Facebook*. Indeed, they had approached Zuckerberg and asked him to help them create an online social network for Harvard under the name *Harvard Connection*. But Zuckerberg denied the accusation. A lawsuit was filed, and in 2008 Zuckerberg was obliged to give the Winckleross brothers a settlement that included 1.2 million company shares to each.

By 2006, Facebook was up and running and everyone could create an account on the platform. After registering to use the service, users can create a user profile, add other users as friends, exchange messages, post status updates and photos, share videos, and receive notifications when other users update their profiles, comment on posts, or click the like button regarding a post. Additionally, users may join common interest groups organized by school or college, workplace or other criteria, and categorize their friends into lists according to specific criteria.

In March 2006, Facebook's value was reported to be around $2 billion. In December, it increased to $8 billion. In October 2007, Microsoft invested in it, giving a valuation of $15 billion. Nowadays, Facebook is well-known as one of the GAFA; the four Biggest Tech companies in the world (Google, Amazon, Facebook, Apple).

However, Facebook and Zuckerberg have been involved in several controversial scandals where the personal data of millions of users have been set at the disposal of companies for economic as well as political reasons, violating privacy policies and intellectual property rights.

3.3.4.2 X

X is a free microblogging service founded in 2006 by Jack Dorsey, Evan Williams, Noah Glass and Biz Stone, and its original name was Twitter (it was renamed on the 24th July 2023 due to the change in ownership). The platform's main characteristic is the famous 140-character bursts of information called a tweet. Users can include links to other content, images, short videos and vines in their tweets, and public or private broadcasts. Celebrities, journalists, politicians, and other public figures use X to comment or make statements. Media outlets use X to broadcast breaking news.

Since its founding, X has evolved into a social media juggernaut, and its popularity is often used as a benchmark of influence. Technology Author Steven Johnson described X (at the time known as Twitter) as

"remarkably simple" (Johnson, 2009): "As a social network, Twitter revolves around the principle of followers. When you choose to follow another twitter user, that user's tweets appear in reverse chronological order on your main Twitter page. If you follow 20 people, you will see a mix of tweets scrolling down the page; breakfast-cereal updates, interesting news links, music recommendations, even musings on the future education."

Tweets are, by default publicly visible, senders can restrict message delivery to their followers. Users can tweet via various compatible external applications apart from the X website, and Short Message Service (SMS) available in certain countries.

One of the most discussed issues for wittier users is the 140-character message. This limit has substantially altered how users compose their posts. They must make their point as tersely as possible. This limit can sometimes alter the meaning of the point itself or lead to a more well-defined message. At the same time, it gives X the exact form of service that its founders wanted to offer to social media; small bursts of information.

A word, phrase, or topic that is tagged in tweets at a greater rate than others is called a "trending topic." Trending topics can result from an event that prompts people to talk intensively, a topic of common interest throughout the user interface, or the result of a concerted effort by users. This segment of X helps users find out what is happening around the world.

X demonstrated how fast news spreads in the social media realm. They are being commented on and argued by users ranging from power-positioned people to simple citizens around the world. Having such topics openly discussed in a huge international think tank is obviously a huge benefit of the digital age. Simultaneously, though, it is terrifying once someone realizes the impact of social media on public opinion. It must be underlined that sometimes a message could be composed incorrectly or misconceived, as well as the fact that media manipulation is a very frequent reality, intentionally or not.

3.3.4.3 LinkedIn

LinkedIn is an American business and employment-oriented online service that operates via websites and mobile apps. Launched on May 5, 2003, the platform is primarily used for professional networking and career development and allows job seekers to post their CVs and employers to post jobs. The company was founded in December 2002 by Reid Hoffman and the founding team members of Socialnet.com and PayPal.

At the beginning of 2014, the website had almost 259 million members from 170 different sector activities from 200 countries and territories. LinkedIn is mainly used for professional networking and is available in twenty languages. According to a *Quantcast* report, the website had booked more than 178.4 million visitors monthly in July 2013, increasing them to 184 million in October 2013 and surpassing MySpace.

The company's headquarters are in California, US, but there are offices in Omaha, Chicago, New York, London, Dublin, Singapore, Hong Kong, China, Japan, Dubai, India and Australia. With more than 300 million members in 2014, it is significantly ahead of its competitors, Viadeo and Xing, with 50 million and 10 million members, respectively.

The main idea of this website network is to allow users, typically workers and employers, to create their profiles, including résumés, and get in contact with them. This virtual professional contact called "connection," represents real world professional relationship. When somebody is a member, they can invite anyone to connect with them. The platform posts job listings and other business opportunities. Job seekers can review hiring managers' profiles and discover which of their existing contacts can introduce them.

Professionals can write articles of studies on websites which can be classified by topic and writer. This allows for future conferences or booking upcoming. It has become a new way to communicate, convey

knowledge and share tips and experiences for a job. LinkedIn supports group formations, with more than 1.3 million groups available on the platform.

According to a study published in Times magazine, the countries with the most LinkedIn users are: the United States with 93 million, India with 24 million and Brazil with 16 million. France has only seven million and more than 79% of the business staff in Greece are members. The capitalization was more than 20 times the turnover, with 20 billion dollars in 2013. Moreover, the turnover increased by 50% between 2012 and 2013 with 1.52 billion dollars; and the net income amounted to 22.77 million dollars, was a 25% increase in one year. The main source of income is the recruitment service (49%), followed by advertising (30%) and subscription to premium accounts (21%).

What made it so successful in such a short period is the smart way it interlinks the job market's needs. Additionally, LinkedIn's founders reasoned that if they could attract entrepreneurs to their site, then they would also attract those seeking job opportunities and with them, recruiters. To achieve that, they figured out they would have to recruit venture capitalists, as most entrepreneurs are searching for capital. To lure the venture capitalists, they created a tool that would give them what they needed: a way to check the references, the professional experience and network of their potential new investments. This tool was also useful to the recruiters and with these tools on board, everything else followed. Eventually, giving the right benefits to job seekers and employers was the base for a social media website that changed how recruiting works.

3.4 Social Networking Sites and Social Network Analysis (SNA)

As pointed out in the definition of social media websites, Social Networking (SM) sites are a category of social media that offers individuals a platform to construct a public or semi-public profile within a bounded system, to articulate a list of other users with whom they share a connection, and to view and traverse their list of connections and those made by others within this system. The presented categories overlap to some degree with others and therefore, social networking is an attribute that may be evident in several social media platforms. However, it must be clear that social networking is a specific feature and not a synonym of the term social media itself.

Since their introduction, social networking sites (SNSs) such as MySpace, Facebook, Cyworld, and Bebo have attracted millions of users, many of whom have integrated these sites into their daily practices. As of this writing, hundreds of SNSs, with various technological affordances, supporting a wide range of interests and practices. While their key technological features are consistent, the cultures that emerge around SNSs vary. Most sites support maintaining of pre-existing social networks, but others help strangers connect based on shared interests, political views, or activities.

What makes social networking sites unique is not that they allow individuals to meet strangers but instead that they enable users to articulate and make their social networks visible. This can result in connections between individuals that would not otherwise be made. On most sites, the list of friends is visible to anyone permitted to view the profile. The label for the relationships differs depending on the site. Popular terms include *Friends*, *Contacts*, *Fans*, *Followers* etc.

Social Networks are nothing new. They have been present for as long as humans form societies and socialize, and they have introduced the term "Social Capital." Although they have always been subject to scientific investigations through the lens of social scientists, the deployment of Social Networking Sites (SNS) brought them to the foreground. The digitization of social networks provides a favorable setting for modern scientific research, allowing for the use of established methods like Social Network Theory and various techniques such as multidimensional statistics, data mining, content analysis, and social media scraping. In fact, the relevant literature indicates that by combining methods like these researchers can produce better investigation results.

Scientifically speaking, a social network is a social structure comprising a set of social actors (such as individuals or organizations) and a set of dyadic ties between these actors. The actors are referred to as nodes, vertices, or points. The relations are referred to as edges, arcs, lines or ties. Consequently, the nodes in the network represent its actors, which could be people, groups, or organizations while the connecting links show relations or "flows" between the nodes.

Social network theory allows for studying relationships between individuals, groups, organizations, or even entire societies. The ties through which any given social unit connects represent the relationship and the convergence of the various social contacts of that unit. According to one of its axioms, social phenomena can be primarily conceived and investigated through relations between and within units instead of the properties of these units themselves.

By applying the principles of social networking theory, an analysis of the network's linkage behavior can be implemented to determine important nodes, communities, existing or even future links and evolving regions of the network. Such analysis provides a good overview of the global evolution behavior of any underlying network. More specifically, three main areas of interest can be outlined:

- **Community Detection:** To find structurally related groups in the Network
- **Influence Analysis:** An analysis of the dynamics of interactions. Determining the most influential members of the social network by using flow models or page rank style methods
- **Link Inference:** Finding inferring links that are not yet known in the social network. It is known as the Link Prediction procedure where future linkages are determined.

Presenting details and methodologies of the Social Networking Analysis is outside the scope of this book. However, it can be proved useful to view some involved notions in order to have a feeling of how these scientific methods can provide research results in this field, such as finding influencing entities (influencers) in a social network. For this purpose, the means of centrality will be presented below.

There are several ways to measure centrality in a social network: "how central" a node or a whole network is. For example, Degree *Centrality* is the number of direct connections a node has. What really matters is where those connections lead. From this perspective, the actor with the most ties is the most important (**Figure 3.1**).

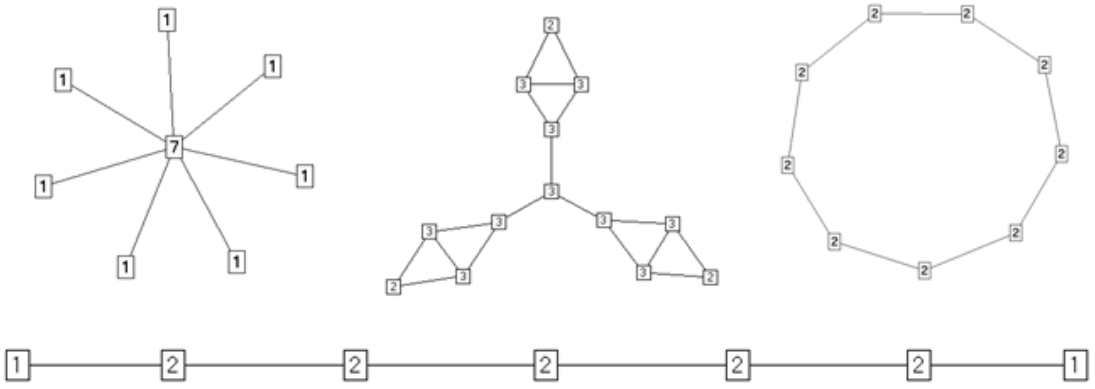


Figure 3.1 *Degree centrality in four simple social networks (Hanneman & Riddle, 2005).*

From another perspective, *Betweenness Centrality* can be defined as follows: a node with high betweenness stands between most of the pairs of the rest of the nodes. Therefore, it can exert control of the information flowing in the network, and it has great influence among its peers (**Figure 3.2**). Centralization can generally be measured using mathematical formulas and the indicated value in **Figure 3.2** should only be observed as an absolute value.

Another approach might be the one of Closeness Centrality. In this case, the measure of closeness of a node expresses how close it is to everyone else. From this perspective, an actor is considered important if they are relatively close to all other actors (**Figure 3.3**). Generally, these measures provide analysts with various of available approaches to social networking topics, and it is up to the issue under investigation which one may provide better results. For instance, actors that appear very different when seen individually may be comparable in a global network through the lens of centrality. In **Figure 3.4**, the two circled nodes have different numbers of individual connections. However, if the betweenness centrality is the issue, then they are the same, as indicated by the node size in the network graph.

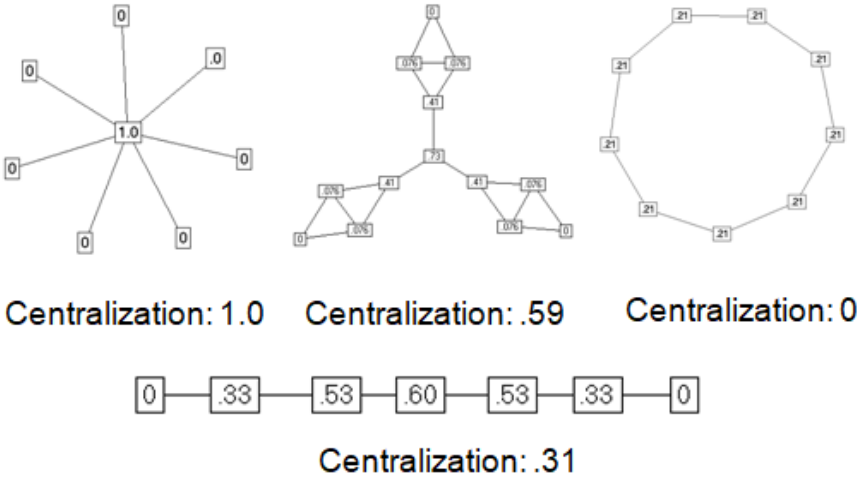


Figure 3.2 *Betweenness centrality in four simple social networks (Hanneman & Riddle, 2005).*

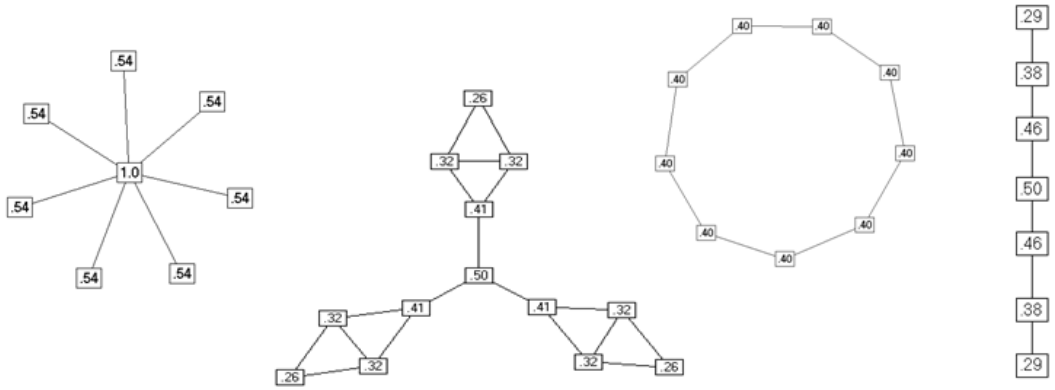


Figure 3.3 *Closeness centrality in four simple social networks (Hanneman & Riddle, 2005).*

These three definitions offer a simplified example of what calculations can be made and what information can be extracted over digitally implemented social networks, such as social networking sites. Notions like betweenness are exploited to provide, for example, the resulting list of sites by a search engine or to find influencers on X if the diffusion of campaigning information is what matters. The horizons of such investigations opened because digitally implemented social networks are implemented using data (e.g., adjacency matrices), which can be directly available for mathematical research.

On top of that, social networking sites are extremely rich in content, and they typically contain a tremendous amount of content and linkage data, which can be leveraged for analysis. Comments, likes, retweets, and so on, can be the input data for various research methods. The linkage data is data related to social network structure like the notions described above. The content data may contain text, images, and

other multimedia data in the network. The richness of this kind of network data provides unprecedented opportunities for data analytics in the context of social networking sites. Indeed, social networking sites such as Flickr, Message Networks, or YouTube contain a tremendous amount of content that can be leveraged to improve the quality of the analysis. For instance, a photograph sharing site, such as Flickr, contains a tremendous amount of text and image information in the form of user tags and images. Similarly, blog networks, email networks and message boards contain text content that are linked to one another. It has been observed that combining content-based analysis with linkage-based analysis provides more effective results in a wide variety of applications.

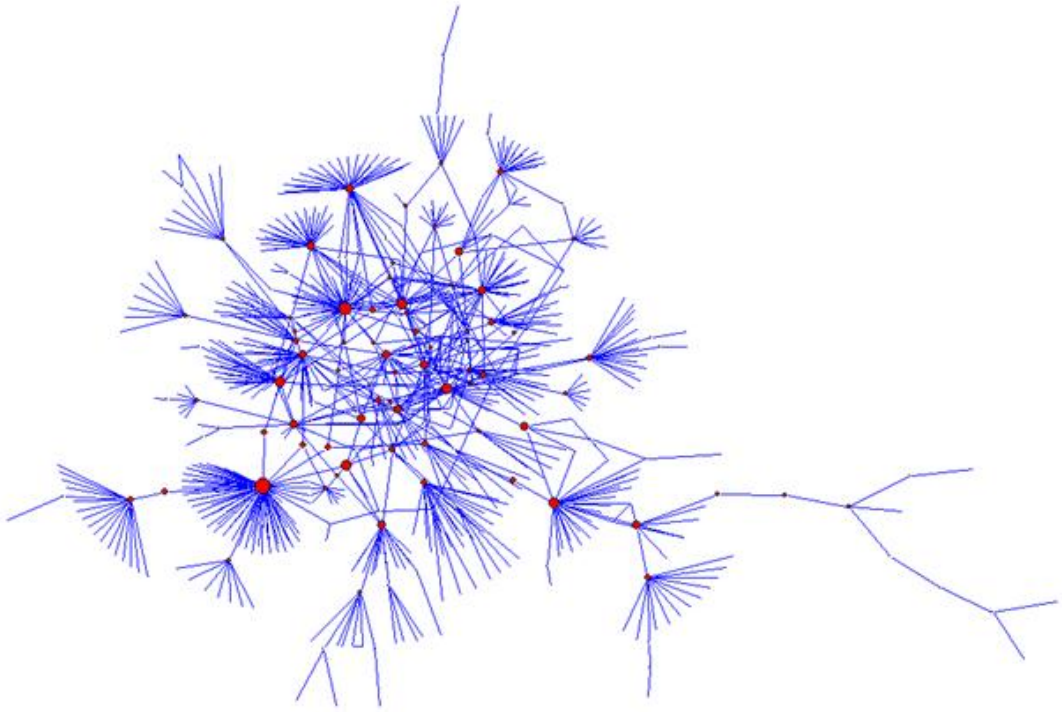


Figure 3.4 *Node size proportional to betweenness centrality.*

Figure 3.5 shows the social network of the Greek political blogosphere, the most popular blog in 2011 whose topic of interest was Greek politics. Since each blog can recommend other blogs by posting hyperlinks towards them in its blogroll, the resulting interconnection scene can be treated like a social network, whose nodes are the blogs themselves, with the ties being the hyperlinks. By applying a multidimensional analysis using clustering methods of statistics, SNA over linkage data, and Content Analysis over the post of each blog, Vagianos and Zafeiropoulos found in a study (2021) that the blogs formed 3 clusters with similar behavior (**Figure 3.5**).

By applying the SNA techniques mentioned above, the following questions can be answered over a social network: who the Connecter or Hub in a Network is, who has control over what flows in it, who has the best visibility of what is happening in the network, who are peripheral players and if they are considered to be important. The issues that can be resolved can be:

- **Bottlenecks identification:** central nodes that provide the only connection between different parts of the network,
- **Number of links:** for example, insufficient or excessive links between departments that must coordinate effectively,
- **Degrees of separation,** e.g. compared with connecting all pairs of nodes in the group,

- **Short distances:** these transmit information accurately and in a timely way, while long distances transmit slowly and can distort the information,
- **Isolation:** People that are not well-integrated into a group and, therefore, represent both untapped skills and a high likelihood of turnover,
- **Organizational subgroups or cliques:** groups that can develop their own subcultures and negative attitudes toward other groups.

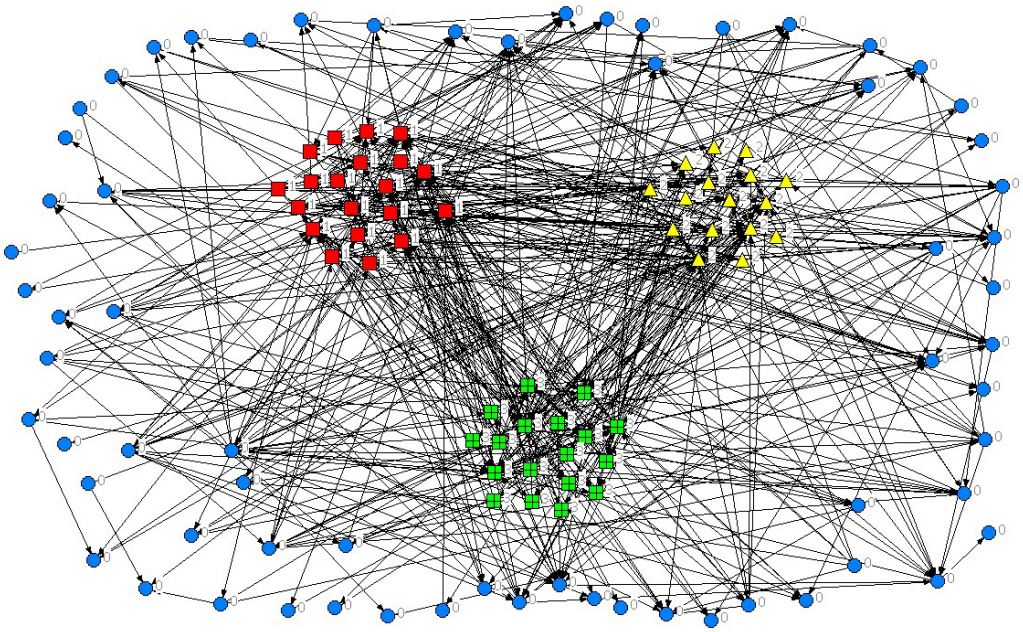


Figure 3.5 *Clustering in the social network of the most popular Greek political blogs in 2011 (Vagianos & Zafeiropoulos, 2021).*

Delving further, the ensuing areas of investigation within Social Networks, as manifested by Social Networking Sites, hold significant importance:

- **Statistical Analysis:** The connectivity behavior of the nodes is examined to see if most nodes have few connections, with several "hubs" or whether the degrees are more evenly distributed (Clustering behavior),
- **Random Walks:** To estimate the probability of visiting each node. This probability is estimated as the page rank. Nodes that are structurally well connected have a higher page rank and are also, naturally, of greater importance,
- **Node classification:** To model the changing structure of the network and identify the laws that govern long term changes,
- **Expert discovery:** To identify experts or teams of Experts that can perform particular tasks,
- **Link Prediction:** To determine or predict the future links of the social networks,
- **Privacy:** Privacy mechanisms in Social Networks,
- **Visualizing:** A natural way to summarize the information of the network,
- **Data Mining:** Data mining techniques provide researchers and practitioners the tools needed to analyze large, complex, and frequently changing social media data,
- **Text Mining:** Retrieving information from embedded text (e.g. comments on Facebook or blogs,

- **Integrating Sensors:** Sensor data (such as geolocation data) as an integral part of social network data analytics,
- **Multimedia Information Network Analysis:** Retrieving information from shared media SNs (tags, comments etc.),
- **Social Tagging:** Exploiting properties of tag streams, tagging models, tag semantics, generating recommendations using tags, visualizations of tags, applications of tags, integration of different tagging systems, and problems associated with tagging usage.

For many, network analysis is the keyword of the 21st century. Researchers, politicians and people generally talk about surrounding networks.

As pointed out earlier, *Social Influence Analysis* is a very popular task in today's social networking sites' context. Since social networks are primarily designed based on the interactions between the different participants, it is natural that such interactions may lead to the different factors influencing one another regarding their behavior. This knowledge can be extremely important in various fields, such as electoral campaigning or social media marketing. Equally important is the issue of *Community Detection*. This is closely related to clustering, and it attempts to determine regions of the network that are dense in terms of the linkage behavior. These can be envisaged as the virtual communities of Web 2.0, which will be the topic of the next paragraph.

At this point, the differences between social media and social networking sites should have become clear. In summary, social media is disseminated through social interaction based on user participation and user-generated content. They shift how people discover, share, and read news and information. Social Networking Sites support social networking, focusing on building social relationships among people and thereby building online communities while offering interactive communication among participants.

3.5 Virtual or Online Communities

3.5.1 Definitions and Attributes

Aggarwal (2011) states, "A social network is defined as a network of interactions or relationships, where the nodes consist of actors, and the edges consist of the relationships or interactions between these actors." In other words, a social network is a network of individuals, such as friends, acquaintances, or co-workers, that develop and maintain interpersonal relationships using an online service.

The term "virtual community" or "online community" may have several definitions that go back to the '90s, in the Age of Web 1.0. Rheingold (1993) mentions that "people in virtual communities use words as screens to exchange pleasantries and argue, engage in intellectual discourse, conduct commerce, exchange knowledge, share emotional support, make plans, brainstorm, gossip, feud, fall in love, find friends and lose them, play games, flirt, create a little high art, and much idle talk." He called them "virtual communities." From the beginning, users recognized that technology allows for reciprocal interactions between software and humans. This gave rise to a social entity, one that nowadays is more commonly known as an online community. Others like Wellman and Gulia (1999) defined online communities as "digital networks in which users feel an intrinsic connection toward other members."

Sproull (2004) defined online communities as "large, voluntary collectivities, whose primary goal was membership or social welfare, whose members share a common interest, experience, or conviction, and who interact with one another primarily over the net."

Online communities may be of different types. Some of them are tightly bound, dense groups of individuals that are familiar with one another. These individuals use the digital environment to augment their

existing social relationships (Wellman & Gulia, 1999). There is also another type of online community, including sparsely connected groups of individuals who do not know one another well and have little to no chance of ever meeting them in person.

A few years later, Bagozzi and Dholakia (2002) published their research on their investigation regarding the individual's intention to participate in an online community. They have discovered a few common characteristics that most online communities share. They are listed below:

Shared interest

According to them, most online communities are organized around a specific distinct interest. This common distinct interest may have to do something with a particular product or subject, such as Apple products or cooking, or an affliction, such as Parkinson's disease or amyotrophic lateral sclerosis, otherwise known as ALS, or a demographic characteristic (i.e. single people that like golf and are over fifty).

Consciousness of kin

Similarly, with offline communities, virtual community members feel a "consciousness of kin." That means these people feel connected towards other members and have a collective sense of separation from non-members (Wellman & Gulia, 1999). This feeling of connection helps them increase their willingness to share personal experiences and information with the rest of the group.

Shared set of conventions

Another common attribute that most online communities share is the fact that their members use a shared set of conventions and language, such as emoticons or acronyms; they establish boundaries within the group and follow a particular set of rules while interacting with others, which is also known as "*netiquette.*" Because of the above, virtual communities tend to provide their members with many of the same benefits that one can enjoy when he or she is a part of an offline community.

Active participation

It has also been noticed that although in many offline communities, the content is consumed passively by their members, in online communities, content is generated by their members through active participation. As Werry (1999) put it a few years ago, this content creation is as an important shaping force of the community's character.

Collective expertise

Almost every online community archives the past content by default and without passing any cost to its members. Because of that, these communities represent an aggregation of collective expertise on these topics in a way that is difficult to match elsewhere. In other words, they create a capital of knowledge, increasing the community's value for all members (Werry, 1999).

Freedom of expression

Regarding internal communication, most of the communities in the past were text-based (e.g. chat rooms, e-mails lists), nonverbal expressions and social characteristics such as gender, age, ethnicity and professional status, were being filtered out (Kiesler & Sproull, 1992). These characteristics were intentionally missing, camouflaged, or even falsified. In those days, this allowed individuals to express themselves more freely without worrying about how they looked or talked, as all they cared was the way they expressed themselves via plain text.

Despite the above attributes that most online communities share, there is one essential difference with their offline counterparts. For everyone, membership and participation in an online community is driven "by

volitional choice." Being a virtual community member has no time or place restrictions and individuals can connect with peers, no matter where they live or where they come from.

3.5.2 Types of Virtual Communities

As Internet penetration was logically too low during the first few years of its existence, the very first online communities were usually associated with the business-to-business world. These existed in many sectors, including education, science, banking, healthcare, and technology. Something similar had happened with the telephone. When it was introduced, people believed it was fit only for business-to-business communication. Using telephones for personal communication became feasible later (Fischer, 1992).

With the arrival of specific virtual spaces, strangers found a place to meet and talk. These spaces were commonly known as "chat rooms" and "forums." People were able to talk to each other in real time about their topics of interest, from sports and politics to music and movies. These spaces provided a valuable medium for users to share their experiences, solve problems, meet peers at conferences, debate on various subjects, explore new career opportunities and keep up with the latest news. They could use applications like IRC (Internet Relay Chat) or Usenet, chatrooms, or simple email to establish a virtual place where their communication could be deployed.

Nowadays, the most common online communities include or are included in online networking websites (e.g. Facebook, X and LinkedIn), forums and blog platforms (e.g. Wordpress, Blogger), video game platforms (e.g. Steam, Twitch) and virtual worlds (e.g. Second Life). Times have changed, and because of that, people may create and join online communities for a much wider variety of reasons.

First, a motivation to do so is the fact that people want to engage in discussions regarding religious or political beliefs, favorite teams, technologies, brands or hobbies. This kind of community is better known as "fandom" (consisting of "fan" plus the suffix "-dom," as in kingdom). Sometimes, these fandom communities shape the phenomena around which they are organized, as Nancy K. Baym (2007) has pointed out. One such example is the Season 3 premiere of *Sherlock*, the British television crime drama. *The Guardian* once mentioned that this episode's plot was crucially responsive to fan reaction.

In many cases, people want to connect with others to keep up with upcoming events or the local community. Social media provides a variety of tools to enable connection to peers at almost zero cost, in a way that was not possible before.

Businesses can also create online communities to communicate messages to potential customers. This last part has become increasingly common since the arrival of Facebook, with the introduction of Fan Pages. Even before Facebook, some brands hosted certain websites that accommodated online communities. *Heineken*, for example, allowed individuals to establish their virtual bars, chatting with strangers and meeting their friends. Palmer (1996) argues that consumers have an underlying need to form an emotional bond with the products they buy.

There are also communities of transaction, which primarily facilitate buying and selling products and services and delivering information related to those transactions (like *eBay*). From a marketing perspective, some communities offer member-customers reduced search costs, access to a broad range of information regarding offers and better services (like *skroutz.gr*).

Online communities can also be created for education purposes, as most university departments have an online presence in the social networking universe. Students join these communities to discuss upcoming classes and assignments and share news related to their studies.

Health care is also one of the most popular subjects for online communities. Individuals join these groups to gather information, offer advice and provide psychological support to those who need it, either due to a disease or becoming a parent etc.

People may join and participate in an online community for many reasons: to receive useful information, to make connections, to amuse themselves, to enhance their reputations, and many others. However, one of the reasons seems to be the most popular. Raacke and Bonds-Raacke (2008) have found that most college students who use certain social networking websites, such as MySpace and Facebook, dedicate a significant chunk of their day to these platforms for making new friends or getting in touch with old acquaintances. However, this can be true even for older people, as Ridings and Gefen (2004) point out. Social support and friendships are the main reasons for participating in such an online community. Through these communities, one can communicate with connections, both those they personally know offline and those they only know virtually.

As stated before, membership and participation in online communities are driven by volitional choice and may be terminated by the individual without much effort (Bagozzi & Dholakia, 2002). In the Web 1.0 age, one could just quit a chat room or stop logging-in to a forum, and this can also hold in the present, where one can effortlessly leave a Facebook Group or stop logging-in Second Life.

An interesting difference between Web 1.0 and Web 2.0 virtual communities is the shift from anonymity to self-publication. In the virtual communities of Web 1.0, the norm was to participate under the cover of a nickname. The digital identity was generally tailored through text writing styles and discursive activity. Anonymous communications and the "anonymity of the screen" constituted a primary site of early investigations into Computer Mediated Communication (CMC) and still goes on. However, in shifting to the Web 2.0 age and the formation of communities on social networking sites, the focus is not on anonymity but on self-publication. In this new virtual world, participants have the opportunity, and nowadays, this is the norm, to publish not only themselves using multimedia data but also their whole network of connections, which is part of their online identity.

3.5.3 Virtual Communities Members' Roles and Relationships

Although online communities differ from their offline counterparts in some ways, members' roles are often quite similar. As Angeletou et al. (2011) have pointed out, the roles in an online community are the following: moderators-mediators, celebrities, elitists, lurkers, and trolls-flamers.

Users who contribute frequently, push for discussion, and focus on supporting the community are characterized as moderators-mediators. When those users manage to be influential, and being able to set the standards for community interactions, they are characterized as celebrities among their peers. A smaller chunk of users tends to communicate information with a smaller user group, but at the same time they demonstrate high values. They are called elitists. Moreover, the role most frequently observed is that of lurkers. These members do not contribute much and instead absorb the information that others share within the community. They are like passersby; they look, but they do not contribute to the community. Finally, there are the trolls-flamers, who demonstrate high intensity and persistence, but their primary goals are to raise discussion on a topic of their interest and disrupt the community's peace.

Critics of online communities support that online relationships can never be meaningful because they separate people from physical contact, and therefore, they become isolated. Some online communities focus on very particular topics. As a result, relationships in these cases can be narrow, existing only for information exchange and processing. This, of course, is a positive attribute when efficiency and fast results are what counts. Such examples are *Quora* and *Stack Overflow*. Nevertheless, the nature of these platforms supports narrow relationships, as people tend to post questions and search for answers as soon as possible. Walther

(1995) has argued that the web does not prevent more meaningful relationships from happening. It just simply slows the process. Communication via the web is usually asynchronous and thus slower. It has been found that in online communities implemented through social networking sites, many participants seek ways of integrating their offline experiences. The rise of SNSs indicates a shift in the organization of online communities, which are primarily organized around people, not interests, as in the case of Web 1.0. Early public online communities such as Usenet and public discussion forums were structured by topics or according to topical hierarchies, but social networking sites are structured as personal (or "egocentric") networks, with the individual at the center of their community and the connections (relationships) being in the foreground.

3.5.4 Concerns

Communities on social networking sites are many times considered "miniatures" of our society. Therefore, some societal problems may exist, with the two most common being privacy and harassment.

It has been frequently observed that privacy mechanisms provided by such websites are often weak. This happens for several reasons, including permissive default settings, poor interface design, and social conformance. In most SNSs, it is the users' responsibility to decide how to set their privacy settings. When Strater and Lipford (2008) examined the results of their study, they found that for many people, the decisions regarding privacy disclosure were made in haste and early in profile creation. In most cases, users never went back to change these settings. The only things that made them review the privacy options were disturbing events, such as a privacy intrusion by receiving messages or calls from a stranger.

Moreover, the Internet is generally filled with trolls and flamers, people that aim to intervene in an online community harmfully. The same principle applies to social networking websites too. Trolls make posts that are designed to provoke other members or situations. Their primary motivation is the sense of power and recognition that such actions give them.

Usually, trolls tend to hide their real identity. By staying anonymous, they can make any posts or comments they want and, at the same time, avoid any repercussions. Thus, some people decide to use their real names and addresses, taking pride in that behavior. Sometimes, their harassment may result in personal conflicts that, if escalated, can derail the community, taking attention from its core mission. In some cases, it has been reported that some people may feel annoyed enough to leave the community.

There are times when members of an online community join forces against a common threat. Sometimes that "common enemy" may be another individual or a certain entity, like a company. Such is the example of *Systemgraph* vs. X, a conflict in the Greek sphere of X a few years back. The company had sued a disgruntled customer for defamation, as he resorted to his blog to complain about his experience with the company. *Systemgraph* was asking for up to €200.000 as compensation. Because of its choice, X users from all over the country joined forces and took the customer's side, bringing up pro-free speech arguments and declaring that they would never buy any products from that company ever again. This example shows that members of an online community may act collaboratively, deriving this attitude from sharing common ideas and beliefs among their peers.

3.6 Participatory Culture

Participatory Culture is a newly introduced term that describes the users' attitude in the Web 2.0 World and their behavior when using its applications. A participatory culture is one in which members believe their contributions matter and feel some social connection with one another. As expected, the participatory culture features are strongly related to the Web 2.0 principles prevailing in social media and social networking sites.

Driven by technology, forms of participatory culture are manifested in communication, collaboration, circulation of ideas, contribution, and collective knowledge. With a view to Virtual Communities, the main axes of this culture are the following:

- Relatively low barriers to artistic expression and civic engagement.
- Strong support for creating and sharing creations with others.
- Some informal mentorship whereby what is known by the most experienced is passed to novices.
- Members who believe that their contributions matter.
- Members who feel some degree of social connection with one another (at the least, they care what other people think about what they have created).

According to Jenkins (2006), conveying this culture means only some members must contribute. However, all must believe that they are free to contribute and that what they contribute will be appropriately valued.

As Interactivity is a property of technology and Participation is a property of culture, participatory culture is emerging as it absorbs and responds to the explosion of new media technologies that make it possible for average consumers to archive, annotate, appropriate, and recirculate media content in powerful new ways.

Eventually, in the Web 2.0 world, many will only dabble, some will dig deeper, and still others will master the skills that are most valued within the community. The community itself provides solid incentives for creative expression and active participation. Participatory culture is reworking the rules by which communities and individuals operate using shifting the focus of literacy from individual expression to community involvement.

3.7 Conclusion

The internet revolutionized modern forms of communication, uncovering new horizons through the quick delivery of messages, accessibility, and the interactivity among other significant improvements. Web 2.0 has altered the landscape by moving Internet users to the center of the scene by giving them the tools to be content creators as well as the judges of content of their peers. This brilliant idea of Tim O'Reily revitalized the Internet as a platform and raised questions about whether the new landscape resembles the Public Sphere, as it Jurgen Habermas has captured it. Technology and social circumstances enabled Internet users to quickly adopt the new style of living in the digital realm by forming digital social networks using of social media and social networking sites. They created profiles to augment their offline subsistence, tailored digital identities, and formed communities serving various needs.

As expected, this new world provides opportunities and upgrades several sectors of everyday life but also introduces a range of risks. The multidimensional aspects of this new reality will be the subject of all the following chapters of this book.

The challenge that the new digital media landscape introduces at all levels at the dawn of a new era of participatory culture is how humans should develop themselves, living in a world consisting of networks and belonging to virtual communities, to evolve into effective participants and ethical communicators.

References

Aggarwal C., 2011. *An introduction to social network data analytics*. Springer US, 2011.

Andrus D. C., 2005. "The Wiki and the blog: towards a complex adaptive intelligence community." *Studies in Intelligence*, 49.

Angeletou S., Rowe M., and Harith A. 2011. "Modelling and analysis of user behaviour in online communities." *The Semantic Web*–ISWC 2011: pp. 35-50.

Bagozzi R. P., and Dholakia U. M., 2002. "Intentional social action in virtual communities." *Journal of interactive marketing*, 16.2: pp. 2-21.

Baym N.K., 2007. "The new shape of online community: The example of Swedish independent music fandom." *First Monday* 12.8.

Best D., 2006. "Web 2.0 Next Big Thing or Next Big Internet Bubble?", Lecture Web Information Systems. Technische Universiteit Eindhoven.

Bonds-Raacke J., and Raacke J., 2010. "MySpace and Facebook: Identifying dimensions of uses and gratifications for friend networking sites." Individual Differences Research 8.1: pp. 27-33.

Boyd D. M., and Ellison N.B., 2007. "Social Network Sites: Definition, History and Scholarship." *Journal of Computer-Mediated Communication*, 13 (1), article 11.

Brown J., Broderick A. J., and Lee N., 2007. "Word of mouth communication within online communities: Conceptualizing the online social network." *Journal of interactive marketing*, 21.3: pp. 2-20.

Bruggerman J. (2008). *Social Networks: An Introduction*. Routledge, 1st edition.

Chan C.M.L., Mamata B., OH L.B., and CHAN H.C., (2004). "Recognition and Participation in a Virtual Community." Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.

Delwiche A., and Henderson J. J., (2012). "The Participatory Cultures handbook." Chapter 1, pp. 3-8, Routledge, 2013.

Dewing M. 2010. "Social Media: An Introduction," Publication No 2010-03-E, Library of Parliament, Ottawa, Canada, 3 February 2010.

Dongyoung S., 2008. "Social Network Structures and the Internet: Collective dynamics in virtual Communities." Cambria Press.

Faraj S., and Johnson S.L., 2011. "Network exchange patterns in online communities." *Organization Science,* 22.6: pp. 1464-1480.

Fernback J., 1999. "There is a There There: notes towards a definition of cybercommunity," in S. Jones (Ed.), *Doing Internet research*. Thousand Oaks, CA: Sage. pp. 203-205.

Fischer C.S., 1992. America calling: A social history of the telephone to 1940. University of California Press.

Getting B., 2007. "What Are 'Tags' And What Is 'Tagging'?", Available at: https://www.practicalecommerce.com/what-are-tags-and-what-is-tagging [Accessed 8 April 2017].

Gotved S., 2002. "Spatial Dimensions in Online Communities.' *Space and Culture*, Vol. 5 (4): pp. 405-14.

Graham P., 2005. "Web 2.0." Available at: http://www.paulgraham.com/web20.html

Greenmeier, L., and Gaudin S., 2007. "Amid The Rush To Web 2.0, Some Words Of Warning – Web 2.0 – InformationWeek." www.informationweek.com

Gupta S., and Kim H.W., (2004). "Virtual Community: Concepts, Implications and Future Research Directions." Proceedings of the 10th Americas Conference on Information Systems, New York, 2004.

Hanneman R.A., and Riddle M., 2005. "Introduction to social network methods." Riverside, CA: University of California, Available at: http://faculty.ucr.edu/~hanneman [Accessed 3 November 2013].

Hiltz S.R., and Turoff M., 1993. *The Network Nation.* The MIT Press, Revised Edition.

Hinchcliffe D., 2007. "The State of Web 2.0." Web Services.

Huges M., and Kroehler C., 2015. "Sociology - The Core." USA.: Kindle Edition (11th).

Jenkins H., Purushotma R., Weigel M., Clinton K., and Robison A. J., 2009. "Confronting the challenges of Participatory Culture." *Media Education in the 21st Century*, The MIT Press, Cambridge Massachusetts, 2013.

Jenkins H., 2006. *Convergence Culture*. New York University Press, New York.

Johnson S., 2009. "How Twitter Will Change the Way We Live." Depaul University.

Kiesler S., and Sproull L., 1992. "Group decision making and communication technology." *Organizational behavior and human decision processes* 52.1: pp. 96-123.

Kiesler S., Kraut R.E., Paul Resnick P., and Kittur A., 2012. "Regulating behavior in online communities." *Evidence-based social design: Mining the social sciences to build online communities,* pp. 125-178.

Kietzmann H., Jan D., and Hermkens K., 2011. "Social media? Get serious! Understanding the functional building blocks of social media." *Business Horizons* 54: pp. 241-251.

Leimeister J. M., Sidiras P., and Krcmar H., 2002. "Success Factors of virtual communities from the perspective of members and operators." *Proceedings of the 37th Hawaii International Conference on System Sciences*, 2004.

Macionis D., and Gerber B., 2010. "Sociology. Canada." 7th Canadian ed.

MacManus R., and Porter J., 2005. "Web 2.0 for Designers." Web 2.0 Design: Bootstrapping the Social Web. Available at: https://www.digital-web.com/articles/web_2_for_designers/ [Accessed 8 April 2017].

Mandiberg M., 2012. *The Social Media Reader*. New York University Press, New York.

McWilliam G., 2012. "Building stronger brands through online communities." Sloan Management.

Niklewicz K., 2017. "How the social media mechanisms push its users to populism." [online] Available at: https://www.academia.edu/35550681/populism-on-social-media-PUBLISHED.pdf [Accessed 5 January 2020].

O'Reilly T., 2005, "Design Patterns and Business Models for the Next Generation of Software." What Is Web 2.0, O'Reilly Media, Inc, Available at: http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1 [Accessed 8 April 2017].

O'Reilly T., 2005. "What is Web 2.0," published on O'Reilly's website (oreilly.com) in September 2005.

Palmer A. J., 1996. "Integrating brand development and relationship marketing." *Journal of retailing and consumer services* 3.4: pp. 251-257.

Pariser E., 2011. *The filter bubble: What the Internet is hiding from you*. New York: The Penguin Press.

Postmes T., Russell S., and Martin L., 2000. "The formation of group norms in computer‐mediated communication." *Human communication research* 26.3: pp. 341-371.

Rheingold H., 1993. *The virtual community: Homesteading on the electronic frontier*. MIT press, 1993.

Richardson W., 2006. *Blogs, Wikis, Podcasts, and Other Powerful Web Tools for Classrooms*. Corwin Press.

Ridings C.M., and Gefen D., 2004. "Virtual community attraction: Why people hang out online." *Journal of Computer‐Mediated Communication* 10.1.

Rodzvilla J., and Blood R., 2002. *We've Got Blog: How Weblogs Are Changing Our Culture*. Perseus Pub., 2002.

Shen K. N., and Khalifa M., 2013. “Effects of technical and Social design on virtual community identification: a comparison approach.” *Behavior and Information Technology*, 32:10, pp. 986-997, Taylor and Francis, 2013.

Sigala M., 2008. "Web 2.0 tools empowering consumer participation in New Product Development: findings and implications in the tourism industry." Annual International International Council for Hotel, Restaurant and Institutional Education, (I-CHRIE) Convention “Welcoming a new era to hospitality education.” Atlanta, Georgia, USA: 30 July – 2 August, 2008.

Sikos L.F., 2011. *Web Standards: Mastering HTML5, CSS3, and XML*. Apress Pub, 2011.

Smith G., 2008. *Tagging: People-Powered Metadata for the Social Web*. Berkeley, CA: New Riders.

Strater K., and Richter Lipford H., 2008. "Strategies and struggles with privacy in an online social networking community." *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, Volume 1, 1 Sep. 2008, pp. 111-119.

Toder-Alon A., Brunel F. F., and Schneier Siegal W. L., 2005. "Ritual behavior and community change: exploring the social-psychological roles of net rituals in the developmental processes of online consumption communities." *Online Consumer Psychology: Understanding and Influencing Consumer Behavior in the Virtual World* (2005), p. 7.

Vagianos D., and Zafiropoulos K., 2020. “An Effective Multidimensional Model for Analyzing Social Web Big Data – Testing in simple Web 2.0 Applications of Internet Politics.” Communications of the *IBIMA Journal*, IBIMA Publishing, USA, (ISSN: 1943-7765), Vol. 2021 (2021), Article ID: 589003, Available at: https://ibimapublishing.com/articles/CIBIMA/2021/589003

Walther J.B., 1995. "Relational aspects of computer-mediated communication: Experimental observations over time." *Organization Science* 6.2: pp. 186-203.

Ward H., 2000. *Principles of Internet marketing*. Cincinnati (OH) 7.

Wellman B., and Milena G., 1999. "Net surfers don't ride alone: Virtual communities as communities." *Networks in the global village*: pp. 331-366.

Werry C., 1999. "Imagined electronic community: Representations of virtual community in contemporary business discourse." *First Monday* 4.9.

Zeng F., Li H., and Wenyu D., 2009. "Social factors in user perceptions and responses to advertising in online social networking communities." *Journal of Interactive Advertising* 10.1: pp. 1-13.

Chapter 4 From Traditional Media to Networked Media

Abstract

In Chapter 4, a thorough description of the current networked state of Media is attempted. The features distinguishing Networked Media from classical Media are highlighted, emphasizing on their democratic and decentralized nature, where the audience can also be the contributors. The unavoidable involvement of computers as an input/output device and the resulting community formation is also highlighted, as the community members participate and consume the DM content. The benefits of this development of inter-networking have allowed for greater political and social comment and discussion. The cooperative/collaborative practice of Networked Media, in which many can contribute and interact with the production of DM content, is explained by presenting a case study of the largest Mass Communication medium of human history: YouTube.

4.1 Traditional Mass Media

Traditional media refers to the media that has been present for years. They include radio, broadcast television, cable and satellite, print, and billboards. Because they succeeded in reaching a large audience, the term "Mass Media" was introduced and has remained popular until today.

Until the end of the 20th century, a classification of mass media could lead to seven mass media industries as the following:

- **Print**: books, newspapers, magazines, etc. that started in the late 15th century.
- **Recordings**: vinyl records, magnetic tapes, cassettes, CDs, and DVDs that started in the late 19th century.
- **Cinema:** started in about 1900.
- **Radio:** started in about 1910.
- **Television:** started in about 1950.
- The **Internet:** started in about 1990.
- **Cell phones:** started in about 2000.

Each mass medium has content types, creative artists, technicians, and business models. The Internet includes blogs, podcasts, websites, and other technologies built atop the general distribution network. Due to digital technologies, the Internet and cell phones are often called digital media while radio and TV are called as broadcast media.

Print, Recordings, Cinema, Radio, and Television operated on a one-way communication channel delivering certain amounts of information to many receivers. The Internet and the very first cell phones also operated on the same basis, maintaining, in a way, these characteristics. On the one hand, the Internet and, more specifically, the World Wide Web (www) was initially a vast collection of Websites that only those with technical expertise, or those who could hire them, could create them, and thus diffuse them in a one-way mode to a global audience. On the other hand, cell phones, although two-way communication devices, still operated in one-way modes mainly because the short message service (SMS) could be exploited for massive transmission of messages to a given list of recipients for marketing or campaigning purposes.

Boundaries began to blur once technology enabled cell phones were used to access the Internet. The initial stages of this process exploited new technologies, such as WAP or GPRS, to deliver Internet packets over wireless signaling channels. The versions of the Web delivered to mobile users were filtered replicas of the original content that could be delivered to desktop terminals due to bandwidth and phone screen limitations. What caused a total reversal were two significant changes that were to have unpredictable impact: the Web 2.0 and the smartphones supported by wireless communication technologies such as 3G networks. The former changed the landscape in terms of content producers and interactivity. The latter manifested itself as the gateway to the former by engaging huge audiences perpetually connected to services on the move with an amazing collection of technologies, such as geolocation sensors and high-definition cameras. Broad access to the Internet has also been boosted with the advancements of Wi-Fi and Wi-Max technologies that massively supported the connection of smart devices to the Internet at a global level (**Figure 4.1**).

All in all, technological convergence was a reality under the Internet umbrella. This is referred to in literature as the "convergence of modes," which led to the new media system: the networked media.

4.2 Networked Media

The term "Networked Media" derives right from what was stated above. It refers to decentralized forms of mass communication via which individuals and groups can actively contribute to sharing and shaping a

universe of media content. According to *IGI Global*, it includes innovative ways for supporting people in their daily lives and initiating technology-enabled social change that strongly involves users for co-creating and emerges as a result. Networked media are "characterized by individual nodes or pages of content separated in time and space, in relationships that are not predicted by proximity or order."

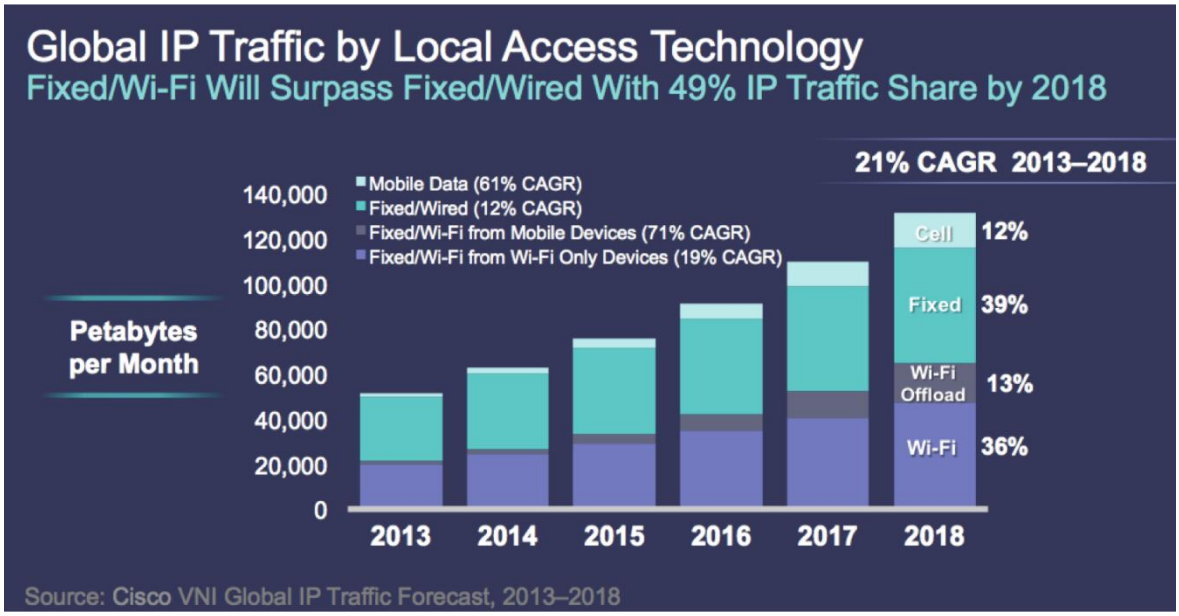


Figure 4.1 *Global IP Traffic by Local Access Technology (Source: https://blogs.cisco.com).*

Decentralized media play a crucial role in providing a better arena within which involved parties can have more control over their privacy and the ownership and dissemination of their information and content. Therefore, networked media will be more protective of censorship, monopoly, regulation, and other exercises of central authority. More crucially, a decentralized motive for the new type of media cuts the boundaries of the past by providing users more freedom to interact with each other and allowing them to project their views without fear.

Despite how it is often positioned, traditional and networked media do not have to go head-to-head. These mediums can be used together. The convergence of modes implies this hand-in-hand operation with technology being able for years to support this; telecommunication, computer and broadcasting networks converged based on digital networking, new data transmission and storage technologies, such as optic fiber, satellite communication and advanced software (Cowhey & Aronson, 2009).

It must also be noted that the convergence was not solely technological; Organizational convergence also took place in the first decade of the 21st century with new forms of local or global communications being introduced supported by computer networking, telecommunication infrastructure, digitization, and in many cases open-source software.

The following features distinguish networked media from classical media, such as broadcast media and the printed press:

- Networked media is typically **democratic** and **decentralized**. The audience can also be the contributors.
- Networked media often requires the **involvement of computers** as an input/output device.
- Networked media requires a **community** to **participate** and **consume**.

Networked media is about cooperative and collaborative practice in which many can contribute to producing "media." The benefits of the inter-networking development have allowed for greater political and social comment and discussion while it is also widely thought of in a much broader context of globalization.

As to have a clear idea of the new prevailing type of media, some distinguishing features are listed below (Shah, 2020):

- **Value**: New media is often far less expensive than traditional media, which requires a high entry cost.
- **Global Reach:** New media has a global reach, whereas traditional media tends to be highly regional. With new media, a global audience can be reached for a fraction of the cost.
- **Communication/Interaction:** New media tends to be much more interactive than traditional media. New forms of media, such as social media, allow for direct communication and interaction between all available combinations involving citizens, organizations, political parties, etc.
- **Cost Efficient:** New media is also more cost-efficient. Spending money on new media will likely yield a higher reach than spending the same amount on traditional media.
- **Mobility:** Due to the supporting wireless technologies, networked media follows users wherever they are.
- **Ease of Use:** Networked media requires some time to learn, especially for older generations. Graphical and user-friendly interfaces make it easier and easier for users to get involved in the processes.
- **Customization & Personalization:** Networked media can be easily customized according to the user's personal needs.
- **Choice of Audience and Targeting Capabilities:** Networked media can be highly targeted using Data Mining techniques and highly accurate algorithms. Networked media is excellent if you are trying to target specific individuals or demographics. The targeting capabilities go far beyond that of traditional media.
- **Trust:** Having a presence on social media allows businesses or other actors to establish a sense of trust with consumers or followers.
- **Amount of Usage:** People spend an ever-increasing amount of time engaging in networked media, with their cell phones, and less and less time watching TV or listening to the radio.
- **Accuracy:** An advantage of networked media is the accuracy of its results. Unlike TV ratings, new media allows for combing results that show how many people saw an ad and whether it led to a click-through. These results can be considered when evaluating a social media advertising strategy.
- **Data-Driven**: New media is highly data driven. All related information is kept and can be accessed according to the general outlining context: how many people visited a webpage, number of views or downloads, number of connections in a social networking site, number of likes in Facebook etc.
- **Level Playing Field**: Social media provide a level playing field for all involved parties. It does not take exorbitant amounts of money to grow a business or deploy an electoral or crowdfunding campaign using social media.
- **Real-Time Results:** Unlike traditional media, the results received from new media with monitoring techniques are often in real-time. That allows for applying instant changes to achieve maximum effectiveness. It also gives new media a leg up over traditional, where it often takes time to see the results of a campaign.

- **Virality**: Truly effective networked media has the potential to go viral. Content can be potentially shared with millions of people.
- **Marketing:** Traditional media is a form of outbound marketing where businesses send their message to consumers. New media is a form of inbound marketing, where businesses interact with individuals who seek them out. Inbound marketing tends to provide more willing consumers than outbound marketing.

Conclusively, networked media supported by the Internet and its explosive penetration in the first decade of the 21st century (**Figure 4.2**) brought the rise of new forms of societal communication supported by computer networks of globally distributed and interactive senders and receivers. According to Manuel Castells (2009), "the communicating and information processing power of the Internet is now distributed via the wired and wireless communication paths to all contexts of social life. Therefore, everybody and everything finds a way of existence in this multimodal interactive communication context."

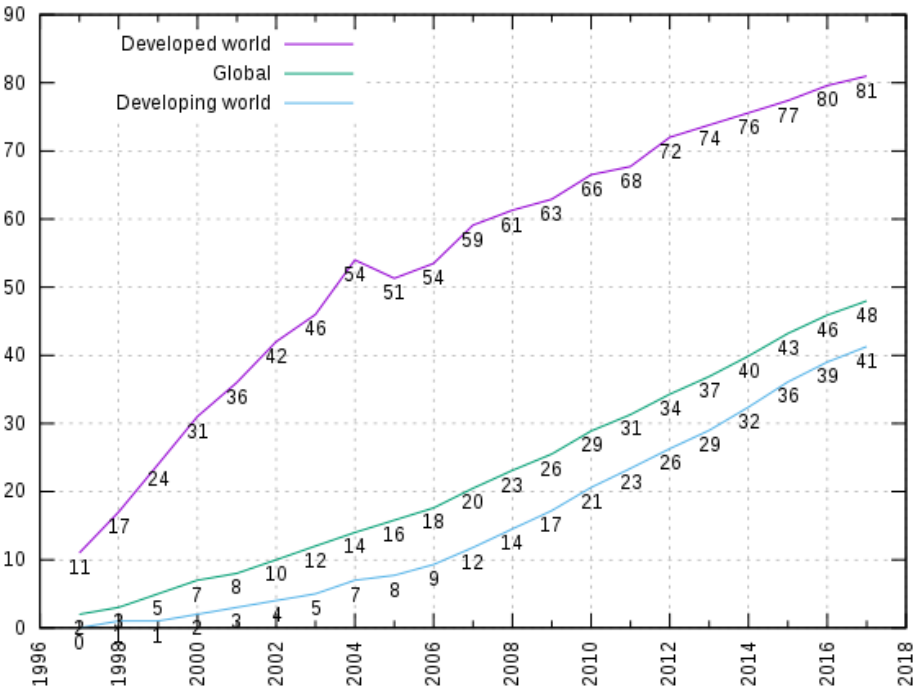


Figure 4.2 *Internet users per 100 inhabitants globally (Source: Wikimedia Commons).*

4.3 A Networked Media Case Study: YouTube

Fifteen years after its foundation and having been localized in more than 85 countries, YouTube remains a unique phenomenon and a fine representative of networked media regarding its popularity increase and business model features. Based on Web 2.0 principles, YouTube's model is a leading example of the so-called Mass Collaboration Economy, an economy model based on the Web 2.0 principles, that achieves that by turning media shared content into commodities and profit.

In an attempt to highlight the virtues of the networked media more thoroughly, an outline of the YouTube platform is presented here, composed of its history, its statistics and a financial overview that made this phenomenon the biggest Mass Medium in human history. Its diverse impact is addressed in many areas of human activity, including Culture, Social Relations, Politics and Economy, all at a global level. YouTube platform has been localized in Greece since 2012 and is the second most visited site according to Alexa, surpassing Facebook over the last few years (Vagianos & Messerschmidt, 2019).

4.3.1 History

YouTube was founded by Chad Hurley, Steve Chen, and Jawed Karim, who were all early employees of PayPal (Cloud, 2006). Prior to PayPal, Hurley studied design at the Indiana University of Pennsylvania. Chen and Karim studied computer science at the University of Illinois at Urbana-Champaign. YouTube's early headquarters were situated above a pizzeria and a Japanese restaurant in San Mateo, California (Alleyne, 2008).

The domain name "YouTube.com" was activated on February 14, 2005, and opened for uploads on April 23, 2005. The first YouTube video was titled *Me at the Zoo* and showed co-founder Jawed Karim at the San Diego Zoo. Like many technology start-ups, YouTube started as an angel-funded enterprise from a makeshift office in a garage.

In November 2005, venture firm Sequoia Capital invested an initial $3.5 million; additionally, Roelof Botha, a partner of the firm and former CFO of PayPal, joined the YouTube board of directors. In April 2006, Sequoia and Artis Capital Management invested an additional $8 million in the company, which experienced huge popular growth within its first few months. In June 2006, YouTube joined an advertising and marketing partnership with NBC. On October 9, 2006, Google bought YouTube for $1.65 billion. As YouTube wished to keep operating independently, both the co-founders and its 67 employees at that time continued working under Google. The deal was completed on November 13, making YouTube the second largest acquisition Google made. PC World Magazine named YouTube the ninth of the Top 10 Best Products of 2006.

4.3.2 Statistics

In July 2006, YouTube had more than 65,000 newly uploaded videos and 100 million views each day simultaneously. On Alexa, YouTube surpassed MySpace and became the fifth most popular website. According to Nielsen/NetRatings, YouTube averaged almost 20 million monthly visitors (around 56 percent male and 44 percent female, with the dominant age group being between 12 and 17).

According to Google, in 2010, over 85,000 videos were uploaded to YouTube daily. Statistics in 2017 pointed out about 576,000 hours were worth of video content every day (Russell, 2013). Users watch billions of hours of videos a day. Each month, 1.5 billion logged-in users visit the website and 400 hours of videos are uploaded, every minute. The average time spent on the domain is 40 minutes (Hamedy, 2017).

The localized versions of YouTube are available in 88 countries, and it is broadcast in 76 languages all around the world. It covers 95% of the Internet population. Currently, YouTube is blocked in China, Iran and North Korea. The number of videos uploaded to the website monthly is more than three times what the major US television networks have created in the last 60 years. YouTube reaches more 18–34 and 18–49-year-olds than any cable network in the US. This makes YouTube the internet’s largest video hosting website today.

4.3.3 Social and Political Impact

According to the above stated statistics, YouTube is now considered the largest Mass Communication Medium in Human History. CNN, Al Jazeera, Kenya’s NTV, France24, and other media outlets maintain their YouTube channels. The Queen of England chose YouTube to issue her 2007 Christmas broadcast, while Tony Blair, Ex-British Prime Minister, was the first World Leader with a YouTube Channel. According to Alexa, YouTube was ranked as the second most popular site globally (Fortson, 2015). This has severe political implications as many authoritarian or totalitarian governments face the platform as an enemy and have thus decided to block YouTube Services. Examples include China, Iran, Turkey and North Korea (Cannell & Travis, 2018).

On the other hand, from a social and cultural perspective, YouTube has managed to change the sense of entertainment by embodying all the values of Web 2.0 Technologies, such as user generated content, interactivity, community building and on demand consumption. These, along with its simple but effective

business model explained in the next section, have brought up the thousands now existing "YouTubers," for most of whom YouTube offers a regular occupation where thousands of people are making a full time living off the site.

Densely linked with various industry components, such as the Music Industry, Cosmetics etc., YouTube has managed to turn things upside down by establishing new prevailing rules that now govern the business landscape.

4.3.4 Business Model and Collaboration Economy

The Internet's recent history is full of legendary business success stories where each case has unique characteristics and business plans. Their success is always a combination of a nicely tailored business plan with a coincidence of prevailing circumstances at the right time and place. No common business plan can apply to all cases, guaranteeing the success of every venture.

YouTube follows an advertisement-based business strategy. It provides free to access content to a very high user base, fully exploiting its highly gained success and popularity, which is the reason why YouTube does not require charging for its services to make money (Winkler, 2013). Therefore, the actual product that YouTube sells is its users.

The conditions that have allowed for YouTube's success are the ones brought by Web 2.0 technologies (Lacy, 2008). In their book *Wikinomics: How Mass Collaboration Changes Everything*, Don Tapscott and Anthony D. Williams explored how some companies in the early 21st century have used mass collaboration and open-source technology, such as wikis, to be successful (Tapscott & Williams, 2010). According to Tapscott, Wikinomics is based on four ideas: Openness, Peering, Sharing, and Acting Globally. Most of these values are found within the operation context of YouTube, making it an excellent example of the Economics of Mass Collaboration. Itis its Web 2.0 features that make this platform an attractive Gateway to a Mass Collaboration Economy, benefiting all involved parties: the platform as an enterprise, the advertisers, and its users, all interacting in a multiplexed arena where producers of the content are also its consumers.

In a simplified perspective, two rules seem to hide beside YouTube's success:

- Rule #1: "If you do not t pay for the product, YOU are the product".
- Rule #2: The 80/20 Principle (**Figure 4.3**).

Figure 4.3 *The 80/20 Pareto principle (Source: https://braining.gr).*

Rule #1 operates under Web 2.0 values: User generated content, community, and interactivity. It also describes a digital realm of relative Openness, Peering, and Global Sharing, constituting the Wikinomics realm.

Rule #2 originates in the writings of the legendary economist Vilfredo Pareto. In his book, *80/20 Principle: The Secret to Achieving More with Less*, Koch (1998) describes the unequal relationship between

inputs and outputs and states that 20% of the input variable produces an output of 80%. Under certain circumstances, this rule can be used to fine-tune a business model.

The 80/20 principle lies in the statistics of YouTube where only 30% of its uploaded videos result in almost 60% of their views. Combining this with the advertisement strategy, where the more videos you view, the more money YouTube makes, it is visible that the openness of YouTube allows enough space for viral videos, which will be the responsible ones for the maximum percentage of the desired outcome for all. The rules mentioned above operate in a Business Model which includes a variety of Services, such as:

- SERP advertising: sponsored videos where the advertiser pays YouTube based on the number of views it gets after such an ad has been clicked.
- Embedded Advertisements where YouTube earns money based on the number of views; a proportion of that fee is paid to the creator of the video.
- Landing Page Advertisements: the page that opens first without logging in. YouTube charges advertisers the most for a landing page advertisement.
- YouTube Red: an add free subscription service offered in 2016 at a monthly subscription rate of $10.
- YouTube TV: a great addition to YouTube's revenue model with over a billion users, offered at $35/month.
- Affiliate Earning: related products under some videos on YouTube.

Targeted advertising features are fully deployed in all these services by exploiting all available Big Data to identify the right audience for each ad.

Apart from these, YouTube has also launched partnership programs like Google *AdSense,* allowing content creators to be paid for their uploading content. Under *AdSense,* YouTube typically takes 45 percent of the advertising revenue for specific videos, while the rest goes to the creator (44:55 principle). Under this partnership, all YouTube users can use it as a regular occupation where the profit derives from the videos' virality (Rich, 2018). It is worth noting that the definition of "virality" dynamically evolved: a few years ago, a video could be considered "viral" if it hit a million views, while now it should get more than 5 million views in a 3–7-day period. The readjustment of the term is another way to describe the growth rate of the domain.

The AdSense program produced fertile terrain for countless users who pursued producing viral videos and thus gaining fame and money overnight. Since viral videos are attracting attention of advertisers, YouTube has launched a Rewarding policy giving a silver play button for channel creators of 100,000 subscribers, a 24-karat gold play button for gaining 1 million subscribers and a Diamond play button for those having 10 million subscribers.

4.4 Conclusion

Due to the maturity of society itself, escorted by advancements in technology, the transition from traditional media to networked media was unavoidable. Due to the convergence of modes, this transition was smooth enough as these two can co-exist and cooperate without confrontation. However, the change in the media landscape was unprecedented. Scholars indicate the revolutionary implications in various fields, from the democratic and decentralized nature of the new media to the new attitude of all the parties involved in the exchange of content. The global nature of the Internet provided fertile ground for the spread of new media services, like YouTube, which in a few years surpassed media giants that had been there for decades. Success stories exist and will keep emerging but only the future will show if humanity exploits the new features towards beneficial outcomes.

References

Alleyne R., 2008. "YouTube: Overnight success has sparked a backlash." *The Daily Telegraph*, 2017.

Burgess J., and Green J., 2009. *YOUTUBE*. Digital Media and Society Series, Polity Press, 2009.

Cannell S., and Travis B., 2018. *YouTube Secrets: The Ultimate Guide to Growing Your Following and Making Money as a Video Influencer*. Lioncrest Publishing, 2018.

Castells M., 2009. *Communication Power* (Ch. 2). Oxford University Press.

Cloud J., 2006. "The YouTube Gurus." *Time* 2006.

Cowhey P., and Aronson J., 2009. "Transforming Global Information and Communication Markets: The Political Economy of Innovation." DOI: https://doi.org/10.7551/mitpress/9780262012850.001.0001

Fortson K., 2015. "Youtube's Impact On Our Society, The Mycenaean, Leesville Road High School Newspaper." (retrieved from http://themycenaean.org/2015/11/youtubes-impact-on-our-society/) Hamedy S., 2017."People now spend 1 billion hours watching YouTube every day." *Mashable*, 2017.

Hiller R. S., and Kim Jin-Hyuk K., 2014. "Online Music, Sales Displacement, and Internet Search: Evidence from YouTube." *6th Annual Conference on Internet Search and Innovation* (Conference proceedings), Chicago IL, 2014.

Koch R., 1998. *The 80/20 Principle: The Secret to Achieving More with Less*. Doubleday, 1998.

Lacy S., 2008. *The Stories of Facebook, YouTube and MySpace: The People, the Hype and the Deals Behind the Giants of Web 2.0*. Richmond: Crimson. (ISBN 9781-85458-453-3), 2008.

Lister M., Dovey J., Giddings S., Grant I., and Kelly K., 2009. *New media: a critical introduction*. Routledge.

Pierce D., 2015. "YouTube Is the Sleeping Giant of Livestreaming." *Wired*, 2017.

RBB Economics, 2017. "Value of YouTube to the music industry." Paper I, *Cannibalisation*, 2017.

Rich J.R., 2018. *Ultimate Guide to YouTube for Business*. (2nd Edition), Inc. The Staff of Entrepreneur Media, 2018.

Russell J., 2013. "YouTube reveals users now upload more than 100 hours of video per minute, as the site turns eight." *The Next Web*, 2017.

Sarukkai R., 2010. "What's bigger than 1080p? 4K video comes to YouTube." *Official YouTube Blog*, 2017.

Shah M., 2020. "Traditional Media vs. New Media: Which is Beneficial." https://www.techfunnel.com/

Tapscott D., and Williams A., 2010, *Wikinomics: How Mass Collaboration Changes Everything*. Penguin Group (expanded edition), 2008.

Vagianos D., and Messerschmidt K., 2019. "YouTube: a Web 2.0 Collaboration Economy Gateway. Statistics and Impact." Published in *The UWB* (University without Borders) *Journal*, Volume 2, 2019 - No 1 (ISSN: 2585-2825).

Waldfogel J., 2017. "How Digitization has created a Golden Age of Music, Movies, Books, and Television." *Journal of Economic Perspectives*, Volume 31, Number 3, Summer 2017, pp. 195–214.

Winkler R., 2013. "YouTube Growing Faster Than Thought." *Wall Street Journal*, 2016.

Chapter 5 The Digital Divide

Abstract

In this chapter, the term "Digital Divide" is defined. Information is given about the economic and social inequalities between groups of people in each population regarding their access, use, or knowledge of information and communication technologies. It is highlighted that these inequalities can occur both within countries and between differing countries or regions worldwide. In the former case, the gap refers to inequalities between individuals, households, businesses, or geographic areas, usually at different socioeconomic levels or other demographic categories. In the latter case, it is known as the global Digital Divide, referring to the technological gap between developing and developed countries on internationally. Exceptional cases like the North-South or the gender divide are presented along with ways of measuring the Digital Divide by authorized bodies. Finally, it is stated why the Digital Divide should be bridged and the obstacles in the bridging procedure.

5.1 Introduction

A *DigitalDivide* is an economic and social inequality between groups in a given population regarding their access to, use of or knowledge of information and communication technologies. The term refers to inequalities between individuals, households, businesses, or geographic areas, usually at different socioeconomic levels or other demographic categories, within countries. Between differing countries or regions of the world, the Digital Divide is synonymous with the global Digital Divide, examining this technological gap between developing and developed countries on an international scale.

The Digital Divide has been primarily defined as a gap between those who have access to Information and Computer Technology (ICT) and those with no access to them. A differentiation should be made between accessing and using the internet (Norris & Conceicao, 2004). The term *Digital Divide* was first used by Larry Irving Jr., the former US Assistant Secretary of Commerce for Telecommunications and Communications during the 1990s. He aimed to shift the public focus towards the already existing gap in American society between those who could access ICTs and those who could not. This phenomenon was first observed in the American society. However, the *global Digital Divide* concept was captured in order to describe the differences between developed and less-developed countries (Acilar, 2011).

At first glance, social divides due to modern technology advancements can be traced back to the lack of physical access to the materialistic aspect of the problem, such as computer possession. Hardware accessibility is, however, part of the problem. It only represents one simplified dimension of this topic. Modern day's media social divide is much more complex than a shortage of computers in households.

With the growing importance of these kinds of technologies, the Digital Divide is also growing. In general, Information and Computer Technology include hardware, software, telecommunication technology as well as computers (Ogunsola & Okusaga, 2006). This growing importance of ICTs has also been recognized in the political realm because, since the 1990s, the Digital Divide has been considered a politically "hot-topic" (Selwyn, 2004). There are different subcategories of the Digital Divide, such as the gender divide, the age divide, and the income divide (Acilar, 2011). All these side aspects need to be carefully considered to have a clear view of the global Digital Divide.

According to the United Nations (UN) Development Program (2001) and the United Nations Development Program (1999), the factors that influence worldwide IT use include:

- **Income:** In Bangladesh, an average computer's price was equivalent to eight years' pay compared to the USA where the price was equivalent to only one month's salary.
- **Cost of connection:** Internet bills in Nepal constitute 278 percent of a month's salary compared to 1.2 percent of an American's salary.
- **Gender:** Women comprise only 7 percent of African users and 4 percent in the Arab States.
- **Age:** Most users in China and America were under thirty.
- **Language:** Almost eighty percent of websites are in English, yet one in ten people worldwide speaks English.

Based on the parameters above, it is evident why certain social groups have been left behind on ICT accessibility and involvement. Though these numbers and rates have been reduced and gaps have been narrowed, these problematic areas are persistent and still set back a large part of the population.

5.2 Theoretical Considerations

Since the global Digital Divide is of great importance, many scholars have focused on this phenomenon and tried to develop theories that should help explain why such a divide exists. Furthermore, these theories should explain how this divide has developed and why.

For conceptualizing the global Digital Divide scholars use two indices. On the one hand, mono-topical indices are widely used. On the other hand, comprehensive indices also exist but these are rarely used. However, Barzilai-Nahon (2007) argues that comprehensive indices should be used more often, since they take more parameters into account than the mono-topical ones. Therefore, they can conceptualize the Digital Divide more efficiently. The ICT sector has developed rapidly in the recent years, so researchers focus on the Digital Divide changes as well. In the '90s, the focus was mainly on infrastructural access including measures such as ownership, availability, and affordability of infrastructure. These measures have changed during recent years since more and more people own ICTs and different approaches have been applied (Barzilai-Nahon, 2007).

The most common theory adopted to explain the Digital Divide was developed by a comparative political scientist of Harvard University, named Pippa Norris. She sub-divided the Digital Divide into three categories since it is a multi-dimensional concept. The first one is the global Digital Divide which refers to ICT differences, especially the differences in Internet access between developed and developing countries. The social divide gap is considered the second subtopic of the Digital Divide, which addresses the gap in what has to do with access to ICTs between different parts of society in one country (Norris, 2000). The last one is the Democratic divide, which refers to the differences in how different political groups use ICT. **Figure 5.1** shows the countries where authoritarian regimes ban access to specific social media platforms, such as Facebook, X, and YouTube. Norris (2001) argues that rapid development of ICT will lead to new disparities between developed and developing countries and will, therefore, exacerbate new divides, like, the North-South divide.

Figure 5.1 *Social Media under Fire (sources: Google, X, OpenNet Initiative).*

However, some scholars argue that the existence of the Digital Divide is a natural phenomenon, and therefore, its decline will also be a natural process. They argue that government interference in bridging the Digital Divide will not be efficient because it will only shift the burden and costs of using ICT from one part of society to another. Therefore, social injustice is created rather than gap elimination (Yu, 2006).

Selwyn (2004) argues that the Digital Divide leads automatically to digital exclusion, and this term was first used in the context of the ICT differences between the North and the South. Furthermore, he stated that next to the wealth of a country and the capability to invest in ICT, other factors must be considered as well. Therefore, social and cultural dynamics are the main parameters of the Digital Divide.

5.3 Social Inequality in Internet Use per Country and Globally

The Internet can majorly define a person's life choices, education, and career path. Previous analysis of ICT's exclusion of certain groups of people, which mainly focused on developed and developing countries, has shed very little light on the diverse behavior of citizens regarding internet use. Researchers have observed that people with equal internet access tend to use the Internet for different reasons and access it at different intensity levels. Analyzing such behavioral patterns has become critical in contemporary research. The ways citizens benefit from using ICTs are also essential and it is now standard practice to categorize them regarding their online needs and behaviors. Such categorizations are called" user typologies.". In Europe, research conducted by Ortega Egea et al. (2007) used data from European countries (EU15) to compare and classify European users. The outcome was the following five groups:

- **Laggards:** These users occasionally use the Internet, none of e-government services, and rarely use the Internet for personal reasons. They make up 16% of citizens. Most are located in Germany, France, and Ireland.
- **Confused and adverse:** This group has a low level of internet usage in general, for personal reasons and government purposes. It is not very clear regarding the provided services. It makes up for 2% of users, and they are more commonly found in The United Kingdom and Austria.
- **Advanced Users:** People categorized as advanced users frequently use e-government services and online shopping services. They represent 16% of users and are mainly citizens of Holland, the United Kingdom, and the Nordic countries.
- **Followers:** Users of this category go on the Internet frequently, yet not daily. They make use of general online government services as well. The total number of users in this group is 19% and they are mostly found in Holland and Denmark.
- **Non-Internet Users:** As the name implies, users of this group make no use of the Internet. They make up the largest percent of users, 44%, and are found in Greece, Spain, Portugal and Italy.

However, measures have been taken towards the elimination of technological inequalities. For example, according to ITU and the World Bank, the number of internet users per one hundred persons in developed countries in 1998 was 17.0; in developing countries, it was 0.6. The relative size of the digital divide was 28.3. On the upside, in 2004, the number of internet users per hundred persons in developed countries was 53.8 and in developing ones it was 6.7. The relative size of the digital divide had shrunk to 8. Moreover, the average percentage growth in internet use during those years was 143% in Latin America and 346% in South Asia. In China, which constitutes approximately 20% of the world's population, the average percentage growth was an astonishing 694%, higher than any other country. This can be attributed to the rapid economic growth the country has been showing since 1978, with rural areas and the countryside, however, being left behind in technological infrastructure improvements and expansions.

5.3.1 The Case of India

India is a unique case of a modern-day consumerist society, characterized by an outstanding and prominent duality with deep roots in the country's history. A division of its people defines Indian society into castes,

ranking from lowest to highest classes. Castes, though, can also be viewed as a different interpretation of the western hemisphere's divide of" races" and" social statuses", along with the disadvantages these terms include. Understanding the country's history is crucial to comprehend modern day technology's exclusion of certain Indian society members. The hierarchy of castes relies on dharma and karma. Dharma is a person's destiny in this life, and karma is based on the reward or punishment of the fulfilment of dharma in the previous life, determining someone's current cast placement. As a result of the caste system, continuing your parent's trade is a fundamental aspect of Indian culture, and your placement plays a major role in your educational and professional level.

Today, India is the second most populous country, home to 1.339 billion people. However, one-third of the world's poor are found in it. The Internet intended for public use arrived in 1995, yet its estimated users are 47 million, whose annual income is more than three times larger than the average. Although caste mobility is more feasible than in previous years, it still represents a barrier to certain aspects of someone's life. So, engaging with the internet and its numerous applications can greatly benefit society's most suppressed members, creating more democratic grounds. With over 70% of the country being rural areas, there are great barriers to overcome since these areas lack connectivity to the road network, clean water, electricity and internet access. More than half of rural area residents have never even made a phone call, a notion complex for Westerners even conceive! The economic cost of providing power to such areas poses a great problem to governments, which also must tackle issues such as literacy, health, violence and emergencies like floods and earthquakes. The critical point in tackling the problem of ICT division in India is the awareness and understanding of the improvement that such technologies can have in e-governance, connectivity of distant areas, healthcare, education through e-learning, and assistance to agricultural communities. Moreover, there is a need for online representation of the numerous Indian languages that have no existence on today's English language dominated internet. This results in many Indian citizens not being familiar with the information and opportunities found online.

In recent years, governmental initiatives towards the modernization and expansion of ICT within all levels of Indian society have been taken. Numerous organizations have assisted these efforts in tackling problems within vulnerable groups, such as women who work outside of the protection of labor legislation. An example of such attempts is Microsoft's funding of *Datamation,* which assisted women in engaging with modern technologies and thus opened new career opportunities. On a governmental level, Indian authorities have founded an IT Task Force, an IT Action Plan from the Planning Commission and a Ministry of Information Technology (MIT). An example of a government funded initiative is the *Akshaya e-centres,* which enable ICT access to all members of society in Kerala State and promote ICT training, creating new job opportunities. Indian governments now acknowledge that only by investing in its people can India accomplish many improvements with the assistance of modern-day telecommunications.

5.4 Statistics

For many years, the number of people who had internet access was the most evident for measuring the global Digital Divide. The number of Internet users in January 2014 is shown in **Figure 5.2**. Unsurprisingly, most internet users can be found in the northern part of America (USA and Canada), in Europe, Australia, and New Zealand. The North-South division can also be observed here since the percentage of Internet users is significantly lower in the southern hemisphere than its northern counterpart. For example, in Africa, only 18% of the total population uses the Internet. However, its population is almost a third higher than the European one, where the number of internet users is significantly higher.

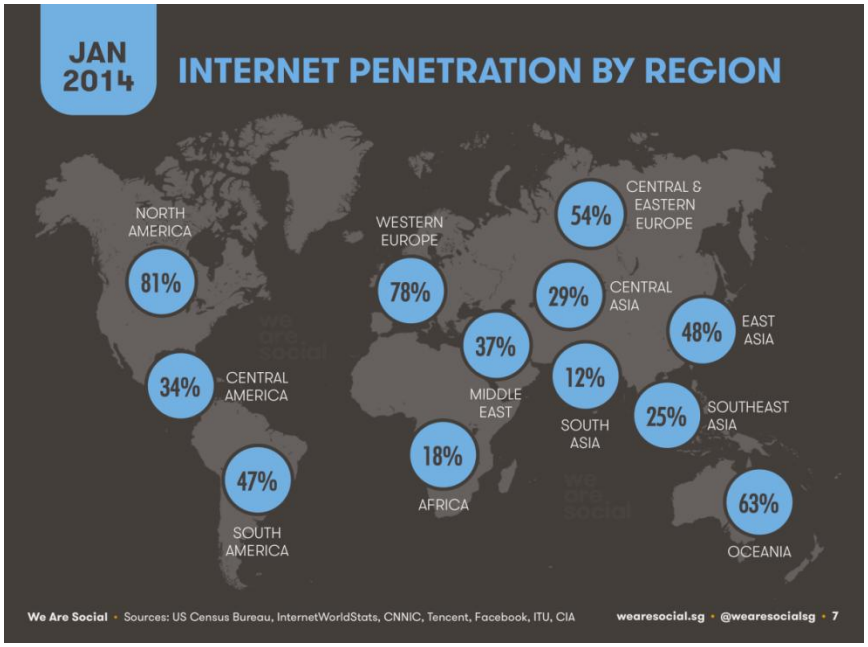


Figure 5.2 *Internet penetration by region in January 2014 (Kemp, 2014).*

In 2014 (Figure 5.2), nearly 75% (2.1 billion) of all internet users in the world (2.8 billion) lived in the 20 wealthiest countries of the world. The remaining 25% (0.7 billion) was distributed among the other 178 countries, representing less than 1% of total users. China, the country with the most users (642 million in 2014), represented nearly 22% of the total, and had more users than the following three countries (United States, India, and Japan). Among the 20 wealthiest countries, India had the lowest penetration (19%) and the highest yearly growth rate. At the other end, the United States, Germany, France, the UK, and Canada had the highest penetration: over 80% of the population in these countries had an internet connection at that time.

The number of Internet users around the globe has surged from 4.4 million in 1991 to 10 million in 1993, to 40 million in 1995, to 117 million in 1997, to 277 million in 1999, to 502 million in 2001, and to more than 600 million in 2002 to almost 3.3 billion internet users in 2015. Despite the rapid worldwide diffusion of the Internet, a disproportionate number of users is concentrated in more developed countries, especially the United States.

In 2001, 169 million Americans were online, about 60 percent of the country's total population and 29 percent of the world's Internet population. There were 172 million users in Europe (28 percent diffusion), 182 million in Southeast and East Asia, including 145 million in China, Japan, and Korea (23 percent globally). South America was home to 29 million users (5 percent globally), while there were 11 million in Oceania (2 percent globally), and 10 million in Africa (1.5 percent globally).

5.5 Causes of the Digital Divide

There are multiple causes of the Digital Divide, and although the internet access levels continue to grow, the divide persists (Steele, 2019). The most important causes of the divide are explained below.

A significant cause of the digital divide is the lack of education, digital or not (Steele, 2019). As such, investing in education is something that can have a significant impact on healing the digital divide. Another cause is income. Wealthy families are ten times more likely to own computers and high-speed internet connection at home than low-income families. For low-income populations, money is scarce. Their incomes are channeled toward basic needs and they view technology as a luxury (Steele, 2019).

Developed countries have invested in advanced digital technologies and high-speed broadband connections. Less economically developed countries do not have the resources to establish the necessary infrastructure. Inequalities in access also exist within the countries. Where you live inside a country matters, as urban regions are more likely to have access or be the first to access new technologies, like 4G or even 5G. Therefore, people living in developed nations have more access to computers, other digital devices, and networks. (Steele, 2019). This procedure starts early and is facilitated by the educational system in a country. Children and adolescents are motivated to develop the skills to utilize computer technology and the internet. This is a big advantage over people not exposed to technology early. This lack of physical access derived from education is frequently the case in developing countries and is responsible for maintaining and sometimes widening the gap between the already existing gap.

Personal interest is also a cause for the Digital Divide. Some people have the resources, abilities, and skills to access computers and the internet. However, due to lacking personal motivation, they do not find it interesting or essential (Steele, 2019) while others might find technologies too complicated to comprehend.

5.6 Setting Indices to Measure the Digital Divide

In order to measure the Digital Divide, national or international surveys are carried out to calculate indices referring to the access and use of the Internet and are conducted by government agencies, scholarly researchers, or international organizations.

One such index is the *Networked Readiness Index (NRI),* which is published annually by the World Economic Forum (WEF) in its "*Global Information Technology Report*" and is considered to be the most important measurement for analyzing the global Digital Divide. Generally speaking, the NRI aims to measure the ability of countries to use ICT. A common practice when setting indices is to subdivide them into a set of sub-indices. In the NRI case, four sub-indices are used. The first sub-index used is the *infrastructure* sub-index, which explores the country's ability to support high levels of ICT. The next sub-index is the *readiness* index which measures how much a society can use ICT infrastructure and digital content. The *usage* sub-index examines the degree of the individual efforts of the main social agents to increase their use of ICT and examines the use of ICT in their daily activities in terms of ICT. Finally, the *impact* sub-index measures ICT's economic and social impacts on society. The final NRI score is then an average score of all these four sub-indices (Bilbao-Osorio et al., 2014).

Figure 5.3 displays a map that indicates the Networked Readiness Index of 2014. The green indicates the highest index whereas the red indicates the worst. The NRI index does not cover grey areas. The best-performing countries are the Western industrialized ones, which can be found in Northern America and Western Europe as well as in Australia and New Zealand. First ranked is Finland, followed by Singapore and Sweden. The former communist countries in Eastern Europe, Russia, and China are ranked in a middle position. The developing countries that belong to the Third World, mainly the African, South and Latin-American, and some Asian countries are performing worse. Myanmar, Burundi, and Chad are the worst-performing countries (Bilbao-Osorio et al., 2014). Therefore, it can be concluded that the division of the world order in developing and developed countries cannot only be observed in political and economic terms but also in terms of their capabilities for using ICT, which leads to a further discrimination of the southern developing countries compared to their northern counterparts.

The Global Information Technology Report (2014) outlines that, in general, the readiness of developed countries in terms of ICT is progressing. In contrast, developing countries still face big problems in bridging their gap, and therefore, their NRIs are stagnating. However, several trends can be observed when examining the evolution of different countries over time regarding their ICT readiness. For example, countries rich in oil and gas resources saw the need to improve their digital infrastructure to overtake an active role in today's

globalized world. Therefore, they heavily increased their investments in ICT infrastructure. However, this development is not the case in the sub-Saharan countries. In these countries, no increase in *ICTization* is observed, and therefore their *ICTization* state is not expected to improve in the upcoming years. As a result, developing countries are further disadvantaged in economic and social development and this situation is not expected to be inversed in today's globalized world (Bilbao-Osorio et al., 2014).

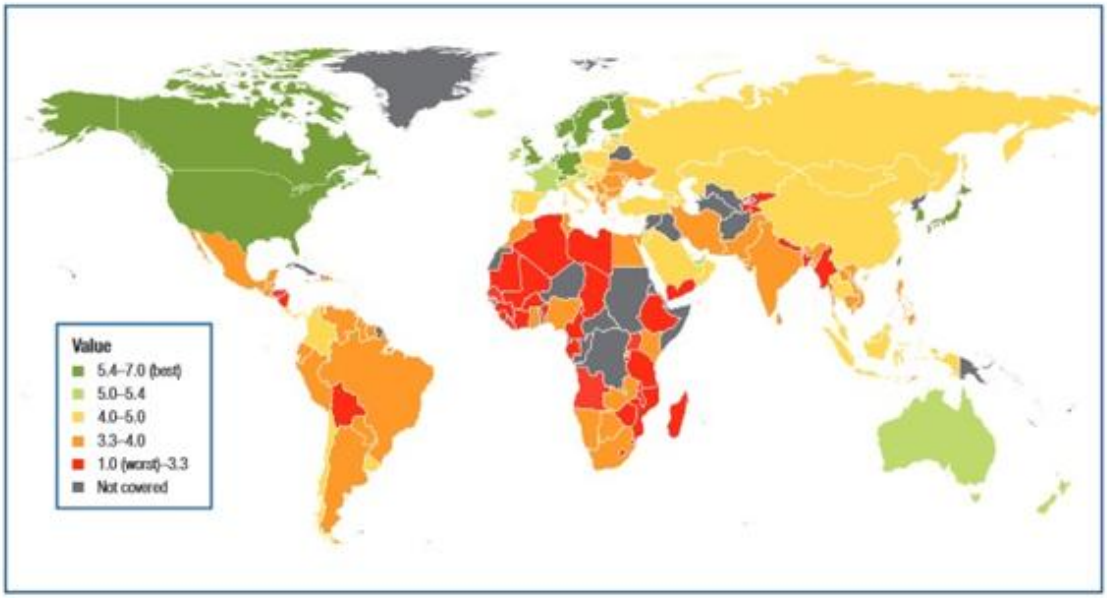


Figure 5.3 *The Networked Readiness Index in 2014 (Bilbao-Osorio, Dutta & Lavin, 2014).*

Another index used to investigate a country's development status is the Human Development Index (HDI). This measure considers the people and their capabilities next to economic growth. It measures the development status among three dimensions: a long and healthy life, being knowledgeable, and having a decent standard of living (United Nations Development Program, 2014). The HDI is the geometric mean of normalized indices for each of the three dimensions.

The United Nations International Telecommunication Union publishes the ICT Development Index. It is based on 11 internationally agreed ICT indicators, grouped into three clusters: access, use and skills. The access sub-index captures ICT readiness. It includes five infrastructure and access indicators (fixed-telephony, mobile telephony, international Internet bandwidth, households with computers, and households with Internet). The use sub-index captures ICT intensity and includes three ICT intensity and usage indicators (Internet users, fixed (wired)-broadband, and mobile broadband). The skills sub-index captures ICT capability or skills as indispensable input indicators. It is given less weight in the computation of the IDI compared with the other two sub-indices. The ICT Development Index is a standard tool for measuring the Digital Divide and comparing performance within and across countries. It must be noted that the ICT Development Index and the Human Development Index (HDI) are related. Therefore, countries with a low HDI do also have a low ICT Development Index.

Finally, the *Infostate* index is proposed by Orbicom, the International Network of UNESCO Chairs in Communications. The conceptual framework of the index introduces the notions of a country's *Infodensity* and *Info-use*. *Infodensity* is calculated considering ICT networks, ICT skills, machinery, and equipment in knowledge-oriented societies. *Info-use* derives from the consumption flows of ICTs, their use in households, businesses, and governments, and the general intensity of their actual use.

Infostate is an aggregation of *Infodensity* and Info-use indexes and represents the degree of a country's "ICT-ization". The Digital Divide is then defined as the relative difference of *Infostate* among economies.

5.7 The Vicious Circle of Globalization

According to Fong (2009), ICTs are crucial in reducing poverty in developing countries since economic growth is proportionally related to ICT. Therefore, the global Digital Divide deprives those people without access to ICTs of socio-economic opportunities. Such socio-economic opportunities are social and economic equality, mobility, e-democracy, and economic growth and innovations. Bridging the Digital Divide will automatically lead to poverty alleviation because people in developing countries will then have the opportunity to take part in today's globalized world. The economies of those countries might then catch up with their more developed counterparts (Fong, 2009).

Globalization has rapidly changed our world over the past years. Since ICTs, especially the Internet, have promoted globalization, they have also fragmented the world in countries that benefit from it and that which do not. Therefore, globalization and the global Digital Divide are interrelated in a vicious circle: Globalization broadens the gap, and the gap broadens globalization. Additionally, since developing countries are facing severe difficulties in terms of ICTs, it is impossible for them to benefit from globalization like developed countries do. Due to this fact, there is clear evidence that these disparities will continue to grow (Norris, 2001).

However, despite the global Digital Divide, ICTs, in general, will continue to provide developing countries with many advantages. Having access to ICTs and appropriately using them has the potential to increase the productivity of a country because the country can then better interact with the other economies in the world. This might then lead to new jobs and economic growth. It is generally accepted that international cooperation can be strengthened when developed and developing countries can productively interact towards mutual socio-economic benefits (Acilar, 2011).

5.8 The North-South Divide

As mentioned above, the North-South Divide describes mainly the division between the wealthy northern part of the hemisphere and the poorer southern part. This division is shown in **Figure 5.4.** Countries in the North, Australia and New Zealand are developed countries whereas developing countries could be found in the South. The developed countries are characterized as being wealthy, having stable governments and innovating technologies. Contrastingly, developing countries are lagging in almost all areas of development especially compared to the northern countries. Corruption is a big problem in these countries. Due to their lesser development, the provision of ICT is complicated in these countries because big problems exist regarding connectivity and capacity. Globalization is predicted to widen the already existing gap because it benefits those countries that have high levels of access to ICTs as well as high levels of digital literacy. Thus, the developed countries will always have a constant advantage over the developing countries.

International Organizations, like the UN and the World Bank also recognized this North-South Divide. It must be mentioned that the World Bank uses an economic measure to divide the world into developing and developed countries. This definition, middle- and low-income countries are considered developing countries. However, this definition is strongly criticized because some countries have a meager income but are rich in other aspects, and therefore, they cannot be considered developing countries (Ogunsola & Okusaga, 2006).

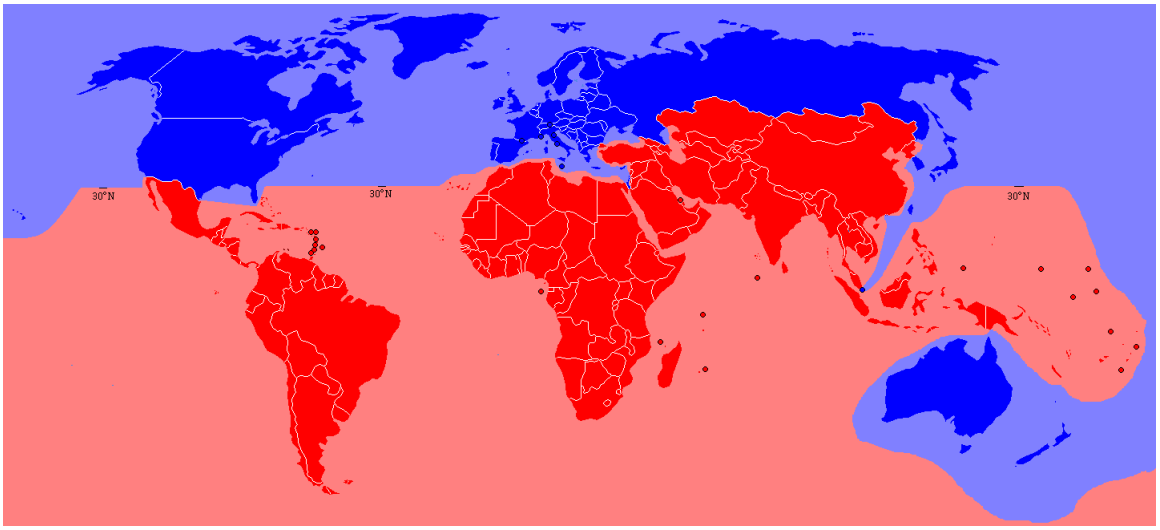


Figure 5.4 *The North-South Divide (Jolly, 2008).*

5.9 The Gender Digital Divide

As stated in the previous paragraphs, the term Digital Divide, formed by Gunkel, describes inequalities mainly in the distribution, access, and quality of digital media worldwide. Still, the term can have different meanings and was "*initially used to differentiate between technophiles and technophobics*" (Moore, 1995). From dividing digital equality around the world, the definition became wider and also describes: "*a deepening divide between the rich and the poor, an unequal distribution of information technologies in public schools, (…), the divide between those with and those without access to new technologies beginning in the late 1990s"* (Gunkel, 2003).

If one now applies these definitions to the means of gender inequalities, scientists make a shift from inequality of" access" to the one of" use" and" design" (Pujol & Montenegro, 2014). Studies by UNESCO to meet the millennium development goal of gender equality show that even though many women have access to ICT-software and digital media, most top-level-positions are occupied by men. "*Only one in four senior officials or managers are women*" (UN 2010, p 24). The "*Broadband Commission*" dealing with this UNESCO research project considers the digital gender gap "*to be a reflection of gender inequalities.*" They suggest that "*women should go online and take advantage of the opportunities that Information and Communication Technologies provide in a modern digital economy*" (Pujol and Montenegro, 2014). Thus, other variables must contribute to the gender divide in digital media. Cecilia Castano took a closer look at the distinction of" access" and" use" of the internet according to gender inequality. She states that "*the difference between access to and the use of technology is one of the most prominent gaps that allows us to identify the concrete gender differences and find a solution to the inequality"* (Bimber, 2000; Castano, 2008). She bases her theory upon data from the Observatory of E-Equality (System of Indicators of Gender and Technology). The observatory's findings show that "*men tend to have an instrumental use of the internet, while women use it for training, communication and caregiving*" (Castano, 2008). One could now make the statement that using the internet as an instrumental tool, as men are using it, enables them to engage in our economic life.

5.9.1 The Creation of Artificial Intelligence (AI) as a Reason for the Gender Digital Divide

However, why do women have different access and, especially, different use of ICT, and thus, are underrepresented in Artificial Intelligence? To tackle this question, the following studies are introduced by researchers on that topic.

In her book "*Artificial Knowing,*" Alison Adam describes Artificial Intelligence as a "*view of the world which prescribes the masculine as the norm and excludes other knowers and knowledge, specifically women*" (Adam, 2006). This theory is complex to support since companies responsible for algorithms usually keep their formulas secret (Crawford, 2016). The masculine could only become the norm because most creators of AI are men and AI, like all technologies, will reflect the "*values of its creators*" (Crawford, 2016). Additionally, Adam states that most AI systems run on personal computers and "*require specialist hardware largely found in academic settings*" (Adam, 2006). Here, she points out, that AI belongs mostly to specialists in the technological field, which makes it even harder for women to become a part of it, as their role in society traditionally does not involve technology. Adam argues that "*AI is best treated as a part of engineering and hence as a technology. (…) Engineering has hardly had a neutral history concerning gender*" (Adam, 2006). Also, she states that the "*socio-biological models*" of AI are politically problematic for feminists. The reason for that is its "*combative, aggressive behaviour*" which shows the "*worst part of human societies*" and is not associated with typically female characteristics (Adam, 2006).

Francesca Ferrando, a researcher in the field of technology at the University of Reading, England, conducted a questionnaire about the male domination of AI and had it answered by more than a hundred students and researchers from the Department of Cybernetics. Her purpose was to highlight the relation between gender as a *"biological, cultural and symbolic frame*" and the development of technology in the future. The respondents' gender was mainly male, which was proportional to the dominant gender in the department (Ferrando, 2014). The results of the involved questionnaire "*placed a clear emphasis on male characters*" (Ferrando, 2014).

5.9.2 The Image of Women in Digital Media

A couple of other reasons play a role when looking at the male bias of digital media. As Watkins and Emerson argue, women are put in a specific role in digital media in the first place; in the media, women are "*associated with the domestic sphere, while the workplace and other public settings are more often characterized as being masculine*" (Watkins & Emerson, 2000). In TV, women are mostly targeted for cleaning and beauty products. Blair and Takayoshi find that the "*image of the female body is portrayed in terms of the masculine gaze.*" The media shows the perfection of the female body that is not the norm and sexualizes their body in order to approach the hetero-male audience for the advertized products (Blair & Takayoshi, 1999). All these stereotypes are represented in digital media, which might also be a reason why women are kept at a distance from the field.

5.9.3 Discussion and Feminist Critique of Technology

Judy Wajcman, known as the founder of "*techno-feminism,*" defined the term" technology" as having a male bias. The word "*conspires to diminish the significance of women's technologies, such as horticulture, cooking, and childcare*" (Wajcman, 1991). This would make it impossible to involve women in technology, except one would give the word a new definition. Also, Eileen B. Leonard criticizes technology as "*systematically steering"* away minorities, and thus, it is and will stay an instrument of "*elite male domination*" (Leonard, 2003).

One can see the Gender-Digital-Divide as a cleavage that must be overcome by society, especially by women. Many things must be done to solve the gap; companies should establish gender quotas to achieve a 50/50 employment rate in the technological field. In order to achieve that, emphasis must be given to the goal of having women not only in jobs associated with traditionally female roles. Additionally, government policies should invest in education which treats everybody as equal, regardless of gender, and encourages girls to be more ambitious in their career perspective. They may also focus more on involving girls in fields that were perceived as only for boys, like technology. One project dealing with the issue is the Spanish action-research

project *Geratech*, which began in 2007 with meetings of different feminist associations to work in technology. Their goal is to "*establish alliances and commonalities*" concerning the "*transformation of socio-technical borders*" and to create joint action (Pujol and Montenegro, 2014).

On the other hand, why does equality mean that women should adopt the traditionally" male" behavior? This logic, as pointed out by Gunkel, "*reproduces a gender binarism that constructs women in terms of lack or difference when compared to men*" (Gunkel, 2003). Men create technology and AI; thus, women must do the same. This logic would be oversimplified and indirectly show men as the standard to which women are compared. Also, this automatically creates a hierarchy between male and female behavior, where female behavior can never be good enough – otherwise, it would be called male behavior. The "*occupations traditionally associated with women have become highly devalued*" (Pujol and Montenegro, 2014).

Eventually, as Pujol and Montenegro said: "*We have to recode the normative patterns that sustain our everyday practices*" (Pujol & Montenegro, 2014). The cultural field needs to be transformed to change the self-sustaining relationship between gender and technology.

5.10 Bridging Digital Divides: Experiments and Actions

During the 21st century, public sectors around the globe have initiated efforts aiming to bridge existing technological divides. Although great improvements have emerged from such efforts, many these actions tend to focus on the narrow definition of ICT's social divides by only providing physical access. Apart from access, which does play a critical role in a person's relationship with ICT, great importance lies within their training. American governments have promoted technology in all aspects of the private and public sector, on the northern side of the hemisphere.

In the mid-1990s, the Department of National Telecommunications & Information Administration (NTIA) of the US Department of Commerce published reports about Internet access and usage, three of which were:

- *Falling Through the Net: A Survey of the "Have Nots" in Rural and Urban America* (1995).
- *Falling Through the Net II: New Data on the Digital Divide* (1998).
- *Falling Through the Net: Defining the Digital Divide* (1999).

The term digital divide has been identified as one of America's leading economic and civil rights issues. The NTIA reports helped clarify which Americans were falling further behind and that concrete steps could be taken to redress this gap. The most significant telecommunications policy, the Telecommunications Act of 1996, removed legal and economic barriers to competition in the industry. This led to the expansion of competition, reduction of fees, and expansion of the variety of choices. Therefore, telecommunications networks became affordable to the public, who were previously deprived of access to information technologies. Moreover, the universal service Schools and Libraries Program, commonly known as "*E-rate*," provided discounts of up to 90% to public schools and libraries to enable telecommunications and internet access. Significant inequities existed between schools in the IT area, with the wealthier ones having more means to obtain and utilize computers and internet access. As a result, the E-rate initiative provided financial assistance depending on the economic status of the community where the school is built.

In China, the Communist Party of China (CPC) is launching several programs in order to enable and promote telephone and internet use in rural areas. The Village Access Project (VAP) in 2004 was an initiative of the Chinese government that provided telecommunication services in rural areas. By 2007, 99.5% of China's villages were equipped with at least two working telephone lines. Countries within Europe have also been launching programs in this direction. For example, some of the United Kingdom's governmental initiatives

include the National Grid for Learning Standards Fund, which aimed at getting all schools and libraries connected to the internet, and the governmental commitment to providing all its services online.

Scenarios of the future governance of Digital Europe 2030 include:

- **Open Governance**: Society members in this scenario will have exceptional access to information and technology and can interact with governing processes and potentially solve societal problems.
- **Leviathan Governance:** In this scenario, crucial decisions would be made by AI information systems, and technologically advanced systems would manage public information and services.
- **Privatized Governance:** Decisions in this scenario would be made by business representatives. ICT-supported decision-making systems owned by corporations would manage people's needs.
- **Self-Service Governance:** In this ICT-enabled society, citizens would address emerging problems themselves.

Nevertheless, the main points any government must invest in are education, physical infrastructure, motivation for ICT industry development, cooperation, and compliance with relevant international organizations' guidelines and policies.

5.11 Conclusion and Future Predictions

As stated above, to bridge or at least reduce the gap between information-poor and information-rich, which is the long-term goal of the international community, several policies should be applied, and measures should be taken. Access and infrastructural policies, such as investments, taxation, or subsidies are necessary, but more than such policies are needed. They need to be combined with educational policies because more than simply establishing the ICT infrastructure is required. People in developing countries need to be digitally literate in order to be able to use the new infrastructures and technologies. The ultimate goal should be to make ICTs accessible to most of people in each country (Stryszowski & Reynolds, 2013).

Bridging the Digital Divide can also have a broad range of social implications. Knowledge and information can improve the quality of life. Therefore, poorer southern countries must develop their National Information Infrastructure, boosting the national economy and leading to economic growth (Ogunsola & Okusaga, 2006). According to this theory, ICTs can be considered a perfect leveraging factor for poorer southern countries because they will increase the economic well-being and prosperity of the people there (Stryszowski & Reynolds, 2013).

The 21st century has become dominated by technology. Digital media and IT devices have become a considerable part of almost every person's life, facilitating actions in personal and public sectors. However, technology often tends to maintain and sometimes increase already existing inequalities. To respond to this phenomenon, governments seek means in order to provide the appropriate equipment and education on this matter. Global improvement has consistently been occurring, attempting to bridge gaps between rich and poor, north and south, female and male, old and young, or between rural and urban areas. The evolution and development of ICT industries have brought broad and affordable solutions to the public in the telecommunications sector.

However, there still is much to do for the global Digital Divide to be bridged shortly. If the developing countries do not manage to catch up, a widening of the gap may also occur, especially considering the vicious circle of globalization. In this scenario, the developed countries will benefit more and more from it, and the lag of the developing countries will remain.

References

Acilar A., 2011. "Exploring the Aspects of Digital Divide in a Developing Country." *Issues in Informing Science and Information Technology*, 8.

Adam A., 2006. "Artificial Knowing-Gender and the Thinking Machine." Routledge, London. Available at: https://content.taylorfrancis.com/books/download?dac=C2004-0-29149-1&isbn=9781134793563&format=googlePreviewPdf [Accessed 19 November 2017].

Ahmed S.N., Reyes-Macasaquit M., Tschang T., and Quibria M.G., 2003. "Digital divide: determinants and policies with special reference to Asia." *Journal of Asian Economics*, 13. Available at: https://*doi*.org/10.1016/s1049-0078(02)00186-0 [Accessed 17 December 2017].

Alles P., Esparza A., and Lucas S., 1994. "Telecommunications and the Large CitySmall City Divide: Evidence from Indiana cities." *The Professional Geographer* 1994 Vol. 46; Issue 3.

Badger E., 2019. "How the Rural-Urban Divide Became America's Political Fault Line." [ONLINE], Available at: https://www.nytimes.com/2019/05/21/upshot/america-political-divide-urban-rural.html [Accessed 15 May 2019].

Barzilai-Nahon K., 2007. Gaps and Bits: Conceptualizing Measurements for Digital Divide/s. *The Information Society: An International Journal*, 22(5), pp. 269-278.

Bell G. & Brand M., 2008. "What women want in a cell phone." *Transcript, National Public Radio*, June 10. www.npr.org

Bilbao-Osorio B., Dutta S., & Lavin B., 2014. "The Global Information Technology Report 2014 - Rewards and Risks of Big Data." *The World Economic Forum*.

Bimber B., 2000. "Measuring the Gender Gap on the Internet." *Social Science Quarterly 81*, No 3: pp. 868-876.

Blair K., and Takayoshi P., 1999. *Feminist Cyberscapes: Mapping Gendered Academic Spaces*. *New Directions in Computers and Composition Studies.* Stamford: Ablex Publishing Corp.

Brandtzæg P., Heim J., and Karahasanovic A., 2011. "Understanding the new digital divide - A typology of Internet users in Europe." *International Journal of Human-Computer Studies*, 69. Available at: https://doi.org/10.1016/j.ijhcs.2010.11.004 [Accessed 13 November 2017].

Broster D., Centeno C., and Misuraca G., 2012. "Digital Europe 2030: Designing scenarios for ICT in future governance and policy making." Government Information Quarterly, 29. Available at: https://doi.org/10.1016/j.giq.2011.08.006 [Accessed 15 October 2016].

Castaño, Cecilia (2008), *La segunda brecha digital*. Madrid, Ediciones Cátedra.

Chen W. & Wellman B., 2003. "Digital Divides and Digital Dividends." NetLab, Centre for Urban and Community Studies, University of Toronto.

Crawford K., 2016. "Artificial Intelligence's White guy problem." *The New York Times*. Available at: https://pdfs.semanticscholar.org/8600/6acb8650fe9c2a2b056e5271d9b525e09c3c.pdf [Accessed 8 November 2019].

Ferrando F., 2014. "Is the post-human a post-woman? Cyborgs, robots, artificial intelligence and the futures of gender: a case study." Springer Link, New York. Available at: https://eujournalfuturesresearch.springeropen.com/track/pdf/10.1007/s40309-014-0043-8 [Accessed 8 November 2019].

Fong, M. W. L., 2009. "Digital Divide: The Case of Developing Countries." *Issues in Informing Science and Information Technology*, 6.

Goding P. & Murdock P., 2001. "Digital divides: Communications policy and its contradictions." *New Economy*, 8.

Gunkel D., 2003. "Second Thoughts: Toward a Critique of the Digital Divide." *New Media & Society* 5, No 4: pp. 499-522.

James J., 2007. "The Digital Divide Across All Citizens of the World: A New Concept." *Springer Science+Business Media B.V.*, https://10.1007/s11205-007-9156-9

Jolly M., 2008. "The South in Southern Theory: Antipodean Reflections on the Pacific." *Australian Humanities Review,* 44.

Kemp S., 2014. "Social, Digital & Mobile Worldwide in 2014." Available at: https://wearesocial.com/us/blog/2014/01/social-digital-mobile-worldwide-2014/ [Accessed 12 November 2014].

Leigh P. R., 2010. "International Exploration of Technology Equity and the Digital Divide." *Information Science Reference*. Available at: https://b-ok2.org/book/844625/2ca08f [Accessed 15 November 2016].

marketingcharts, 2019. "Here are 3 Stats About Traditional Media Audiences to Keep in Mind in 2020." From marketingcharts. Available at: https://www.marketingcharts.com/featured-111409 [Accessed 15 December 2020].

Meedia, 2018. "Sexistische Algorythmen: Amazons künstliche Intelligenz zur Bewerber-Auswahl benachteiligte systematisch Frauen." Available at: https://meedia.de/2018/10/17/sexistische-algorithmen-amazons-kuenstliche-intelligenz-zur-bewerber-auswahl-benachteilige-systematisch-frauen/ [Accessed 11 December 2019].

Moore D., 1995. *The Emperor's Virtual Clothes: The Naked Truth about Internet Culture*. Chapel Hill: Algonquin Books.

Nations Online, 2014. "First, Second and Third World." Retrieved 12.11.2014, 2014, Available at: http://www.nationsonline.org/oneworld/third_world_countries.htm

Norris D.T. & Conceicao S., 2004. "Narrowing the digital divide in low-income, urban communities. New Directions for Adult and Continuing Education." 2004(101), pp. 69-81.

Norris P., 2000. "The Worldwide Digital Divide: Information Poverty, the Internet and Development." Paper for the Annual Meeting of the Political Studies Association of the UK, London School of Economics and Political Science, 10-13th April 2000. Round table on The Future Role of New Media in Elections Wednesday 12th April 10.45-12.15.

Norris P., 2001. *Digital Divide - Civic Engagement, Information Poverty and the Internet Worldwide*. C. U. Press (Ed.).

Ogunsola L.A. & Okusaga T.O., 2006. "Digital Divide between developed and less-developed countries: The way forward." *Journal of Social Sciences*, 13(2), pp. 137-146.

Ortega Egea, J.M. Menendez, M.R. Gonzalez, M.V.R., 2007. "Diffusion and usage patterns of Internet services in the European Union." Information Research 12 (2) Paper 302. Available at: http://informationr.net/ir/12-2/paper302.html

Pujol J. & Montenegro M. 2014. "Technology and Feminism - A strange couple." Revista de Estudios Sociales. Bogotá. Available at: https://revistas.uniandes.edu.co/doi/pdf/10.7440/res51.2015.13 [Accessed 8 November 2019].

Rao S.S., 2005. "Bridging digital divide: Efforts in India." *Telematics and Informatics*, 22.

Selwyn N., 2004. "Reconsidering Political and Popular Understandings of the Digital Divide." *New Media Society*, 6(341).

Steele C., 2019. "What is the Digital Divide?", Digital Divide Council. Available at: http://www.digitaldividecouncil.com/what-is-the-digital-divide/ [Accessed 8 January 2020].

Stryszowski P. & Reynolds T., 2013. "Capturing Digital Dividends and Closing Digital Divides." OECD - Ogranisation for Economic Co-operation and Development.

UN News Centre, 2012. "Digital divide closing, but still significant, says United Nations telecoms agency." Available at: http://www.un.org/apps/news/story.asp?NewsID=43265 [Accessed 15 November 2014].

United Nations Development Programme, 2014. "Human Development Index (HDI)." Available at: http://hdr.undp.org/en/content/human-development-index-hdi [Accessed 11 November 2014].

Wajcman J., 1991. *Feminism Confronts Technology*. Cambridge: Polity Press.

Warschauer M., 2003. "Technology and Social Inclusion: Rethinking the Digital Divide." The MIT Press, Available at: https://b-ok2.org/book/466216/f3865c [Accessed 5 November 2014].

Watkins, S. Craig and Rana Emerson, 2000. "Feminist Media Criticism and Feminist Media Practices." *The ANNALS of the American Acade*.

Xia J. & Lu T.J., 2008. "Bridging the digital divide for rural communities: The case of China." Telecommunications Policy, 32. Available at: 10.1016/j.telpol.2008.07.006 [Accessed 5 November 2014].

Yu L., 2006. "Understanding information inequality: Making sense of the literature of the information and digital divides." *Journal of Librarianship and Information Science*, 38(229).

Chapter 6 Digital Media: Promoting or Undermining Democracy?

Abstract

In this chapter, a theoretical investigation is attempted to evaluate internet's contribution to establishing a "better" democracy. Therefore, the aspects of a democratic society are presented to juxtapose features of the Internet, such as the free flow of information or the potential for greater online participation. Considering factors like the Digital Divide, the barriers to access to certain information, and digital surveillance in the name of citizens' protection or ads' implications of authoritarian regimes, it is concluded that the Habermasian Public Sphere has yet to take root in the online arena, while great expectations of the Internet for enhancing citizens' participation and reducing political apathy still need to be fulfilled. On the other hand, new participatory practices have been introduced through several projects aiming to diminishing the democratic deficit.

6.1 Introduction

The Internet, as a means of practicing democracy, is launching a new era of interaction and communication where citizens and states can engage in more meaningful and productive online discussions. Through this procedure, a new world order emerges in which people can enjoy greater access to institutionalized democratic procedures with fewer restrictions than in the past. Unsurprisingly, previously marginalized individuals can participate in public procedures and fulfill their role as active citizens. At the same time, states can apply more successful procedures of good governance and fulfill their provision of protection as well as services to their citizens. The internet strengthens and expands this possibility by enabling the creation of digital platforms, which are used as tools of information dissemination, and services provision and platforms for civic interaction through a decentralized and dynamic system. In that sense, with its near-infinite possibilities, cyberspace appears as a vehicle for fulfilling democratic ideals, allowing for more inclusiveness. Cyberenthusiasts argue that this postmodern type of the so-called e-democracy is the closest humanity has seen since the direct democracy of ancient Athens.

On the other hand, these great expectations are met by growing skepticism among citizens, experts, and politicians about the systems' credibility and safety, enabling a wide spectrum of information exchange between social structures and official institutions. The quality of democracy developing in the cyberspace virtual world and the efficiency of participation in governance procedures are highly debated, as these systems are not invulnerable to malicious acts, mistakes, or inaccuracies in their design.

6.2 Democracy

Democracy is the type of governance in which the ultimate source of power lies within the people. That is not just the etymology of the word but its true meaning and, at the same time, the prerequisite on which a democratic state is based. Thus, true democracy can only be direct because only then do citizens have the full authority in their hands (Ifestos, 2009), the same rights for participation in the political procedures and "*an equal seat at the table when it comes to negotiating a social contract*" (Richardson & Emerson, 2018). Therefore, "direct democracy" usually refers to citizens making policy and law decisions in person.

"Deliberative democracy" (or discursive democracy), as a term, corresponds to democracy in which deliberation is central to decision-making. It adopts elements of both consensus decision-making and majority rule. The tracks of deliberative democracy can be traced as back as 2,500 years ago, in ancient Athens, but it was already getting criticized. Even though it seemed that discussion of public matters would improve decision-making for some people, others believed that it could lead to bad decisions. Still, Athens was based on direct democracy in the *agora, where* several thousand citizens were gathering while discussions were mostly between a small number of orators whose aim was to persuade the people to vote for or against a decision (Elster, 1998).

Essential to the notion of deliberative democracy is argumentation and collective decision-making, a state where the main feature is participation. The concept of deliberative democracy is based on the fact that solving political problems requires discussions that lead to the best argument, which consensus accepts as a solution. This means that public opinion based on deliberation legitimizes power and holds it accountable. This implies that participation in public deliberation is equal and free (Dahlberg & Siapera, 2007).

As human societies have progressed, countries have adopted representative systems of democracy, which at least retain the rule of the majority principle through the voting procedure and the citizens' election of representatives in parliaments (Kumar, 2017). Therefore, the term "direct democracy" is opposed to representative democracy, which means transferring political power to a particular group of politicians who are elected as representatives. The transition from direct to representative democracy took place due to the

huge increase in the number of citizens since the classical era, along with the equal increase in the complexity of the decisions that modern society has to make (Zisopoulou, 2018). It was a necessary adjustment. The result, however, was that democracy declined since citizens were excluded from the decision-making process, and therefore, they showed reduced interest in politics (Jaeger, 2003), moving to a state of political apathy.

The distancing mentioned above of the citizens from the public sphere and political life led to the so-called democratic deficit that modern democracies experience, which translates into high percentages of abstention from elections and undermines the legitimacy of governments and their decisions (Zisopoulou, 2018). The democratic deficit is a threat to modern states since it undermines their legitimacy and makes them less efficient and active. Therefore, for the democratic deficit to be reduced, there must be a change in the context within which citizens are called to operate to play a greater role in shaping their countries' governmental policies.

6.3 E-democracy

The introduction of the internet in our everyday lives can be considered a change, capable enough of altering the way democracy works and giving birth to digital democracy or e-democracy, which can boost the active participation of citizens in politics, thus reducing the democratic deficit (Zisopoulou, 2018) mentioned above.

E-democracy can be defined as "*the use of information and communication technology (ICT) to foster interaction between citizens, elected representatives, and other democratic stakeholders such as political parties, civil society organizations (CSOs)*" (Oni et al., 2016). The ICTs play a significant role by delivering information and political knowledge (Zang et al., 2018), making people more keen and able to participate in decision-making (Spirakis et al., 2010). However, e-democracy, can be interpreted in two different ways, which derive from the various uses researchers have attributed to it. This diversification is the product of two distinctive schools of thought regarding technology and its effects on human societies. On the one hand, technological determinism proposes that technology is the catalyst element that defines the nature of societies; in this case, it argues "*that the internet plays a decisive role in social changes*" (Dafoe, 2015). Within this approach, we can find the roots of the revitalization of a direct democracy scenario since it is assumed that the new context that the internet creates and the tools it dynamically provides influence the decision-making process and pave the way for the return of direct forms of democracy.

"*Even the vision of citizens' self-government—evoking the Athenian ideal of a virtual agora or ekklesia seems to have renewed relevance as a possible model for future democracy*" (McCaughey & Ayers, 2003). On the other hand, social determinism views technologies as mere tools, inherently neutral, which are implemented on the base of the current structure of the society. According to this approach, the internet is just like any other technology and it is up to people to use it in a way that suits their current societies. Therefore, e-democracy cannot be anything more than the enhancement of representative democracy because other societal and structural factors have a fundamental influence on the development of democracy, with the internet being just a supplementary tool not able to cause extreme changes in the ways politics are conducted (Zang et al., 2018). This approach, considers e-democracy complementary and interlinked with the traditional representative democracy (Korthagen et al., 2018). Sundberg (2019) states that instead of looking at e-Democracy as a set of transformative tools, we ought to consider how technology can be utilized to conserve what we already have, such as a separation of power that can make a state more resilient against authoritarianism for example, by creating interfaces towards citizens but preserving separation on the inside. To sum up, ICTs themselves are not democratic or not democratic (Spirakis et al., 2010), but they can be used in order to create new forms of engagement in the political process (Oni et al., 2016) between the government, elected officials, media, political/societal organizations, and citizens (Kneuer, 2016), to make it more "democratic" than it is.

6.4 The Public Sphere

6.4.1 An Introduction to the Public Sphere

In political philosophy, the concept of the public sphere was invented by Jürgen Habermas (Habermas, 1989) to describe "*a realm separate form political, religious, or economic interests, in which citizens articulate shared opinions through public debate*" (Poell, 2009). It can also be defined as "comprising the institutional communicative spaces that facilitate public discussion and the formation of public opinion" (Enjolras and Steen-Johnsen, 2017).

Jürgen Habermas studied the 18th-19th century *bourgeois salons* where literate bourgeois discussed public matters and formed political opinions. The public sphere, after that, extended to broader parts of the population along with the development of literacy, the lengthening of compulsory schooling, the development of the press, and the freedom of association. The appearance of the Internet and ICTs were the last landmark in this expansion process. Scholars began using the expression "*networked public sphere*" to describe the public debate on the Internet: on blogs, forums, or social media. The Internet allows real time interactivity worldwide, virtually signifying the death of distance. Thus, it appeared as a perfect tool for direct democracy, during a philosophical movement rethinking democracy by making deliberation a core principle. Deliberation is thought, on the one hand, to allow the adoption of better public policies and, on the other hand, to confer a new democratic legitimacy. In this intellectual context, the networked public sphere was believed to perfect the classical public sphere. Habermas' concept relies on Talcott Parsons' systems-functional framework of separate spheres of society (political public sphere – informal public sphere – civil society – lifeworld), linked by theoretically deduced exchanges of flows (Friedland, 2006). However, in this imperfect framework, gaps, barriers, and dichotomies, are made up by the network integration.

"The Internet allows for a broader, more inclusive, and densely linked public sphere. It does not just place far more information in the hands of interested citizens; it transforms public debates by enabling online communities to use collaborative methods to create content, and correct inaccuracies" (Hindman, 2008). This idea of the regeneration of democracy through digital media and particularly the Internet was, for a time, widespread in the academic and intellectual world. Eminent thinkers such as Manuel Castells (1996) and Yochai Benkler (2006) defended this ideal of democratic progress through technique (technological determinism). The skyrocketing development of information and communication technologies (ICTs) in the mid-late 1990s led them to think that direct democracy could arise. In contrast, the heavily criticized representative democracy was thought to be in crisis. Therefore, "*forms of democracy without other mediation than technique*" (Benvegnu, 2006) were believed to occur.

Nonetheless, the movement of technological determinism is strongly contested by other scholars. This approach ignores that the phenomena of appropriation are at the same time long, complex, and unpredictable and lead to diversified uses, including some that might be poles apart from those imagined or developed in the first place: the diffusion of a technique at a larger scale does not necessarily lead to the reproduction of the first observed uses. Moreover, the software programs developed and used to feed the public debate are not neutral media, simple vectors of discussion on the particular space the Internet opens; their conception and adaptation are the objects of social struggles.

6.4.2 The Fragmentation of the Habermasian Public Sphere

As stated above, the public sphere is not static. It is elastic, and most of all, the object of social struggles. It has already been mentioned above that the Habermasian public sphere is not a neutral concept. It is socially and historically located in the 18th-19th century bourgeoisie. Many authors critically use the concept of the public sphere to describe what they think is the public space. Two main evolution patterns of the public sphere can

be observed: the fragmentation of the public sphere into smaller sphericules, and the renationalization of the public sphere (analyzed in the next paragraph).

"*The male-dominated public sphere is constituted upon a particular mode of cultural behavior and communication which privileged masculine norms of interaction and marginalized others based on gender, class, and ethnicity. It is a tool of gender and class-based hegemony, a function of control that gives the illusion of consensus and inclusion. Instead, it is based on naturalizing specific and contingent forms of social organization and interaction*" (Fraser, 2016). Nancy Fraser describes the public sphere as a masculine bourgeois mechanism of domination, excluding, through its norms, women and non-bourgeois. In his theory, Habermas prioritizes consensus and rationality over contestation and conflict, deemed contrary to the spirit of the public sphere. It is a way for the bourgeoisie to make social movement and social change illegitimate and protect its interests. Fraser and others postulate the co-existence of several public spheres. These competing publics have many names: public sphericules, counter publics, indigenous public spheres, and subaltern counterpublics. John Budarick defines them as "*marginalized groups in society which have for a long time constructed their language and, through deliberation, construct their terms and articulate their desires and needs*" (Budarick, 2016). We might take the example of the feminist public sphere, which, through networks of education, public speeches, organizations, managed to acknowledge in the dominant masculine public sphere's phenomena like domestic violence, femicide or salary gap as public issues, and not private. Here lies one major input of the Internet: it facilitates the construction of counter-public spheres. Social groups without access to the mass media can construct shared identities and interests and coordinate public actions more efficiently. It enhances the role of minority or ethnic media. However, are these ethnic media effective in influencing the public sphere? According to Budarick, "*Without some form of institutionalized avenues for cross-cultural dialogue, the role of ethnic media is unlikely to expand beyond the articulation of discursive subaltern publics, contributing to an image of cultural diversity with little political substance.*" To remedy this issue, Charles Husband theorizes a multi-ethnic public sphere, "*a commonly shared public space in order to avoid the political ineffectualness that multiple public spheres can bring*" (Husband, 1998) including the wide publication of alternative and subaltern ideas to "*hear, understand and acknowledge*" it.

6.4.3 Globalization and Digitalization of the Public Sphere

In parallel with the emergence of multiple counter public spheres, a phenomenon of transnationalization of the public sphere can also be observed. The traditional Westphalian nation-state is passing. Nowadays, *"transnational communities held together over time and space by a series of processes, beliefs and organizations*" (Husband, 1998) develop forms of transnationalism with the help of transnational communications networks (satellite television, digital communications technologies, telecommunications).

Budarick theorizes a renewal of the definition of diaspora. The traditional Greek definition of *"a forced dispersal from the homeland with a longing and commitment to one day return"* (Husband, 1998) emphasizes that the territory would now be irrelevant. A diaspora would now be "*formulated and sustained through a transnational imagination that encompasses multiple transnational linkages, identities, and communicative practices*" (Husband, 1998). In this context, cross-border media is of specific importance. However, it is difficult to constitute transnational publics, beyond the diaspora phenomenon, since imagined communities and nation-state still dominate the common representations. *"The formation of a transnational public requires sustained political debate across borders and a common consensus over issues of public importance across different sociopolitical landscapes"* (Husband, 1998). The only issues constituting a transnational public sphere are the specific global issues, unresolvable by a single nation-state. We can quote global warming, potential global extinction, or the infamous Covid-19 pandemic. Nevertheless, even though these issues are, in fact, globalized and international, they are being tackled with the old methods, each nation-state addressing the problem in its way.

6.4.4 Media and the Public Sphere

Media is and has always been at the core of the public sphere. It allows the diffusion of ideas, the education of the readers, and the formation of imagined communities linked by the same events. *"It is the most important institutional communicative infrastructure of the public sphere, a negotiator of public consent. It constitutes a realm of shared experiences, an interface in the relations within and between institutions" (*Hjarvard, 2013). "*The media contributes to the cohesion of society by linking its differentiated parts together on a symbolic level*" (Enjolras & Steen-Johnsen, 2013). The mass media, dominant in the 20th century, has been profoundly changed by the rise of social media and the Internet. Newspapers have known a *"perilous decline"* (Bowd, 2016) for decades, fastened by technological and social developments. At the beginning of the century, some thought the Internet would allow large-scale participative journalism: everyone could become a journalist through blogs. However, this myth of digital participative journalism quickly faded away.

Two main issues can be drawn out: the advertising business model is no longer sustainable, and the audience demand for information is dispersed. "*Fragmenting of audiences has begun to occur as audiences utilize both online and traditional media*" (Bowd, 2016). Henceforth, maintaining a social media presence has become compulsory for traditional media. Social media accentuate the fragmentation by providing new ways for news consumers to access information and interact with providers. In alternative terms, an individual has the option of acquiring information through various mediums such as print newspapers, television broadcasts, online publications (including both entirely digital platforms like Buzzfeed or Vice, as well as the digital adaptations of conventional newspapers), or social media platforms, regardless of their origin. On the other hand, publicists have moved their budgets from newspapers towards Google or Facebook, which are indeed much better investments.

This decline can be measured. There were 55,000 daily newspaper journalists in the US in 2007 and less than 35,000 in 2015 (Cagé, 2019). Paradoxically, *"the demand for news produced by professional journalists is doing well. It has, in fact, never been so high"* (Cardon, 2019). As we just said, the consumption of news has changed. For instance, the French nonspecialized newspaper *Le Monde* sells 250,000 copies daily but receives between 1.5 and 2 million visitors on its website.

All these mutations are synonymous with changes in the professional routine of journalists. They must learn new forms of publishing, be familiar with new platforms (media in a literal sense) and new audiences. The one-to-many model of information distribution is over. *"Internet technologies have facilitated the involvement of audiences in the observation, selection, filtering, distribution, and interpretation of events" (Bowd, 2016). The social process of information transmission is blurred. "The growth of the networked environment – and particularly of social media – is impacting on understandings of the public sphere (or spheres), and through this the role played by news media*" (Bowd, 2016). It is much more difficult to understand who gives to whom a piece of information. The information flows are *"non-linear, decentralized, and multi-directional"* (Bowd, 2016). From this, they emerged what we now call fake news, false news, and their counterpart, the fact checking services. More and more newspapers dedicate money and individuals to fact checking; verifying that news from other sources is accurate. It is a mutation of the social function of journalists: they are supposed to find the truth of social events through inquiry, and interviews now that their word has lost its value. Journalists now chase fake news, fact-check and confirm false information as a result of losing the exclusive right to report on the truth. Bernard Enjolras and Kari Steen-Johnsen studied the transition between mass media and networked media in Norway (Enjolras & Steen-Johnsen, 2013). In terms of communication, mass media were characterized by centralized means of information production and large investments in physical capital. In contrast, networked media are decentralized thanks to relatively cheap personal computers. In terms of information production, mass media has high levels of capital concentration, while networked media decentralizes and democratizes the means of production and distribution of information, knowledge, and culture. These processes lead to the nonmarket production of information and

large-scale cooperative efforts such as Wikipedia. To sum up, the media went from gatekeeping to gate watching (Bruns, 2009). Gatekeeping describes a function of control exercised by professionals over the production process of information, publications, and what is available to the public. Now, we are in the era of gate watching, a phenomenon of increasing reliance on the public as selectors and filters of content. Data gathered by sociologists suggest *"a displacement in the monopolist role of the media in bringing news and information to citizens"* (Enjolras & Steen-Johnsen, 2013). The media lost its monopoly on the political agenda-setting, and the politicians have direct access to the civil society, without the media as intermediary.

6.5 Enhancing the Current Levels of Democracy

According to what has been stated above, the discussion has moved into the new opportunities and tools that the internet introduces and the possible ways that they can enhance the democratic process. The main purpose of e-democracy is to enhance the quality and make the interaction between the government and the citizens easier. ICTs have exactly this role as they operate as channels of communication between the political elite and civil society. Furthermore, they allow people to share ideas with each other and with specialists conveniently, which results in a better understanding of the matter in question (Zisopoulou, 2018). Thus, a universal expression of will becomes possible through internet discussions, which have the unique feature of lacking mediators, and therefore, people can exchange ideas directly. Another differentiation is that *"…on the Internet, as opposed to classic media (newspapers, television), horizontal rather than vertical communication is possible – when information is transmitted from the source of information to the recipient. In Internet communication, each participant can be a subject concurrently as a source and as a recipient of messages"* (Linde, 2019).

The new channels of communication that the internet provides, which are faster, more direct, and easier to use, can be used to promote both bottom-up and top-down initiatives (Hennen et al., 2020). The bottom-up initiatives are introduced by private, nongovernmental, charitable organizations or activists, usually aiming to increase transparency and accountability. They also provide a variety of online platforms that allow citizens to contact politicians and highlight issues to public bodies or just send their complaints (Oni et al., 2016). On the other hand, top-down initiatives, are introduced by public authorities and are meant to please citizens' demands for greater civic engagement while increasing efficiency and lowering costs (Oni et al., 2016). No matter how these channels are introduced, e-democracy *"enhances political interactions and increases transparency, allowing people to be more involved in political decision-making processes and strengthen the responsiveness of political actors since represented and representatives can easily enter into dialogue on social media"* (Kneuer, 2016).

Some tools that are provided by the internet and make e-democracy a quite advantageous way of participating in the political process are: political forums, discussion sites, e-petitioning platforms, and e-voting processes (Bright et al., 2019). All these help citizens save time and money when participating in democratic processes (Spirakis et al., 2010), since other forms of mobilization require people to have at least some spare time to participate in the public sphere (Bright et al., 2019). Moreover, it can be easier to influence political debates from the comfort of everyone's house, through the internet. Moreover, e-democracy allows for the transition of the voting procedure to an e-voting one, in which the elections can be conducted solely through the internet (Spirakis et al., 2010).

Finally, e-democracy does not limit itself to local or national public affairs participation; it also applies to forming international discussions (Spirakis et al., 2010). At the same time, all these tools also play a role in countries with authoritarian regimes, where they increase the number of protests and the information flow (Evans, 2019) and thus contribute to the probable overthrow of the regime and the birth of democracy in its place.

The main reason why it is not possible anymore to create direct democracy systems is the number of citizens. While there were only a few thousand in ancient times, in today's democracies, we talk about hundreds of millions. India's population is approximately 1.4 billion making it the world's largest democracy. In the traditional communication process, only one person can speak at a time, which was workable in the small communities of the past. However, now, due to the complexity of matters discussed and the number of people able to participate in that process, the number of potential conversations grows exponentially. The internet has changed that, as it offers the ability to create networks where citizens can exchange ideas, discuss, and debate, allowing them to search for truth collectively.

The oratory and rhetoric that preceded voting as well as the public discussions in the agora constituted the essence of democracy as it was introduced in ancient Greece, and that is what e-democracy has the potential to achieve today.

6.6 Internet and the Public Sphere

The internet's political uses–or the internet's input to public debate and democracy–can take various forms, from blogs and forums to passive politicization on YouTube.

6.6.1 ICTs: Non-Neutral Tools

First, it must be highlighted that technology is not neutral but is considered to be *"external to politics, forgetting that the identity of communication devices is the object of a social construction*" (Benvegnu, 2006). Nicolas Benvegnu studied two websites of the early 2000s, created by two administrative entities responsible for constructing a national road east of France. One website was traditional, with a top-down logic, administrated by public servants publishing official news about the road: the digital version of classical official communication. The other was participatory, using the SPIP (Système de Publication pour l'Internet) software. Stemming from uzine.net and the Indie Web Manifesto, the SPIP allowed an original editorial platform that confused the roles of reader, writer, and administrator. At the time, this kind of collaborative platform was new. On uzine.net, visitors could discuss and publish their articles about a single theme: the civic appropriation of the Internet. One French administration decided to use the SPIP: *"Every internet user had the possibility to propose an article about the RN 19, or give their point of view on the forum attached to each article*" (Benvegnu, 2006).

Even in these early Internet times, 250 articles were published by 60 different authors. "*The website shows that the road is not just a bitumen coating across the Territoire de Belfort. The process at stake in a website opened to everyone's publication and founded on the co-production of information shows and stages the number and diversity of actors contributing to the fulfillment of an arrangement, and thinking about how this arrangement contributes to the development of a territory*" (Benvegnu, 2006). With this example, we note that the Internet cannot be considered synonymous with horizontal participation in direct democracy.

6.6.2 Structure of the Internet

Although the idea of inherent equality on the Internet is widespread, Matthew Hindman argues that winner-take-all patterns dominate political and public discourse. *"Political content online is overwhelmingly concentrated"* (Hindman, 2008): an internet user is improbable to find a political blog or a forum dedicated to public issues unless they search for it. *"The Internet and increasing media choice have amplified the importance of citizen motivation. Citizens with little interest in politics and without firm ideological or partisan commitments have shifted away from political news and towards soft, entertainment-driven content"* (Hindman, 2008).

According to Hitwise, a source of Web traffic data, in 2008 (when the article had been published), news and media Web sites accounted for only 3% of total Web visits. Political content is available for people searching for it. If we narrow down "*news and media Web sites*" to "*politics,*" it represented only 0.1% of total site traffic. In comparison, adult content represented 13%. This data is quite old, without a doubt, but I did not find any reason that would have revolutionized the Internet in the last 10 years in the sense that political content would now be the majority. Moreover, even within this 0.1% of political content, winners-take-all patterns can be observed, which is contrary to equality and fluid public debate: within the 970 most popular political websites, the top 50 sites account for 62% of the traffic, which makes 38% for the other 920 sites. Regarding blogs, Hindman states that most political blogs do not receive any visitors. They are, in fact, not public, and therefore, outside of the public sphere. "*The problem is that 99% of Web content about public issues does not qualify as part of the public sphere by this measure*" (Hindman, 2008).

6.6.3 Blogosphere and Forums: Another Bourgeois Sphere?

Matthew Hindman proposes a short sociology of the top-list bloggers. In 2008, they were lawyers, professors, journalists, senior managers, technology professionals, white and male, extraordinarily well-educated since 2 out of 3 attended an elite college and university. As a twist of fate, they are, in fact, quite similar to columnists of the most-read newspapers but even more elitist: "*While 20% of the op-ed columnist have a doctorate, 75% of the bloggers do," and "columnists provide a greater substantive representation of women and ethnic minorities*" (Hindman, 2008). "*The online public sphere is already a de facto aristocracy dominated by those skilled in the high deliberative arts*" (Hindman, 2008). However, on a theoretical plan, can blogs even be a part of the public sphere? Thomas Poell explores this question, studying 51 Dutch blogs and four forums in 2004 after the assassination of the controversial Dutch figure Theo van Gogh by a Dutch Moroccan.

The basis of the Habermasian public sphere is a critical rational public debate, which forums provide ideally in theory; anyone with an Internet connection can participate anonymously, suppressing some social markers. However, most forum discussions "*appeared to be neither inclusive nor critical rational*" (Poell, 2009). It seems that forums were then used not for debate, but for entertainment or personal expression. Forums are echo chambers: on the far-right Pim Fortuyn Forum, the assassination was proof of the failure of multicultural politics; on the international left-wing Indymedia, it symbolized the polarization of social relations to which Van Gogh had heavily contributed; on the Morocco Community forum. It was only an individual madman without any link to religion or ethnicity. Thus, forums are far from the criterion of critical rational debate. However, some critical rational arguments could be found at the margins, indicating "*that at least some forums incidentally meet the norm of critical rationality. They do suggest that Internet forums can, under specific conditions, facilitate this ideal*" (Poell, 2009). On the other hand, of their homogeneous character, "*blogs seem to be even less of an egalitarian platform of public debate than web forums*" (Poell, 2009). In this case study, only 51 blogs reacted to the assassination, quite a few compared to the estimated 30 million blogs in 2004.

6.6.4 Progress of the Internet: Alternative Public Spheres and Monitorial Citizenship

"*If we hold on to a strict normative definition of the public sphere based on the criteria of inclusiveness and rationality, we inevitably have to dismiss the mass of blogs and forums for failing to live up to this ideal*" (Poell, 2009). However, from the perspective of multiple alternative public spheres presented above, Internet blogs and forums are indeed the instruments of the emancipation of subordinated social groups. "It allows for the participation of groups who do not master the critical rational discourse used by politicians, intellectuals, and journalists who dominate mass media discussions" (Poell, 2009). There is another field in which the Internet participates in a networked public sphere: "*scandals it has either discovered or allowed to unfold more rapidly*"

(Hindman, 2008). Reporting scandals as a function of a public sphere is labelled by Michael Schudson "*monitorial citizenship*" (Schudson, 1998).

6.6.5 The ICTs' Unique Forms of Democratic Participation

The Internet and the ITCs participate in a networked public sphere because they transform aspects of a democracy. They allow new forms of democratic participation by enabling a large-scale collaborative democracy, "*easy and costless*" (Enjolras & Steen-Johnsen, 2017) and new forms of political mobilization.

Somebody might think about the 1st May of 2020, the first International Labour Day without demonstrations because of the Covid-19 pandemic: in France, trade unions called for online demonstrations, and many Internet users published photographs of banners and slogans from their homes. Another French example is the Presidential campaign of 2017, where the candidate Jean-Luc Mélenchon developed his YouTube channel to reach a new, younger audience: he has 449,000 subscribers, while the French President only has 138,000, even though he won. His young supporters on Discord, a communication software widespread in video-gaming communities, even developed a videogame to participate in their way to the campaign. These new forms of political and civic participation are individualized and take over the traditional forms of engagement in parties, associations, and trade unions. There is a shift from collective to connective action (Bennett & Segerberg, 2012): We can observe large-scale, fluid social networks rather than hierarchical institutions and membership groups with a collective identity. This is what Dominique Cardon calls "*civic tech*": *"various initiatives which, with a more civic than political vocation, endeavor to use digital resources to transform the political rules or intensify engagement within the current rules*" (Cardon, 2019). He distinguishes three different areas of civic tech. In representative democracy, civic tech makes the decision processes more open and transparent and enriches the citizens' information. He quotes *voxe.org*, a political platform comparator, *Acropolis*, a Twitch channel of political popularization, and *nosdeputes.fr*, a website where the open data of the French Parliament are formatted. In participative democracy, we can quote the famous petition websites *Change.org* or *Avaaz*. Finally, he labels "*internet democracy*" political movements aiming to go over representative democracy by establishing an imperative mandate through the ITCs. The Pirate Party has developed a software named "*Liquid Democracy*", through which the voters decide what their MP will vote for in Parliament. They can give their vote to another voter if they feel incompetent.

6.7 E-democracy: The Cybersceptics' Perspective

What has been stated above constitutes clear evidence of the potential for the improvement of democracy through the internet. However, cybersceptics argue that there are some problems with e-democracy on a theoretical and practical level. First of all, the whole concept of enhancing the existent democracy with the use of the internet is based on accepting that citizens have the will to participate in the political process. However, they lack the tools and the means to do so. This is evident in several cases of e-democracy proposed platforms. At the same time, while e-democracy solves some fundamental problems that societies faced before the e-participation, it also reproduces others and creates new ones that prohibit the e-democracy process from working correctly. It is often taken for granted that a nation-state would provide its citizens with all the necessary means to participate in its political life equally and where they could merge and enhance their worldviews in the Aristoteles' way, that is, searching for the truth together in the public sphere (Ifestos, 2009), could become mature enough to achieve the full public participation in the decision-making process. Nevertheless, e-democracy faces several needs to improve its implementation and use. In many cases, the extra means it provides cannot achieve the level of participation necessary for reestablishing a direct form of democracy, which would result in the Aristotelian ideal of democracy.

So far, the usage of the internet in the way politics are conducted has been considered as something inherently positive in that it enhances the democratic process. However, evidence-based empirical results suggest that the relationship between the internet and democracy is not linear and that sometimes the internet has a negative impact on democracy (Evans, 2019). It has been stressed that e-democracy is just a neutral tool that, if implemented properly, can enhance representative democracies. Hence, being a tool, apart from enriching democracy, it can also become a stress factor with harmful results on democracy's quality (Kneuer, 2016). First of all, there is the problem of implementation, which is most evident in developing countries. These countries face several problems regarding the deployment of the internet in democratic processes some of them being the lack of well-established frameworks for e-democracy realization, sustainability, and the low acceptance rate among their citizens.

Another issue that is present worldwide is the use of bots, either from people within the state or by outside enemies, in order to produce fake news and propaganda in social media (Persily, 2017). Fake news and propaganda infect the online structure of e-democracy, resulting in the alteration of citizens' true will and thus undermining democracy. These bots have the advantage of being automated, while the bot generator's identity is undiscoverable, making it impossible for the state to dictate if this is an inside or outside threat (Persily, 2017). Interestingly, the features that give the internet its power, namely anonymity and lack of accountability, enable foreign powers to intervene in other states' e-democracies (Persily, 2017) with the best target being the presidential campaigns and the voting procedure itself. A prominent example of this that comes immediately to mind is the case of the 2016 American elections. While the presidential campaigns of 2008 and 2012 confirmed our arguments laid above in the paper—that digital tools enhance democracy by expanding people's engagement— the 2016 one made clear that there are severe threats to e-democracy and limits to its positive contribution (Persily, 2017).

It has also been argued before that e-democracy has the advantage of reducing significantly the time needed to participate in the political procedures. While this is true, another aspect relates to the distinction between the time required to participate physically in the public sphere and the time required to learn about that issue you will argue about (Bright et al., 2019). The physical dimension is where the internet thrives by almost eliminating the time it takes to participate in the decision-making process. However, there is still a significant amount of time that the individual needs to learn about a topic and shape their point of view, which indicates that time still plays a role. That inevitably leads to unequal participation since not all people have the same amount of free time—this, of course, has to do with the economic capabilities of citizens in large part—to consume in getting informed about the various topics of discussion (Bright et al., 2019).

As it has been described in Chapter 5, in several countries, citizens do not have the means to participate in public decisions or influence the ones of their representatives because of the lack of democratization of ICTs and internet skills due to the Digital Divide. Of course, this is a big issue for e-democracy. In the future years, governments worldwide may turn to electronic means of governance, but unless all countries have access to Internet, e-democracy will fail.

Unequal participation translates into unequal influence. By participating more in online democratic activities, users give themselves more "*voice*" than others, allowing them to focus the community's activities on their interests (Bright et al., 2019). Likewise, a proportion of the population cannot get involved in the first place. That is because e-democracy processes are based on computer science and require accessible software. However, not all citizens can afford to access electronic means and ICTs (Chinn & Fairlie, 2007), resulting in several people being unable to make their voices heard, which derives straight from the second form of Pippa Norris' Digital Divide definition. "*The challenge for e-democracy is to find a way to promote the views of those less active or inactive at all and limit those with high activity*" (Bright et al., 2019). In order for e-democracy to function effectively, equality of access is needed.

Moreover, according to the third form of the Digital Divide's definition of Pippa Norris, some countries have censorship policies towards the Internet. Internet censorship is controls what can be accessed, published or viewed online, usually enacted by authoritarian regimes. These countries are usually characterized as "*enemies of the Internet*" and apply strong censorship, limiting access to information, social media platforms, and generally news sources or e-participation platforms. China is the most representative case of censorship where Web 2.0 applications such as YouTube, X, or Facebook are blocked, as analyzed in Chapter 13. Therefore, political discussions between citizens are barely possible. Therefore, countries considered as enemies of the Internet are far from e-democracy.

Eventually, there have been significant changes in the techniques applied by Security Agencies worldwide after the 9/11 incidents. In the name of National Security, citizens' personal data are monitored in an attempt to locate online criminals or terrorists' activities giving rise to severe objections against this invasion to civil liberties. This also constitutes a drawback of the Internet's potential to establish a better democracy. The so-called Surveillance Society context will be thoroughly presented and analyzed in **Chapter 13**.

6.8 Case Studies of E-democracy Projects

Numerous projects worldwide that aimed to establish platforms that would motivate people to engage more actively in civic participation and democratic processes. To outline the features of such attempts, some of these projects are presented in the following paragraphs.

6.8.1 The eVA Project (Czech Republic)

The eVA (electronic friendly administration) pilot project has been running in the Czech Republic since February 2002. There were info-kiosks installed in smaller municipalities (towns: Slany, Podebrady, Beroun; municipalities: Smecno, Klobuky, Zvoleneves, Morina, Mestec Kralove, and Patek) to strengthen and simplify the communication between citizens and the municipal office. Approximately twelve issues have been picked to be settled through the info-kiosk. The main functions included: guidelines for settling particular matters, necessary forms, the ability to send completed forms to the relevant institution, feedback to the citizens from the municipal office, information and regional news. The accessibility outside office hours and the removal of any negative "human factor" issues were the main advantages of the system. This pilot was monitored for one year, then the outcomes were assessed in order to decide whether this should be further extended to other municipalities.

6.8.2 Municipality of Casalecchio di Reno, DIRE (Italy)

DIRE was a project aiming to prepare a new generation of citizens for new ways of interacting and communicating with central and local administrations. It paved the way for greater online citizen participation in civic life and policy making. The project's goal was to raise awareness of new communication technologies and teach high school students in the Casalecchio area how to use ICT for new kinds of civic engagement. The project would last for five years and included a series of initiatives, such as the building of new technology labs in schools, a training course led by university lecturers on the use of computers and information networks, the establishment of an online discussion forum where students could exchange opinions and ideas, teaching them the necessary language and allowing them to experiment with ways of discussion and interaction with administrations. The project was conducted in partnership with the University of Bologna.

6.8.3 The 2002 "E-community" Competition (Germany)

When launching the "*e-community*" competition, the German Federal Minister of the Interior, Otto Schily, said, "*With the competition, we wish to encourage local authorities, cities and counties to avail themselves of the options provided by the Internet by means of creative projects so as to rejuvenate democracy.*" The Federal Ministry of the Interior would promote municipal participation concepts, with this new prize. With the prize of € 100,000, German cities, counties, and municipalities would be given the opportunity to implement e-democracy projects. The deadline for project proposals was 31 October 2002, and the prize was to be awarded to three local authorities in December 2002. The e-community prize should be used for the implementation of submitted project proposals. The experience gained through their implementation would also benefit the e-democracy projects of other administrations.

6.8.4 E-citizens in Amsterdam (The Netherlands)

This was a one-year experimental project where the districts and neighborhoods involved could follow one another's activities and learn from their own and each other's mistakes. The project focused on interactive policy making, rather than primarily on the associated ideological discussions. Its priority was to explore the potential role of the Internet in shaping public decision-making processes and how this affects the relationships between citizens, public servants, and administrators. The project has been implemented in Amsterdam at the district level, in "*Slotervaart*" and "*Noord,*" and at the neighborhood level, e.g. in the "Westerstaatsman" neighborhood.

6.8.5 Interactive Policy Making IPM (European Commission)

On 3 April 2001, the European Commission adopted a communication on Interactive Policy Making [IPM – C (2001)1014], which aimed to improve governance by using the Internet to collect and analyze reactions in the marketplace for use in the European Union's policy-making process. This initiative would be used by 26 Commission services to evaluate existing EU policies and for open consultations on new initiatives. Interactive Policy Making formed part of the "*e-Commission*" initiative and was linked to the Commission's governance and better regulation initiatives. All this was part of an effort to improve how the Union ran. The Commission argued that better accepted policy decisions would result in better participation of stakeholders in preparing these decisions. To that end, user-friendly systems were required. They needed views from businesses and citizens to build relevant and effective policies. It was also necessary to know what people thought about their new policy ideas and proposals put into place. The Internet helped them to collect and analyze this data. It also helped them to do this transparently. The IPM initiative aimed to help the Commission respond more quickly and accurately to the demands of citizens, consumers, and businesses to make EU policy making more transparent, comprehensive, and effective.

6.8.6 Engaging the Finnish Youth, VALTIKKA (Finland)

A website built by the Finnish Youth Corporation Allianssi and the Ministry of Education provided an informative channel for topical societal matters and a discussion forum. It was directed especially at young people from 14 to 19 years of age. The website's content has been formulated with students and special press officers of youth information. It allowed users to participate in planning the website's content. It was, therefore, an information and discussion channel, and an open forum to all important approaches made by civil organizations and individual activists. Through this dialogue, Valtikka aimed to motivate youth to participate in societal processes more efficiently while making those processes understandable and interesting. The idea behind Valtikka was that comments and ideas left to be seen on websites were not enough to make participation meaningful. Because of that decision, experts were invited to answer questions

posed by users and analyze weekly opinion polls. Moreover, experts were interviewed on the site whenever there was major news relevant to the lives of young people or when new laws were to be issued. Valtikka aimed to present structures and activities of the society, and the people working within it. It was an open channel for civil society actors and civil servants, elected officials, MPs, professionals, and experts. It was generally for anybody who wanted to promote young people's social involvement. One could contribute by either writing to the column section of the site or by answering the questions raised by youth on the "Ask Valtikka" page. Posters, postcards, and banner ads financially supported the promotional campaign, which focused on young people and their interest groups.

6.8.7 AGORA 2000 (Italy)

The AGORA 2000 project aimed to involve citizens fully in the decision-making process. The objective was to bridge the gap between citizens and regional/urban decision makers to get shared, enhanced solutions to territory planning issues. AGORA 2000:

- Supported the decision-making process of local/regional authorities; the objective was to define several possible alternative scenarios, with the identification and quantification of, as far as possible, quantitative parameters for comparing scenarios.
- Presented taken decisions, their rationale and, in general, the overall decision process to citizens using a user-friendly interface and intuitive 3D representation tools.
- Checked reactions from citizens and collected feedback from them.

The Project partners included: Comunità Montana Valle Maira (Italy), SATA. ApplicazioneTecnologie Avanzate (Italy), Amministrazione Regionale Toscana (Italy), Ayuntamiento de Valencia (Spain), Universidad Politecnica de Valencia (Spain), Universidad Politecnica de Madrid (Spain), Aquitaine Europe Communication (France), Business Flow Consulting (France), Ergon Consulting and Systems (Greece), Municipality of Anatoli (Greece).

6.8.8 The DEMOS Project

The reason for establishing the "*Democratic Efficacy and the Varieties of Populism in Europe*" (DEMOS) project was that voter turnout across Europe had dropped to historic lows, and more and more citizens were losing interest in politics. In the media, some observers have talked about this apathy as a "failure *of democracy,"*, others have gone further and have labelled it as "a crisis of representation." One reason for the diminishing interest in voting and political involvement is the growing distance between citizens and the decision-makers, whether local, national, or in Brussels and Strasbourg. This could be because political problems have become more complex and individual decisions involve a large mix of interests, but in what has to do with politics, decisions are not sufficiently well-communicated to the citizens. The gap between the individual citizens and political institutions was seen as too large, while the chance of having any individual influence was considered to be too small. The DEMOS project aimed at developing innovative online consultation tools. An open Web-based system would attempt to offer a user-friendly interface. It would include software modules that allow DEMOS' based systems to be adjusted to the full range of processes of online debate. The approach and the system would be tested at two trial sites – the Municipality of Bologna and the City of Hamburg.

This has also been a collaborative project and the partners were TUHH Technologie (Germany), GMDForschungszentrum, Informationstechnik (Germany), Ibermatica (Spain), IPSOS-RSL (UK), Pixelpark (Germany), Municipality of Bologna (Italy), Nexus-International Broadcasting Association (Italy) and Freie und Hansestadt Hamburg (Germany).

6.9 Conclusion

In this chapter, the relationship between the internet and democracy has been examined. More specifically, the democratic deficit has been analyzed regarding the distancing of citizens from the political procedures that took place in the transition from direct to indirect or representative systems of democracy. It has been highlighted that the use of the internet can enhance the level of democracy in modern societies, not by going back to a form of direct democracy but by strengthening the representative ones based on the fact that the internet is just a tool, according to the social determinism school of thought. Indeed, it became evident that e-democracy offers many advantages and provides the necessary tools to increase the participation of citizens in the decision-making process and establish a productive discussion among them inside the public sphere. However, some obstacles have been spotted. First, these tools may not change the percentage of people interested and willing to participate in the political process. Second, e-democracy, while solving some problems, it also introduces other issues that undermine the whole process.

The transformation of the Habermasian public sphere by the ICTs has also been examined here. First, the philosophical concept of the public sphere developed by Jürgen Habermas has been explored in depth, showing its epistemological debates. It was proven that multiple public spheres coexist, by replacing the concept in its own historicity, and by explaining the elasticity of the public sphere. The changes in the media sphere, a part of the public sphere, were described. The ITCs have provoked the fragmentation of the audience and forced the traditional media to take a position on the digital market and invent new forms of journalism to keep exerting a hold over the diffusion of ideas, news, and the formation of public opinion.

The myth of an egalitarian Internet that would magically resolve the crisis of representative democracy was dispelled. In fact, studies on blogs and forums have shown that despite a theoretical leaning towards rational critical debate for all, they are used as the exact contrary. However, the Internet brought good news to the contemporary public sphere: it helps the political minorities to build their alternative public sphere, allows monitorial citizenship, and creates new forms of political mobilization and participation.

"*The central problem with the online public sphere is that it excludes so many citizens. It is bewildering, and darkly humorous, to see white, male bloggers with Ivy League degrees writing about how the Internet is empowering 'ordinary citizens.'*". What they mean by this is that the Internet is empowering people like themselves (Hindman, 2008). The networked public sphere is not an egalitarian realm that suppresses all social inequalities. Digitalizing our societies has been an ongoing process since its beginning, and it is difficult to predict the future. The Covid-19 pandemic and the quarantine seemed to quicken this digitalization process through the massive development in a short period of remote working, distance-learning courses and digital communications.

The ICTs present the same issues as the original bourgeois Habermasian public sphere: inclusiveness, accessibility, and freedom from government and market interference. Gender, race, and class are still determining factors to access the public sphere, even though it is digital or networked. "*The Internet pluralizes but does not inherently democratize spheres of social, cultural, political or economic activity*" (Budarick, 2016).

Conclusively, e-democracy can enhance indirect democracy by increasing citizens' level of participation and by enabling them to discuss in the public sphere on the web; but not in the same level of participation as in ancient Greece's direct democracy. At the same time, new challenges that come alongside e-democracy can also have degrading results.

References

Babeau F., 2014. "La participation politique des citoyens ordinaires sur l'Internet. La plateforme Youtube comme lieu d'observation." *Politiques de communication*, vol. 3, no. 2, pp. 125-150.

Bennett W.L., and Segerberg A., 2012 "THE LOGIC OFCONNECTIVE ACTION, Information." *Communication and Society*, 15:5, pp. 739–768.

Benvegnu N., 2006. "Le débat public en ligne. Comment s'équipe la démocratie dialogique?" *Politix*, vol. 75, no. 3, pp. 103–124.

Bohman J., 2004. "Expanding Dialogue: The Internet, Public Sphere and Transnational Democracy," in Peter M. Shane (ed.). *Democracy Online: The Prospects for Political Renewal Through the Internet*. New York: Routledge.

Bowd K., 2016. "Social Media and News Media: Building New Publics or Fragmenting Audiences?" in Mary Griffiths and Kim Barbour (eds.), 2016. *Making Publics, Making Places.* University of Adelaide Press, South Australia, pp. 129–144.

Bright J., Bermudez S. Pilet J.B., and Soubiran T., 2019. "Power users in online democracy: their origins and impact." *Information, Communication and Society*, pp. 1–16. Available at: http://doi.org/10.1080/1369118x.2019.1621920 [Accessed 22 May 2020].

Bruns A., 2009. Vom Gatekeeping zum Gatewatching, in: Neuberger C., Nuernbergk C., Rischke M. (eds), *Journalismus im Internet*. VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91562-3_3 [Accessed 5 May 2019].

Budarick J., 2016. "The Elasticity of the Public Sphere: Expansion, Contraction and 'Other' Media." in Mary Griffiths and Kim Barbour (eds.), 2016. *Making Publics, Making Places.* University of Adelaide Press, South Australia, pp. 9–26.

Cardon D., 2019. "Civic tech: démocratiser la démocratie." *Culture numérique*. Paris: Presses de Sciences Po, pp. 277–289.

Cardon D., 2019. "Les médias face à la révolution numérique," *Culture numérique*. Paris: Presses de Sciences Po, pp. 247–260.

Chinn M.D., and Fairlie R.W., 2007. "The Determinants of the Global Digital Divide: A Cross-Country Analysis of Computer and Internet Penetration." *Oxford Economic Papers*.

Dahlberg Lincoln and Eugenia Siapera, 2007. "Introduction: Tracing Radical Democracy and the Internet." in Lincoln Dahlberg and Eugenia Siapera (ed.), *Radical Democracy and the Internet: Interrogating Theory and Practice.* Basingstoke: Palgrave Macmillan.

Elster J. (ed.), 1998. "Introduction." In Elster J. (ed.), Deliberative Democracy. Cambridge: Cambridge University Press.

Enjolras B., Steen-Johnsen K., "The Digital Transformation of the Political Public Sphere: a Sociological Perspective." in Kari Steen-Johnsen et al. (ed), *Institutional Change in the Public Sphere: Views on the Nordic Model*, 1st ed., De Gruyter, Berlin/Boston, 2017, pp. 99–117.

Evans O., 2019, "Digital politics: internet and democracy in Africa," Journal of Economic Studies, 46(1), pp. 169–191. Available at: http://doi.org/10.1108/jes-08-2017-0234 [Accessed: 22 May 2020].

Fraser N., 2014. "Transnationalizing the public sphere: On the legitimacy and efficacy of public opinion in a post-Westphalian world", in K Nash (ed.), *Transnationalizing the public sphere*, Polity, Cambridge, pp. 8–42.

Friedland L., Hove T., Rojas H., 2006. "The Networked Public Sphere." *Javnost - The Public*, vol. 13, No 4, pp. 5–26.

Habermas, J. [1962]1991. *The Structural Transformation of the Public Sphere: An Inquire onto a Category of Bourgeois Society*. Translated by Thomas Burger and Frederick Lawrence. Cambridge: The MIT Press.

Hanson Jarice and Alina, 2011. "The Internet as the Public Sphere: Deliberative Democracy and Civic Engagement." in Aroon Manoharan and Marc Holzer (eds.). *E-Government and Civic Engagement: Factors and Determinants of E-Democracy*. Hershey: Idea Group Inc.

Hennen L., Van Keulen I., Korthagen I., Aichholzer G., Lindner R., Nielsen R.Ø. 2020. "European e-democracy in practice." Cham, Switzerland: Springer Open. Available at https://link.springer.com/book/10.1007/978-3-030-27184-8 [Accessed: 22 May 2020].

Hindman M., 2008. "What Is the Online Public Sphere Good For?" in Joseph Turow and Lokman Tsui (eds), 2008. *The Hyperlinked Society: Questioning Connections in the Digital Age.* University of Michigan Press, Ann Arbor, pp. 268–288. http://doi.org/10.2991/csis-18.2019.70 [Accessed: 22 May 2020].

Hjarvard S., 2013. *The Mediatization of Culture and Society*. 1st edition, Routledge.

Husband C., 1998. "Differentiated citizenship and the multi-ethnic public sphere." *The Journal of International Communication*, 5:1-2, pp. 134_148, DOI: 10.1080/13216597.1998.9751869 [Accessed: 5 May 2019].

Ifestos P., 2009. "Worldview of nations: Composition and containment of the states of the states of Europe and the world." Piotita Publications, Athens.

Kneuer M., 2016. "E-democracy: A new challenge for measuring democracy." *International Political Science Review*, 37(5), pp. 666–678. Available at: http://doi.org/10.1177/0192512116657677 [Accessed: 22 May 2020].

Korthagen I., Henneet L., Aichholzer G., Gloria R., Lindner R., Goos K., and Nielsen R.Ø., 2018. "Prospects for e-democracy in Europe." Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/603213/EPRS_STU(2018)603213_EN.pdf [Accessed: 22 May 2020].

Kumar T. M. V., 2017. "E-democracy for smart cities." Singapore: Springer. Available at http://doi.org/10.1007/978-981-10-4035-1 [Accessed: 22 May 2020].

Linde A., 2019. "Comparative Analysis of Cases of Technocratic Governance and Deliberative-Democratic Self-Rule in Internet Sphere." *Proceedings of the International Conference Communicative Strategies of Information Society* (CSIS 2018).

Manga E., Ruth M., "Les TIC, nouvelles formes d'action politique. Le cas des diasporas camerounaises," *Afrique contemporaine*, vol. 234, no. 2, 2010, pp. 127–140.

Margolis M., and Gerson M.R., 2009. *The Prospect of Internet Democracy*. Farnham: Ashgate Publishing.

Oni A., Ayo C., Oni S., and Mbarika V.W., 2016. "Strategic framework for e-democracy development and sustainability." *Transforming Government: People, Process and Policy, 10(3)*, pp. 457–477. Available at: http://doi.org/10.1108/tg-09-2015-0040 [Accessed:22 May 2020].

Papacharissi Zizi, 2009. "The Virtual Sphere 2.0: The Internet, the Public Sphere, and Beyond." in Andrew Chadwick and Philip N. Howard (eds.), *Routledge Handbook of Internet Politics*. London: Routledge.

Persily N., 2017. "Can Democracy Survive the Internet?", *Journal of Democracy*, 28(2), pp.63–76. Available at: http://doi.org/10.1353/jod.2017.0025 [Accessed: 22 May 2020].

Poell T., 2009. "Conceptualizing Forums and Blogs as Public Sphere." in Marianne Van den Boomen et al. (eds.), 2009. *Digital Material: Tracing New Media in Everyday Life and Technology.* Amsterdam University Press, Amsterdam, pp. 239–252.

Richardson J., and Emerson J., 2018. "An Emerging Force for Change (SSIR)." [Online] Available at: https://ssir.org/articles/entry/edemocracy_an_emerging_force_for_change [Accessed: 20 May 2020].

Schudson M., 1998. *The Good Citizen: A History of American Civic Life*. New York, The Free Press, pp. 105-107.

Sifry Micah L., 2014. *The Big Disconnect: Why the Internet Hasn't Transformed Politics (yet)*. New York: OR Books.

Spirakis G., Spiraki C., and Nikolopoulos K., 2010. "The impact of electronic government on democracy: e-democracy through e-participation." *Electronic Government*, *an International Journal*, 7(1), pp.75–88. Available at: http://doi.org/10.1504/eg.2010.029892 [Accessed: 22 May 2020].

Sundberg L., 2019. "Electronic government: Towards e-democracy or democracy at risk?", *Safety Science*, 118, pp. 22–32. Available at: http://doi.org/10.1016/j.ssci.2019.04.030 [Accessed: 22 May 2020].

Witschge Tamara. 2004. "Online Deliberation: Possibilities of the Internet for Deliberative Democracy." in Peter M. Shane. *Democracy Online: The Prospects for Political Renewal Through the Internet.* New York: Routledge.

Zang L., Xiong F., and Gao Y., 2018. "Reversing the U: New Evidence on the Internet and Democracy Relationship." *Social Science Computer Review*, 37(3), pp. 295–314. Available at: http://doi.org/10.1177/0894439318767957 [Accessed: 22 May 2020].

Zisopoulou E. 2018. "E-Government: The Aspects of E-Accessibility, E-Inclusion and E-Participation as Strategies to Promote Active Citizen Participation". "Governance and Public Policy" postgraduate program lecture notes, University of Peloponnese.

Chapter 7 Social Media and Politics

Abstract

Based on the popularity of social media, this chapter highlights their contribution to Politics. In social media platforms, political discussions shape the public agenda and influence public opinion. Moreover, they constitute great tools for political campaigning, having already been used effectively worldwide for more than a decade. Cases of the political use of social media in electoral campaigning are presented, including the "innocent" US presidential elections of 2008 and the 2016 US presidential elections, where there has been clear evidence of international interference as well as the use of fake accounts (bots) for diffusing fake information in order to shape voters' behavior. Finally, a new aspect of political use of social media is marked, digital diplomacy.

7.1 Introduction

Internet, as an instrument of communication, information sharing, and expression of opinion, promotes a new way of interaction, where the individual meets the collective in a dialectic relationship, free from the conventions and restrictions of the past, as well as from those who monopolize information, within a decentralized, networked, changing, and dynamic system; a system, where users are the informants and feeders at the same time of information in a digitally connected universe. In this way, a new social order emerges where ordinary men and women can express themselves, ultimately promoting modern forms of democracy.

However, there are dangers, in this age of digitalized communication. The internet, as opposed to the official and institutionalized sources of information, offers opportunities for manipulation and distortion of data, given that no authority has the mandate or capacity to guarantee the truth or falsity of those posted on its sites. The result is that the internet is potentially a mechanism of misinformation to the detriment of democratic practices. Consequently, the use of digital media raises skepticism among citizens, experts, and politicians about the quality of online information and the ability of citizens to make informed choices.

An inherent feature of democracy is to enable citizens to freely express and interact with one another, regardless of their social status and position in the power structures of their society. Internet and digital interaction platforms strengthen and expand this possibility even more in modern societies. The internet has been a tool for information sharing and open dialogue since its inception, accessible to all those who wish to use it and have the necessary equipment, giving the possibility to connect, express one's self, and communicate with millions of users worldwide. The system is designed based on self-regulation, where control of what is shared or published is limited (or, more accurately, is gradually developed by state authorities or corporate actors). At the same time users enjoy the freedom to choose the subject and content of their postings according to their interests. From politics to ethics and aesthetics to science, nowadays, social media users or other internet platforms can express their opinions with little or no restriction in an unprecedented form of freedom. In this respect, one could argue that this postmodern type of e-democracy with its cyber citizens is, in essence, the closest it has been to direct democracy since the City Church in ancient Athens. The parliamentary podium, to which most people have no access, is replaced by Facebook, X, Instagram, or numerous other online platforms that can host their views. In this sense, cyberspace, with its near-infinite possibilities, is a vehicle for the implementation of democracy and the fulfillment of human rights in our global society. Procedures of an explicitly political nature, such as electronic voting, opinion polling on social and political issues, online participation in public debates, and timely and widespread public access to information on issues of common interest, all have made a significant contribution to reducing the democracy deficit at a global level.

At the same time, the internet and social media compete with or even undermine, the more official sources of information, public or private, which gradually lose much of their role in dominating (or monopolizing in some cases) the flow of information to the public. Undoubtedly, with the significant and unrestricted flow of information, pluralism is increased to the benefit of the public; however, the internet is not only a place of true but also of false information. In other words, no one guarantees the truth of those posted on its sites. On the contrary, digital technology can manipulate and erode data, including audio and visual material (videos, photos, audio graphics, and multisensory presentations), which have a greater power to persuade and ultimately mislead the audience. This increasing trend has given rise to skepticism as there are serious doubts about the credibility of the information circulated online. At the same time, many questions are raised about the quality of shared information and, consequently, the ability of the public to make informed decisions. In this context, democracy is severely threatened and is endangered in our modern societies.

Searching for the truth began more intensively with the introduction of the World Wide Web (Boler, 2008). Since the development of digital media and the Internet, many have wondered about their impact on politics. Questions such as what the contribution to strengthening both democratic values and participation in politics, and more generally in the dissemination of knowledge in politics, will have been of particular concern to many scientists (Sweetser, English & Fernandes, 2015). Indeed, scientists believe that the Internet creates different dimensions of truth that affect politics. More specifically, in the past, events were reported in the media for which their validity could not be ascertained. The digital age has allowed the public sphere to confirm these facts, as citizens now have access to multiple news sources beyond traditional media. Therefore, new opportunities are given to the public sphere to acquire truth (Boler, 2008).

Acquiring truth as a process refers to democratizing politics through digital media (Boler, 2008). At the beginning of the 21st century, we undoubtedly have new sources of democracy in the media and new means of controlling events. Initially, the discussion focused on the results of the Internet (Web 1.0). However, with the development of technology today, attention is focused on social media (Web 2.0) and their impact on politics (Sweetser, English & Fernandes, 2015). There are differing and conflicting views on the impact of the Internet on political life, as it is argued that there is no longer a central factor in determining information, but "the same people who" consume "what is on the Internet are increasingly producing it" (Boler, 2008). Thus, some argue for the positive interaction of the two, believing that it has strong results in information and knowledge as well as in political participation (Sweetser et al., 2015). Others argue that the Internet and digital media are mainly entertainment media and have no effect on politics, as they believe that the mechanisms that encourage political participation and engagement are different (Dimitrova et al., 2011). People using Web 2.0 try to become part of the public sphere, to intervene in it to communicate their point of view and position. Therefore, the use of digital media highlights the realization that many of the facts of traditional media are constructed, the need to change the status quo, and an urgent political need for accurate and responsible reporting (Boler, 2008).

Eventually, the reconstruction of events by the media concerns the question of power and knowledge. The introduction of new technologies has changed the situation, as new sources of information that greatly limit traditional medias' power. The digital age has set new preconditions for participation in the public sphere and the political debate (Boler, 2008). Therefore, it is considered that digital media have led to the democratization of politics and also confirmed the strong correlation between digital media and political participation and knowledge, especially during election campaigns (Dimitrova et al., 2011).

Nowadays, numerous social media platforms have brought the world together, allowing easy communication across the globe, easing the flow of the news, and creating a motley public sphere, much different and much more diverse, vibrant and virtual than the one Habermas had in mind back in 1989. Social media users have greater access to information and can now choose the outlets from which this information comes. Being the most effective means of mass communication, the internet has also changed the game of politics. With the advent of social media, this new-era public sphere is more social, diverse, and participatory and makes for a great venue or political discourse. Voices are amplified in this online space of polyphony and some social media platforms provide new ways and opportunities for political participation, among others. For example, unlike other platforms that restrain their users from passively reading their content, X allows users to engage in public speech, actively and openly express their views and ideas to each other and, contribute to political discussion. Social media also acts as an engine of activism, marshaling users to coalesce and take action around a variety of issues of public concern, such as in online mobbing that can mobilize thousands of people towards a cause, in online petitions that can quickly collect hundreds of thousands of signatures or even in trending hashtags, like *#blacklivesmatter*, that can provide some quick-fix but indicative statistics on political issues. In some platforms, anonymity also acts as a vehicle for free expression and online political participation. It is easier for users to express their opinions and ideas when they are not identifiable

and when stigma is not an option. Therefore, a context of anonymity contributes greatly to the marketplace of ideas.

On the other hand, in a context of extreme competition, nowadays, political actors and candidates can further enrich their agenda and reach a much broader audience, circulating their messages around the globe in seconds through multiple platforms. The platforms also enable them to reach users intended and not intended to receive their messages and communicate directly with voters, achieving a two-way flow form of politics, an interactive political communication between the ones led and the leaders. In addition, voter targeting has never been easier with the cookies turning political as well, with geo-targeting, microtargeting and cookie-targeting being new arrows in the political quiver.

Social media such as Facebook, X, Instagram, and YouTube constantly expose users to strong textual and audio-visual information, turning them into riveting media consumers. When political messaging is funneled through this media, the riveting flow of text, pictures, and sound becomes a political communication tool and influences public opinion more subliminally.

Of course, social media as a political discussion venue has its drawbacks. Echo chambers, for example, are closed groups where polarization is fueled among people with the same beliefs. These people are subject to selective exposure to information that converges with their interests and opinions. Radicalization and hatred emanating from the closed environments of echo chambers that create misinformation, examine only one perspective of issues, and burn any existing bridges of dialogue, let alone annihilate the possibilities of building some new ones. The production and circulation of information on the internet is largely unregulated, and social media can also contribute to the diffusion of fake news. Moreover, the latest technological advances in AI and machine learning have given rise to bots driving fake accounts, giving a new dimension to the online political stage.

7.2 Social Media: Changes in the Political Scenery and the New Generation

The emergence of social media nowadays has changed the way political communication takes place across the globe. Political institutions such as politicians, political parties, foundations, organizations, and political think tanks use almost all social media, such as Facebook and X, as a new way of communicating with their voters. This way, individuals, and politicians can express their views, control wider political networks, connect and communicate with people with shared political interests and views. The active involvement of social media users in the political sphere is an increasingly important element of political communication, particularly during political elections. Particularly today, social media is constantly changing the nature of communication because it is a tool that can potentially mobilize users in a way that has never been done before. Users are thus able to connect and communicate directly with politicians and various political campaigns, as well as to engage in political activities with new ways of communication. Simply by pressing a button, such as *like* on Facebook, or by following some users, such as on X, one can connect using new modes of communication. The ability of users to share, "like" or "retweet" various political messages opens up new horizons for politicians to reach as close to their potential voters as possible.

Furthermore, politicians have a platform to chat with potential voters, which differs from mainstream media. Politicians can reach a large number of supporters in a relatively short period by implementing social media advertising campaigns. Furthermore, the popularity of reading and evaluating political news through social media platforms is growing rapidly. This social phenomenon enables political information, whether true or not, to spread quickly and easily across digitally implemented social networks. Social media websites can also promote political participation by creating communities of shared political interests. This is why authoritarian regimes have limited social media use as tools for public political discourse, prohibiting the relaying of news or coordinating among potential activists. As open forums, social media, give voice to those

who have previously been unable to express themselves freely and, therefore, influence public opinion with their user-generated content.

Numerous social media tools help people engage in politics and express an opinion about a public issue, such as:

- **Personalized News Feeds**: The constant renewal of the list of stories appearing on each user's home page. The News Feed includes status updates, photos, videos, links, app activity, *Likes* from people, pages and groups that follow Facebook users, as well as political ads. The stories and ads appearing in the News Feed are influenced by people's Facebook connections and former activity.
- **Hashtags:** They convert themes and phrases into referrer links, announcements, chronology, or personal pages of users. This helps people find posts on topics that may interest them. To create a hashtag, all it takes is for the user to place the "#" sign in front of the word or phrase he wants to post.
- **Sharing:** Usually under postings and announcements, the option to "share" content is available. This option enables users to diffuse text or multimedia content through their own page, a friend's, or a group's page.
- **Microblogging sharing:** using short messages (e.g. 140characters long) that contain an expression of the moment or an idea. It may contain text, photos, and videos. For instance, millions of Tweets are exchanged in real time every day using X.

Facebook, X, Instagram and other social media platforms are used by individuals, countries, or organizations' representatives. In international relations, they can be used as diplomatic tools and offer possibilities that did not exist before, while giving citizens the opportunity to watch and be informed in real time about events all over the globe. For example, the Trump presidency has demonstrated a robust selection of X diplomacy, as heated exchanges have played out between government officials and foreign dignitaries for the world to follow, all in 120 characters or less. First, there was the war over the wall between Trump and former Mexican President Vicente Fox, with the latter using social media to attack Trump's repeated campaign promising to build a border wall and make Mexico pay for it. The most recent example is the escalation of hostile language between Trump and North Korea's Kim Jong Un, with North Korean officials declaring the President's tweets amount to a declaration of war.

Eventually, changes in the political scenery do not only concern beneficial implications. The spread of fake news has been and continues to be a frequent phenomenon on the internet, while social networking services have turned this scatter into a real epidemic. Fake news is stories mainly written as journalistic, but they are deliberately made to serve a purpose. More than that, bots operating like fake accounts have been developed with the purpose of manipulating or stealing data. They can, therefore, be used to influence politics from another illicit perspective.

7.3 Political Participation

Brady et al. (1995) state that political participation refers to "behaviour that could affect government action." Political participation is the activity of an individual or a group to actively participate in political life by choosing representatives and directly or indirectly influencing public policy. Political participation can be seen in several political activities, including working on a political campaign, seeking party funding, being part of a political campaign team, being a member of a political party, volunteering for political party, seeking support for a candidate, trying to persuade others, contacting politicians, donating money, joining political discussions, signing a petition, attending a political rally, and casting a vote at the election. Polat (2005) argues that the

internet may increase political participation. The internet, and social media, provide a medium to engage in politics.

7.3.1 E-participation

A term that has emerged with the transition from Web 1.0 to Web 2.0 is electronic participation (also written e-participation), which refers to the "ICT supported participation in government and governance processes." These procedures may concern administration, service delivery, decision-making, and policy-making. Therefore, electronic participation is closely linked to the participation of e-Government. The need for the term arose as citizens' interests have received less attention from service providers in developing e-Government services.

A more detailed definition considers e-participation as "the use of information and communication technologies to broaden and deepen political participation by allowing citizens to connect and their elected representatives." The definition includes all actors involved in democratic decision-making, not just top-down government initiatives. Thus, electronic participation can be seen as part of e-democracy, the use of ICT by governments generally used by elected officials, the media, political parties and interest groups, civil society organizations, international governmental organizations, or citizens (voters) within any of the political processes of states/regions, nations, and local and global communities.

The complexity of e-participation processes arises from an extended number of different areas of participation, stakeholders, participation levels, and policy-making phases.

Some applications and models have emerged as part of Web 2.0 that can be used to inspire architecture design for online participation. In particular, "the emergence of user-oriented online communities suggests that it is possible to design socially mediated technology that supports public government partnerships." Some of those applications and mechanisms are the following:

1. **Blogs:** The blog is a website listing entry from the most recent entry to the oldest. The content of the entries can be anything like news, political and social commentary, media and celebrity commentaries, personal diaries, and special issues such as technology, arts, fashion, sports, and gastronomy. It does not require technical expertise to build a blog today, as Google and other providers offer their users free blog building and hosting.
2. **E-voting:** This refers to electronic voting and is the voting procedure that uses electronic means to help or arrange the casting and counting of votes. Depending on the application, electronic voting can use standalone electronic voting machines or computers connected to the Internet. It can include a range of Internet services, from basic results-based transmission to complete electronic voting via shared home appliances. A remarkable electronic voting system must carry out most of these tasks while adhering to a set of standards established by regulatory bodies and must also be able to successfully meet the strong requirements related to safety, accuracy, integrity, speed, cost-efficiency, scalability, and ecological sustainability. Electronic voting technology may include perforated cards, opt-in voting systems, and specialized voting kiosks (including stand-alone electronic voting systems with Direct Record or DRE). It may also include ballot and vote casting via telephones, private computer networks or the Internet. In general, two main types of electronic voting can be identified:
    - Electronic voting, which is subject to physical oversight by representatives of governmental or independent electoral authorities.
    - Remote electronic voting via the Internet (also called i-vote), where voters cast their votes electronically to election authorities from any point.
3. **Reputation systems:** These programs allow users to evaluate each other in online communities to build trust through reputation. Some common uses of these systems can be found on e-commerce

sites, such as eBay, and Amazon.com, as well as in online consulting communities, such as Stack Exchange. These reputation systems represent an important trend in "support for support for internet mediation services."

4. **Online petitions:** An online petition (or e-petition) is a form of submission signed electronically, usually through a form on a website. Visitors to the online report sign the report by adding their details such as name and email address. Since there are several signatories, the resulting document can be delivered to the report's subject, usually by e-mail. The e-petition can also deliver an e-mail message to the report's target each time the report is signed.

The very nature of democracy suggests that free and open communication through various channels is necessary to foster critical practices in democratic societies. According to this argument, social media in a stable democracy can be principal institutions for citizens to understand their society better. Ideally, social media can contribute to the public sphere by providing citizens with information about their world, fostering debate about various issues and encouraging informed decisions about available courses of action. Social media is also a site of contestation in which diverse positions are advanced, significant opinions are heard, interests and inner workings are exposed, and input is received. These all contribute to public debate and the shaping of the daily agenda.

Increasingly, political actors are investing in social media to expand their means of reaching an electorate, especially during election campaigns. At a time when low participation rates and electoral discomfort towards their institutions and political representatives are expressed by Western citizens, especially among young people, the use of social media becomes a means that always has the potential to revitalize the political sphere and civic engagement (Clarke, 2010). Barack Obama's election campaign in 2008 had a great impact, through his effective use of social media (Carpenter, 2010), and other political leaders have been trying to draw inspiration from this model, which has become a common practice. Obama won by nearly 200 electoral and 8.5 million popular votes. A major success factor was how Obama's campaign used social media and technology as an integral part of its strategy to raise money and, more importantly, to develop a groundswell of empowered volunteers who felt they could make a difference. Obama won by converting everyday people into engaged and empowered volunteers, donors and advocates through social networks, e-mail advocacy, text messaging and online video. By November 2008, Obama had approximately 2.5 million Facebook supporters, outperforming McCain nearly four times. Obama had over 115,000 followers on X, more than twenty-three times those of McCain.

Social media, is, therefore, part of political communication strategies. X has more and more registrants, including many politicians who have seen it as an additional means of communication (Small, 2010).

X and Facebook (to a lesser extent) are particularly suited to the aspirations of politicians who want, above all, to increase their attractiveness (Cozma, 2013) and federate the goodwill around their program: "Regular Twitter users are educated, tend to be in their 30s and hold a position of responsibility, all of which is good for engaging decision makers." From its introductory age, X had the potential to reach a large number of potential voters, during election campaigns and in the exercise of power, thus accrediting the myth of direct electronic democracy that we see resurging at each election as a "snake of the sea." "Twitter has been lauded by proponents of democracy for being able to engage" average citizens "in the political process" (Bekafigo & McBride, 2013). X and Facebook also have the advantage of extending their potential to communicate with citizens, and to encourage them to commit themselves: "new information and communication techniques perpetuate themes of local democracy, transparency of decisions, citizen participation." Reinvigorating political participation (Small, 2011) X and Facebook also increase the feeling of proximity, that is, "immediacy of interpersonal communication" between the population and the professionals of politics. Both platforms' contributions to the online political realm will be outlined in the following paragraphs of the chapter.

7.3.2 Youth Political Participation

Nowadays younger generations can take on an increasingly active role in politics, due to increased political news diffused in various types of social media and the high number of young users globally. Younger generations are, therefore, exposed to politics in a way integrated with their online social life.

The creation of Facebook pages, groups, or X Accounts is always a priority when wanting to approach a younger audience. Studies and recent elections have shown that active politicians on social media are more likely to be elected. Traditional political figures are not very fond of the social media concept because their statements can easily be fact-checked by eager youngsters who advocate for more transparency in the field. Additionally, young people will research the politician's background to form a more objective opinion about their politics and life, which may be an advantage or disadvantage for the audience they are trying to gather. (Weeks, Ardèvol-Abreu & Gil de Zúñiga, 2015) The feedback they are getting can help change some policies and be more transparent to the average young audience. These individuals who are highly focused on obtaining as much information from social media platforms as possible, are more likely to be informants and engage in political participation. It has often been observed that young people with a strong online presence in youth groups are more likely to help shape the political attitudes of those around them, whether online or offline. The simplicity of social media allows individuals to approach or be approached by those who are active in the topics they are interested in and hold discussions, conversations, and communicate with an ease that has not been apparent in many traditional ways of participation, resulting in a more willing participation from the young generation. (Weeks, Ardèvol-Abreu & Gil de Zúñiga, 2015). It is much easier to engage in conversations and research topics that one is interested in using a smart phone or a desktop computer than being involved traditionally.

In general, the Internet has become a dominant force in how campaigns are being cultivated, how information is approached and shared, and in how perspectives are discussed. Youth policy now includes an electronic component, as explained by *Black Lives Matter*, the *DREAMer* movement, and countless other examples. Taking part in a demonstration is easier than ever before. Most of the demonstrations and petitions now take place online.

Another point worth mentioning is that social media, as of today, appears to be a more neutral form of communication and information since most of its content is not owned or influenced by big media corporations. However, the content shown should be further researched since it is often only peer-viewed and not thoroughly checked for misinformation. Most young people prefer this source of information because of its independent nature and sheer unlimited source of content, accessible by all groups of people and of course, very interactive in nature. Young people tend not to go through media outlet's sites for information anymore since the content seems biased towards a specific type of audience that does not cater to their interests. A study conducted by Kahne showed that about 41% of the participants had partaken in a political discussion, poetry slam blog, or another form of participation in the last year, and about 45% participated in a more traditional way of going with political parties or donating to an institution. Also, those were the ones who wanted and did indeed vote (Kahne & Middaugh, 2012).

In participatory politics, it is important that the youth can also have a say in politics and sway away from the traditional forms, modernizing how they share their political views. Those who participate and try to influence their peers also help make campaigns and content more creative and interactive, forcing traditionalists to adapt and modernize their programs to attract the youth. Some more conservative and old-fashioned parties see themselves hiring young social media managers to adapt to the modern form of online presence. The youth can be creative with sharing speeches, new adapted policies etc., by using digital media and programs to make the content of the ideas they support more creative and thus get a broader range of participants and increase political participation (Kahne & Middaugh, 2012).

Eventually, it is worth noting that due to the Covid-19 pandemic, social media activity more than doubled for young people since many of the students could not go to school and had more time to consume political, among others, online content across all platforms.

7.3.3 Virtual Political Communities

The amount of information that can be disseminated through the web, the fact that computers have shrunk to the size of handheld smartphones with mobile and perpetual connectivity, and the decentralized character of the Internet have created a fertile ground for people to communicate and express their views on nearly everything, including politics. These factors, combined with the introduction of social media, gave birth to virtual communities. This peer-to-peer mediated communication has provided forums of political action and shaped a renewed public sphere. As the boundaries of offline and online lives blur, online discourse and connections have become vital to understanding politics. Individuals express themselves, inside these networks with examples that vary between heated speech and real political mobilization. Digitally enabled actors and groups create new forms of organization and sometimes have different objectives from the current institutions of the international system. Social media alters the political scale by shifting who controls information and how this information is distributed to every specific user, first, by enabling online users to select their social network, virtual communities, and content to avoid any opposite political standpoints. Second, the networks do not dictate that their users follow specific political views, allowing political actors, including candidates, to shape their content.

Understanding how virtual communities affect political expression and communications is an important issue. The expansion of social networking sites like X, Facebook, Instagram, Reddit, and generally the blogosphere, with political content, is remarkable even by the modern Internet growth standards. Parties, candidates, and even Prime Ministers are using X to communicate with their supporters and almost always answer back to their political enemies. While Facebook and X are the main sites that come in mind when we speak about virtual communities, the reality is that the Internet is full of similar networking sites.

This ability to personalize the user´s online experience based on exactly what they favor is the cornerstone of the success of such sites. Giving the consumer what they crave is essential to doing good business. However, the possible implications of having access only to views you favor may result in echo chambers with significant consequences in the political sphere. Furthermore, the recent scandals (Cambridge Analytica -Facebook) considering privacy breaches and commercialization of online preferences made many people lose their faith and question who and when they should share their personal interests and views. Virtual communities may seem like an open book; however, this virtual transparency is not something to be taken for granted because they never cease to be corporate entities with specific financial goals, managed by individuals with personal ambitions. Consequently, knowledge of these virtual communities remains limited because of the circumstantial factors and the technicalities that refer to each case. Some scholars embrace the use of these communities for expressing political thought. In contrast, others are very skeptical about whether their online presence can shape someone´s political thinking and, if so, how much it can change.

In the past, the most common conceptualization of communities was that they were fixed, stable, and geographically bound. This whole concept of community was transformed after the transition from the class-based system of the past to the information-based global economy. This information society may connect people and companies on a global scale but may also segregate them as some psychological studies have proved. They have shown that increasing Internet usage is associated with higher risks of developing depression and loneliness. No matter that people view their interpersonal interaction in cyberspace as authentic and their friendships and acquaintances that develop online as real. The question is whether these networks are meaningful enough for their members to develop a real political sphere inside them (Owen,

2015). In contrast to that, the fact that most people have different online and offline identification and can remain anonymous is not something that can benefit the development of strong interpersonal ties and help bring to the surface someone's true political standpoints. However, on the other side, this anonymity provides a sense of security that allows the individual to express their true opinion and act against a specific group without fearing retribution from its members. This controversial issue cannot be resolved at the moment, but the truth is that more and more people are joining the political debate online, and corporate social media platforms increase their member count every second.

To conclude, many scholars have focused on how virtual communities formed within Web 2.0 applications affect the creation and expression of political views, governance, and campaigning. A major change is witnessed in the political sphere. Some may suggest that these changes are inevitable consequences of adopting technology. Some of them are just alterations of the behaviors of the past, but one thing is certain: active political players, even if they are heads of state or just regular citizens, are now closer to virtual communities than ever before. Successful political actors are harnessing all this technological progression, leaving the ones needing help to adopt it behind. Older politicians and strategists may prefer obsolete models that worked in the past, but as politics as a process is perpetually evolving, campaigns will readjust themselves to the prevailing conditions. From the citizen's point of view, social media may not be the panacea for democracy, but it creates opportunities for open interaction and a more free and effortless participation. Individuals who become active online and constitute virtual communities have developed a sense of attachment with their fellow group members and sometimes formed their audience, leaving behind the sense of alienation they felt in the past when interacting with the government or other political players. One thing is for sure: the Internet is not static and neither are political actors, so consequently the study of Web 2.0 Communities is paramount for a better understanding of the political world.

7.4 Social Media Applications for Politics

From what has been stated above, the prominence of social media has been particularly highlighted in politics, as it is clear enough that the use of social networking sites, such as Facebook, and microblogging services, such as X, are believed to have the potential of positively influencing political participation.

Facebook is a social networking site founded in 2004 by Mark Zuckerberg to be used by Harvard students. Rapidly, it gained worldwide popularity, and today, Facebook represents the most used social networking site, with over 1 billion users worldwide. X is a free social networking microblogging service that allows registered members to broadcast short posts called tweets. X members can broadcast and follow other users' tweets using multiple platforms and devices. Tweets and replies to tweets can be sent by cell phone text message, desktop client, or by posting at the X website. These two platforms and a few more will be presented below from their political perspective.

7.4.1 X

X was founded in San Francisco by Jack Dorsey and other associates in 2006. It started as an urban lifestyle tool for friends to update each other about their whereabouts and activities, the so-called tweets. While X has some similarities with other social media platforms, it also has some essential differences that set it apart such as (Colona, 2002):

- The customizability of messages by tagging them for people using the @ symbol, an action called tagging.
- Users may post short messages (tweets) of up to 140 characters.
- Categorization for messages with hashtag (#) keywords.

Along with interpersonal communication, X is also increasingly used as a source of real-time information and a place for debate in news and politics. The importance of hashtags has been displayed on many occasions since the creation of the platform. One such instance was the protest of the Spanish Indignados, also known as the 15-M movement. Through the campaign *No Les Votes* (Don't Vote for Them), they were asking people not to vote for any of the three major parties responsible for a hotly contested bill, which are accused of attacking digital freedom in favor of media lobbies (Zavadskaya, 2015). The Spanish indignados displayed great skill when it came to the use of these new technologies. According to Zavadskaya (2015), what causes a striking impression about the 15-M nano stories is how successfully leading activists used X in the build-up of 15th May protests across Spain. Through the use of X hashtags such as #15M or #15mani, *DRY* supporters were able to rally the protesters at short notice, and they were also able to set the changing political and emotional tone of the campaign. While these nano stories may be short-lived, each can play an important role in the struggle context within which it is shared. On a different note, the University of Edinburgh analysis has included an exploration of X use in relation to some geo-political events (**Figure 7.1**). This looked at global X use during critical periods of the Syria and Ukraine crises in 2013 and 2014, analyzed tweets and re-tweets made in the English language, and was able to create heat-maps showing where certain topics were discussed, as well as the overall positive or negative attitude to those topics, country by country (Donaldson, 2016). Moreover, and enlighteningly, it used the net balance of international re-tweets as a measure of influence.

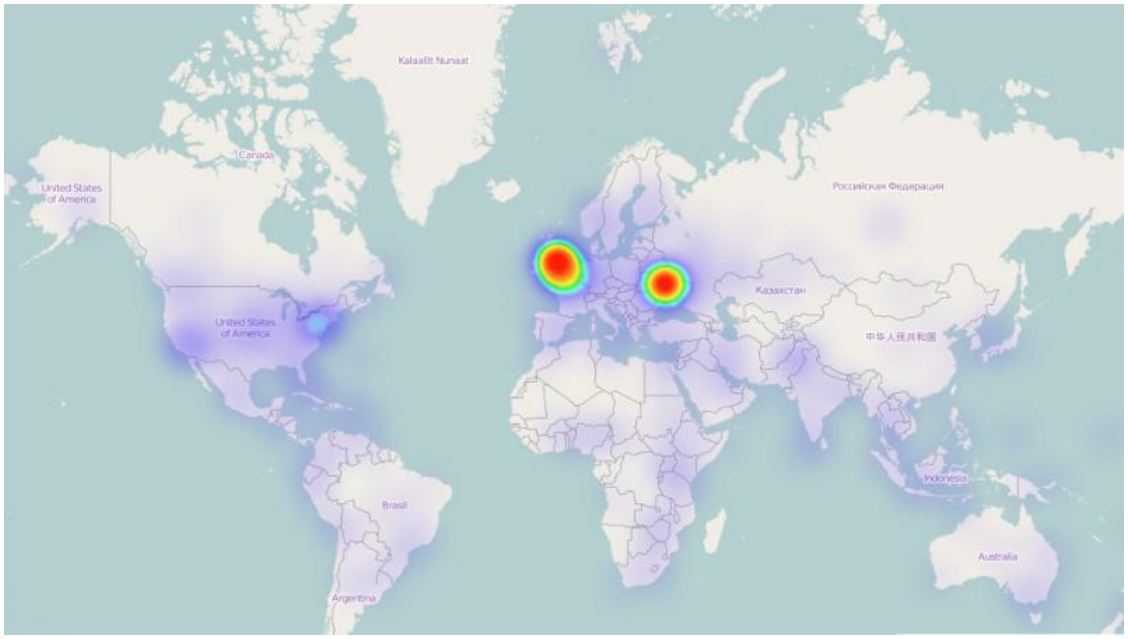


Figure 7.1 *'Heat-map' showing the origin and concentration of tweets in English mentioning Ukraine during the week of 20-27 June 2014. (Source: Courtesy of the Department of Informatics, University of Edinburgh, www.britishcouncil.org, 2016.)*

This analysis yielded results that showed the UK, during those tumultuous times, was one of the largest net exporters of tweets via re-tweeting. In addition, the "cumulative clout" of the UK per capita on X was higher than for any other country. In addition, the UK was viewed favorably in tweets about Ukraine. On these grounds, the UK could be said to be a net exporter of opinion and influence during these recent international events.

Another way of using X politically is for governments to communicate with the public. In the US for example, when the administration announces a major policy or wants to bring attention to a particular issue, it tweets it. According to Colona (2002), in an illustration of open government, the White House Press secretary will take questions from the public sent to him on X and respond using that service. So, all in all, X's virtue is

simplicity due to its character limitation. While a tweet may be clever or witty but never complex, it can promote impulsivity by allowing for tweeting from virtually anywhere at any time (Ott, 2017).

The former US president, Donald J. Trump, "had fully integrated Twitter into the very fabric of his administration, reshaping the nature of the presidency and presidential power" (Shear, 2019). According to a seven month-long-study from October 2015 to May 2016, based on more than 2,500 tweets from @realDonaldTrump, it was found that (Ott, 2017):

- Trump's lexicon is simple and repetitious, relying heavily on monosyllabic words such as "good," "bad," and "sad."
- Trump's Tweets are overwhelmingly "negative in connotation—and the majority of them are outright insults."
- Trump makes frequent use of exclamation points and all caps, such as in the following tweet: "Why doesn't the failing @nytimes write the real story on the Clintons and women? The media is TOTALLY dishonest!".

Additionally, X was an essential part of Trump's foreign policy as he has praised dictators more than a hundred times, complaining nearly twice as much about US traditional allies (Shear, 2019). Moreover, he often used X to lash out at his perceived opponents, and reportedly, more than half of his tweets were attacking someone or something.

From another point of view, some studies show that X contributes to political polarization or encourages the practice of self-segregation. A 2011 paper for the Association for the Advancement of Artificial Intelligence (AI) titled "Political Polarization on Twitter" strongly supports this claim (Conover, 2011). The study looked at the "retweets" and "mentions" that were politically relevant for conservatives and liberals during the 2010 midterm elections in the US. The study found that users usually retweet people with whom they agree while they only give mentions to those with whom they disagree. Retweets serve as ads, while mentions find a middle ground between distinct ideologies. Another important finding of this study was that those with mixed ideologies tended to be mentioned much more than those who lean only to the right or left. So, at least on X, those in the middle can try to lead, influence, or encourage more balanced discussions. Most importantly, the study concluded that mentions outside one's political ideologies could worsen polarization because they reinforce pre-existing political biases. This drives and delivers a critical point that puts in doubt the claim that social media eases polarization through mere exposure. "The fractured nature of political discourse seems to be worsening, and understanding the social and technological dynamics underlying this trend will be essential to attenuating its effect on the public sphere," concluded the authors (Conover, 2011). While there is "substantial cross-ideological interaction," it may make matters worse, suggesting that X users might be less politically polarized if they never interacted with people with whom they disagreed.

X was also used to rally, recruit, and encourage people to show their solidarity with protestors. In other instances, it was used as a broadcast medium, a technology that allowed the protesters to tell their side of the story. In the Egyptian revolution and under the hashtag #jan25 created by a twenty-one-year-old woman, X became the mediated eyes, ears, and voice of the day-to-day life of the protest and was used in various ways during the protest. At times, it was used as a tool for real time communication between protesters, informing each other about the localization of police, where protestors should go, and what media around the world were saying about the events on the ground. X did not start the revolution, but it did help generations of Egyptians realize a world that would have been impossible to imagine not long ago.

Another case demonstrating how young people have used X to spread awareness about an on-going issue is the Rhodes Must Fall (*RMF) campaign*. In this particular case, the students of the University of Cape Town organized a protest campaign whose goal was to remove the British colonialist Cecil John Rhodes' statue from the university grounds in a protest against racism and the culture of black exploitation that seemed to

be apparent in South Africa. This case showed a consistent pattern that appears to be used in many campaigns that aim to engage young people across the globe. With the use of hashtags, the users tried to gain traction and get the attention of mainstream media to the topic. This issue became a trending topic globally, which soon achieved the desired result. Many X users caught wind of the protest and pressured the authorities to take this matter seriously. X's use demonstrated how it can get people who might not be aware of this issue to form an opinion without engaging in a formal protest. The youth who get engaged in such cases exchange and promote flaming problems and concerns that have arisen. At the same time, X allows them to potentially practice their activism and thus participate in a political process. (Bosch, 2021).

7.4.2 Facebook

Facebook was founded in 2004 by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes, all of whom were students at Harvard University. Facebook has been a social networking sites that has taken over the political compass in the last 15 years. It has become one of the major outlets for sharing political opinions or events and for politicians and parties to interact with their audience and reach as many people as possible. After all, the interest in political participation, especially from youth, has recently become a focal point of campaigning. While traditional means of participation still hold a certain amount of value in the democratic process, to this day, rather than the current means, having a cross-platform profile is commonly accepted.

One of Facebook's qualities that give the impression of being one of the points that grab and hold a young person's attention is its interactivity features. Even though traditional participation can be interactive, it will never reach the levels of its online counterpart, which is constantly on the rise. Facebook delivers information to the user in a more understandable, compact, and interactive way, which in return catches their interest. Many users will scroll through their feed and stumble upon topics that their friends or a news site have shared and read through. Through posts, status updates, events, and political groups, the users can enjoy the easy layout and get connected, not only with those on their friend list but with other people around the globe in order to exchange ideas, point out current issues or support one another, something that has proven to have increased the levels of political and civil participation and interest. Studies have shown a direct link between Facebook usage and online and traditional political participation among young users (Stieglitz & Linh, 2012).

Additionally, it is important to mention that youth political participation has increased in recent years because of their direct interaction with politicians and groups in which they are particularly interested. Facebook allows politicians and citizens for direct dialogue through their comment section and private messaging, allowing them to exchange concerns about various topics. Many traditional politicians leaped into social media to attract this younger audience and keep them politically engaged in their party in the future. This action gives the users a feeling of familiarity and friendship, which, as a result, can increase participation and interest and may influence their political beliefs so that, in the long run, they become future voters of their parties (Sandlow, 2021).

While other social media platforms have been used to obtain political information, Facebook appears to be the preferable platform for political participation compared to X, Snapchat, Instagram, and others. One of the cases in which the influence of Facebook in political participation is visible was the 2020 US Elections. The youth turnout increased by almost half compared to the 2016 elections. Not only were the youth more interested in participating in the upcoming elections, but an increase in general political participation was also observed (**Figure 7.2**). In the case of the elections, Facebook was one of the social media platforms that advertized the elections a year in advance. There was an attempt to make the elections more tempting to the younger audience and, in the end, show them that it is vital to use their constitutional right to vote. The increase in social media usage helped with voter turnout and, in recent years, the more considerable

mobilization and sensitization on global issues, such as the environment, the rise of racial injustice, and the widening gap between the poor and rich.

Another demonstrating example was President Obama's extraordinary success in the 2008 presidential election. Back then, the most popular social media in the United States was Facebook, estimated to have one hundred and twenty-five million active users. Three-quarters (74%) of internet users went online during the 2008 election to participate in or get news and information about the 2008 campaign. This represents 55% of the entire adult population and marks the first time the *Pew Internet & American Life* Project has found that more than half the voting-age population used the internet to connect to the political process during an election cycle. Some 38% of internet users talked about politics online with others throughout the campaign, sharing or receiving campaign information using specific tools, such as email, instant messaging, text messages, or X. A full 59% of internet users used one or more of these tools to send or receive political messages. As the online political news audience has grown, the importance of the internet has increased relative to other news sources.

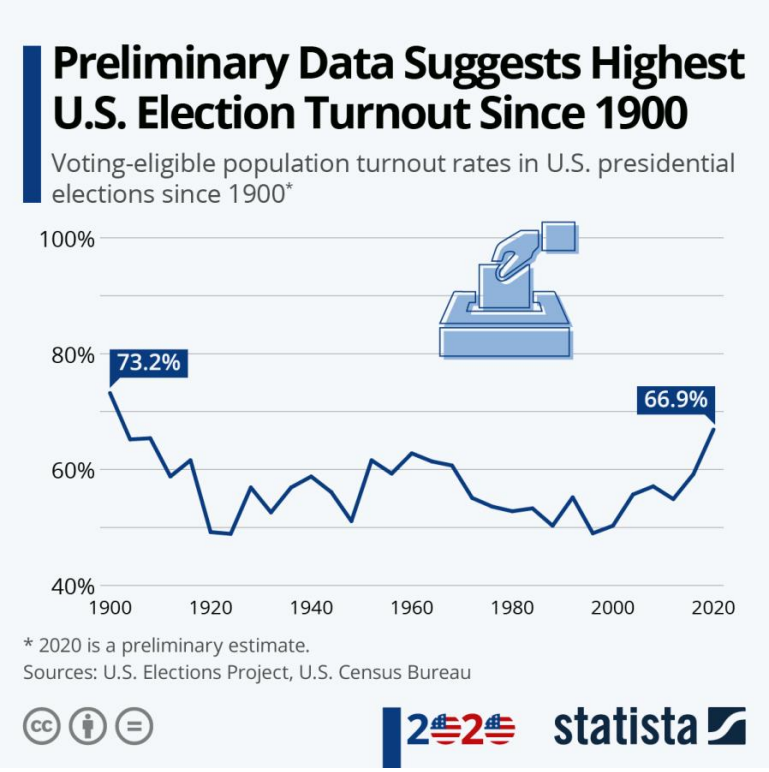


Figure 7.2 *US Election Voter Turnout since 1900. (Source: https://www.statista.com, 2020)*

Although Facebook is one of the most popular platforms for political participation, it appears to have some intriguing aspects. Research done in the US by Joshua Bleiberg, an analyst at the Center for Technology Innovation, and its founding director, Darrell West, suggested that Facebook users create some political bubble when constructing their social network and choosing whom they befriend (Bleiberg & Darrell, 2015). The study revealed that roughly speaking, an average user has five like-minded friends for everyone they have with dissenting political views. This number is much lower than one would like a citizen to encounter inside a democracy, nor does it help the polarizing tendency in America. Also, the Facebook News Feed tries to make the website more enjoyable for the reader. This means that users who often click on partisan news or links will have higher chances of encountering more of those in the future. This can have unintended consequences. For example, “The authors find that the news feed algorithm reduces the politically cross-cutting content by 5 percent for conservatives and 8 percent for liberals.” One of the main issues regarding the algorithm is that

many users consume news content that confirms their beliefs. Hence, individual decisions play a big role even when controlling for where in the newsfeed stories appear. As stated in the study, “the authors estimate that user choice decreases the likelihood of clicking on a cross-cutting link by 17 percent for conservatives and 6 percent for liberals” (Bleiberg & Darrell, 2015).

The study does not present the findings in a way that separates the effects of the algorithm and individual choice. Both factors certainly influence each other. The impact of individual user choices is more significant than the news feed algorithm. Political and social scientists fear these characteristics make social media an 'echo chamber' of the user’s beliefs. It is up to Facebook to modify its algorithm in order to reduce the polarizing effect it might have. This could also add to the trust users have in the company.

Studies have shown that young voters between 20-29 acquire information from sites such as Facebook, X, or YouTube. "Facebook announced it had registered a record of 4.4 million people and expects 160 million more to have seen information about how to vote thanks to its presence on their news feed" (Pastor, 2020). Finally, according to studies, Facebook is a platform for young people not content with the current political situation (Halim et al., 2021).

7.4.3 Instagram

Instagram is an American photo and video sharing social networking service founded by Kevin Systrom and Mike Krieger in 2010. In April 2012, Facebook Inc. acquired the service for approximately US$1 billion in cash and stock. Instagram has become the fastest growing social networking site for politicians (Financial Times, 2019). Indeed, 81% of the leaders of the 193 United Nations member states are active on this platform (Twiplomacy.com, 2018). On April 16, 2020, the most followed leader was Narendra Modi (Price Minister, India (@narendramodi)) with 38.9 million followers. Then, Joko Widodo (President, Indonesia (@jokowi)) with 30.6 million, and finally, Donald Trump (President, United States (@realdonaldtrump)) with 19.1 million followers.

Instagram is mostly used by young people. Indeed, in January 2020, the platform had 35% of its users between the ages of 25 and 34 worldwide. "Over two thirds of Instagram audiences were aged 34 years and younger" (Clement, 2020). Politicians need to define the target audience and public relations (Solo, 2014), as Instagram reaches a wide variety of audiences. The platform offers a multitude of different functionalities and options, and politicians use them to carry out their communication strategy best.

Politicians use Instagram primarily to engage young voters (Twiplomacy, 2018). Diplomats try to assimilate a more millennial aspect on the platform, changing their image, which young people may perceive in other media such as newspapers, television, or radio (Serafinelli, 2018). Politicians post photos showing their lives beyond politics, using the full range of Instagram options, including emojis, stickers, and live videos.

Instagram remains the platform where stories make the difference among all social networking sites. Initiated by the company and the Snapchat application in 2013 and taken over by Instagram in 2016, this feature allows users to share moments of their daily lives without overloading their news feed. Compared to Snapchat, users have easier access to stories, even if they are not following the person who posts them. Stories are used as a strategic tool to make the content more attractive and fun.

Indeed, the stories allow for photos and short videos to be added, staying online 24 hours (or even to keep them in the “Highlight” category above the field), with the possibility to add text (different fonts, colors, sizes), emojis, stickers, filters, date, geolocation, or tags with hashtags. Politicians can also tag other people by using and writing “@” before the username and adding a direct link to their stories. This link allows followers to click on “see more” which can automatically redirect them to this link. This allows for fluidity in their content and makes a more attentive and participating audience.

Moreover, one of the main strengths of the stories is that politicians are not confronted with public comments and user interactivity, which could be detrimental to their image. Moreover, stories on Instagram allow for the chronicling of daily activities (Twiplomacy.com, 2018). For example, during her business trips, Angela Merkel summarizes her activities via stories. In January 2020, the Chancellor went to South Africa. The stages of her trip were meticulously presented, from her arrival to her departure. In addition to 'live' videos and photos, animations are added to have more attractive content: places, texts, and tags. Finally, Stories encourages users to check their feed regularly to be updated of other activities.

Due to Instagram's preference for visual content over narratives, world leaders have used this to showcase their creativity and proficiency with the platform by creating collages or photo montages related to their fields (Twiplomacy.com, 2018). However, some politicians decide to use Instagram differently. In addition to the published photos and videos, they insert screenshots of their tweets initially posted on the X platform. Donald Trump and Giuseppe Conte do this, which allows them to gain much more engagement (Twiplomacy.com, 2018).

Politicians take the platform to present themselves in a more accessible way. Trying to offer followers new ways to identify themselves, politicians try to balance between institutional facets and spontaneity by using Instagram as a tool for proximity. Followers have access to the politician's lifestyle (Jung et al., 2017), and Barack Obama initiated the trend of politicians who share their professional and also personal moments by posting photos with his family and friends, sharing love and friendship. In France, Benoît Hamon (@benoit_hamon), leader of the political party *Génération*, uses other means, posting selfie photos and videos. In addition to his professional life, his intimate and daily life is much in evidence: places visited, tastes, interests, and even humorous stagings through photos with his cat.

Descriptions that accompany photos and posted videos are supporting the visual aspect. Politicians can write whatever they want to spread their ideas and opinions. It should be noted that the platform allows only 2,200 characters and that the longest content is the most engaging (Coëffé, 2017). A picture posted on April 7, 2020, by Barack Obama shows a business meeting between him and Cecilia Munoz (@barackobama). Although he is no longer president, Barack Obama now uses Instagram and continues his fight to spread his convictions, such as human rights, immigration, and the power of women, especially black women.

7.4.4 Reddit

One example of a diverse online community is Reddit. The site was launched in 2006 (Heimans & Timms, 2018) and for a long time, was only popular among programmers and engineers, which is why it has a stripped down and not so appealing user interface. Nevertheless, over the years, it broke into the mainstream, and it is now known for its decentralized nature and diverse user community. The wide variety of subreddits creates opportunities for raising attention and fostering discussion across various areas. Individual mobilization is highly present on the site in philanthropy, activism, political expression, and even sometimes commercial activity. It is known for its political engagement, especially in the US elections with candidates like Barack Obama, Donald Trump, and Bernie Sanders using it for political gain. Some candidates even made *r/IAMA* (IAMA is a *subreddit* for people to show up and directly answer to other people about their life and career) appearances so that they get in touch with possible voters during their campaign. For example, Obama was one of the first to get in touch with voters through Reddit because the site´s demographic profile was the type his strategists identified as advantageous. Indeed, as an illustration of how effective their decision was when Obama posted a URL with the form to register to vote, 30,000 Redditors did so (Strommer-Galley, 2014). Furthermore, Redditors have also shown radical mobilization when protesting the Online Privacy Act. Users had the idea to stop the site´s function as a sign of protest against the senate bill. This incident created a wave of support from other sites, like Wikipedia. Finally on January 18th, 2012, they all went black, with the news

of that creating national headlines and raising awareness worldwide, proving once more the effect that a populous cyber community can produce (Beyer, 2014).

7.4.5 The Political Blogosphere

Political blogs grew more, especially after the events of September 11, 2001, when people turned to blogs to share their feelings and opinions about the tragic terrorist attack in the US. The military activity in the Middle East boosted blogs' activity even more by turning posts thematic to war and political issues. Very early, mainstream media started to recognize the blogs' power as well as the impact of political blogs. Journalists and corporations started to use political blogs to influence, diffuse messages, and shape public opinion as well as the daily agenda. (Kuhn & Crew, 2006)

As the blogosphere has grown, many political newspapers and magazines have created blogs. Bloggers have changed how politics work, affecting campaigns, spreading allegations, and even causing scandals. Political blogs challenge politics by giving power to the people. It was the first Web 2.0 application that Campaigners used for disseminating messages, recruiting, and attracting supporters and donors. Numerous stories and incidents have demonstrated how blogs have affected and played a crucial role in politics (Cornfield, 2004).

An example underlining the blog's potential role in politics is the case of 2006, when bloggers in the US participated and helped Senator Joseph Lieberman lose the democratic primary to businessman Ned Lamont. Joe Lieberman was a former member of the Democratic Party, and he was also nominated for Vice President in the 2000 elections. In 2006, Joseph Lieberman lost to Ned Lamont in the Democratic Party primary elections. Even though the Democratic establishment was supporting him against Ned Lamont, who was not as well known in public as Lieberman was, the bloggers and voters in Connecticut ensured that Lieberman was kicked out of the party. Voters in Connecticut and bloggers got angry because of Lieberman supported the Iraq war and because of his party's opposition to President Bush's policy and actions there. One former blogger and internet organizer got involved in Ned Lamont's campaign against Lieberman. Many bloggers came to Connecticut to show support for Lamont by calling potential voters to encourage them to vote for Lamont. Bloggers used many tactics to achieve his loss; for example, they convinced candidates to donate excess campaign funds to vulnerable candidates. Bloggers even used Google to accomplish what they had started by hyperlinking to negative stories, so when someone looked for the name Lieberman, only negative results were listed. When Election Day came, bloggers were still working against Lieberman by reporting about polling problems and voter intimidation. As a result, Lieberman lost the elections (Farrel, 2008).

This primary win shows what blogs can achieve. Together with social networks, blogs can change politics. Through the years, blogs have gained respect throughout the world, and now they have been considered as something more, as something that has power.

7.5 Campaigning

As noted, digital media and their use for political mobilization are widespread (Sweetser et al., 2015). The process of using digital media in election campaigns first appeared in the Clinton campaign in 1992. At that time, the Internet was not broadly used and the impact was less pronounced. However, information about a pre-election campaign was posted on the new medium for the first time. This was the beginning of the Internet as a campaigning means to stimulate political mobilization, as by the next election in 2000; since then, it has been established as a "common campaigning tool." Therefore, the 2000 election was seen as the "first election on the Internet."

In 2004, the use of the internet as a political tool shifted from an information to a campaigning medium. In 2008, new digital tools such as social networking or microblogging played an active role in the Obama campaigns. Back then, fifty million viewers spent 14 million hours watching campaign-related videos on YouTube, four times McCain's viewers. The campaign sent 1 billion e-mails, including 10,000 unique messages targeted at specific segments of their 13-million-member list. The campaign garnered 3 million mobile and SMS subscribers. The campaign's social network, www.*my.barackobama.com* allowed individuals to connect and activate themselves on behalf of the campaign. Two million profiles were created. Registered users and volunteers planned over 200,000 offline events, wrote 400,000 blog posts, and created 35,000 volunteer groups. Obama raised $639 million from 3 million donors, mostly through the Internet. Volunteers in www.*my.barackobama.com* generated $30 million on 70,000 personal fundraising pages. Donors made 6.5 million donations online, totaling more than $500 million. Of those donations, 6 million were in increments of $100 or less, the average being $80. The average donor gave more than once. The campaign used these tools more effectively than other candidates to organize, communicate, and fundraise, and leveraged them to support its grassroots strategy that tapped into the hearts of the voters. What resulted was both a victory for the Democrats and Obama and the legacy of one of the most effective Internet marketing plans in history, where social media and technology enabled the individual to activate and participate in a movement.

In 2016, digital media was the primary source for the mobilization and organization of Trump supporters. Nowadays, no candidate or government campaign can take place without having Internet presence. From very early, it became clear that the Internet is expected to increase exponentially regarding all aspects of political campaigns " (Dimitrova et al., 2011). According to the Encyclopedia of Political Communication, tools such as blogging, podcasting, political websites with mechanisms for online feedback and participation, social networking, and video sharing on the Internet are considered critical to political communication (Dimitrova et al., 2011). All in all, the cost of participation for citizens is reduced both financially and in terms of time and effort. The internet allows participation on a 24/7 basis and provides access to a wide range of information anywhere, compared to traditional older media. The rich information availability has created a widely informed society and electorate, providing fertile grounds for political campaigning (Dimitrova et al., 2011).

7.5.1 Political Communication

The goal of strategic political communication during election campaigns is to use information and communication as strategically and effectively as possible to reach the objectives set. The strategic goals of parties and campaigns are thus imperative, which suggests that understanding strategic political communication during election campaigns requires understanding political parties and campaigns as organizations. These features influence the priority of campaigning and communication, and how the parties plan and run their campaigns.

At the same time, campaign practices and communication are always dynamic and shaped by the circumstantial conditions formed by the political system, the media system, laws, and regulations, the political culture, and the type of parties and party competition. Therefore, what works in one context may only work in that context. While there are cross-national patterns in campaign practices and communication, more detailed analyses usually reveal that this is due to country differences. Hence, while it is important to identify trends, the country state is crucial and requires re-adjustment to innovations and import of campaign practices.

Social media plays an increasingly important part in the communication strategies of political campaigns by reflecting information about the policy preferences and opinions of political actors and their public followers. In addition, the content of the messages provides rich information about the political issues and the

raising of the issues during elections. As shown earlier in the chapter, several platforms nowadays are widely used by politicians for personal promotion, diffusing policy positions, mobilization, and because they enable a more direct and interactive engagement with the public.

7.5.2 Electoral Campaigns

Election campaigns fundamentally rely on communication. Over the last decade, changes in the communication environment due to innovations in digital technologies, which accompany modernization and professionalization of electoral competition, have forced political elites to adopt and integrate their campaigns with increasingly sophisticated digital communication practices-faced with a sharp decline in party membership and a more demanding, assertive, and distrustful public increasingly willing to intervene directly in the political process (often through the use of digital media-enabled personalized forms of participation), political parties and candidates embraced new online tools as part of their campaign communication. Social networking sites like Facebook, microblogs like X, and video-sharing sites like YouTube have not only given politicians a powerful channel for interacting with a more demanding society, but also have allowed them to offer more personalized images to the public and have allowed less resourceful parties to match well-funded campaigns in sophistication, using creative and relatively inexpensive strategies. Candidates, members of parliament, and local committee members worldwide are now providing information about their policy positions, inviting followers to campaign events or meetings on Facebook, and interacting with their voting public "on the go" and through short messages on X rather than lengthy and time-consuming posts on their blogs or websites.

Research has extensively documented the integration of new media tools, and X specifically, in election campaigns held in numerous European countries. Nevertheless, it has yet to achieve the central role that social media has played in US elections. Developments, such as citizen-initiated campaigning, have also emerged in Europe over the past few years, though with significant variation across countries and parties. Despite lacking innovation, European candidates use social media to contact their supporters directly and increase their exposure at minimal cost. This development enabled lesser-known candidates to rise from obscurity. Social media has also provided a platform for citizens to communicate directly with political candidates.

Communication interaction creates a rich campaign ecosystem, with each aspect feeding the others. Comments and conversations, liking and following, reflect various political and social trends occurring alongside the official campaign. Political activity online thus provides an immediate and visible element to a campaign.

The more posts made to Facebook or X, the more weblog posts are authored, and the more likely they are to reach a wide audience and encourage participation. In this respect, if there is an impact from engaging through a hypermedia campaign, the attention received can also be used as a predictor of votes. Based on a survey of sentiment within X, it was noted that such tools can be a valid indicator of the political landscape offline. Therefore, winning in the battle to have the most proactive hypermedia strategy may also result in increasing awareness, engagement, and support. However, such a conclusion needs further rigorous testing.

The influence of social media use in elections may be different in countries with populations of different sizes and political and electoral systems. Nevertheless, even motivating a small percentage of the population can make a considerable difference to the result of a party or an individual candidate.

7.5.3 Social Media Campaigning Organization and Strategies

E-campaigning is becoming an increasingly popular and effective way of connecting supporters, donors, and other key stakeholders, such as journalists, editors, and owners, that is, all who influence the party's visibility. E-campaigning uses digital and electronic communication channels, like e-mails, blogs, social networking

forums and cell phones. As these tools become increasingly sophisticated and widespread, campaigning organizations should know how to use them strategically.

Analysis of election campaigns often focuses on how the internet is used to connect to people; however, while this is undoubtedly a very important channel, it is not the deciding factor. Technology alone is not sufficient; a successful e-campaign also demands employing people with the right expertise, which requires power, a strong strategy, planning, compelling messages, and integrated tools to implement the strategy adopted.

E-campaigning should establish a direct relationship with supporters. An e-campaigning vision should clarify how e-campaigning activities will be executed to contribute to the campaign vision. Recruiting and mobilizing passionate and empowered local supporters who take back politics from politicians and lobbyists by donating, volunteering, and organizing is vital.

Once the e-campaigning vision has been articulated, the audience, mobilization, recruitment, and tasks must be determined. Supporters need to be inspired through all media available and direct contact should be established to gain donations while giving opportunities and tools for them to organize locally.

Social media can be used direct political messages to certain target groups. Of course, not all citizens can access the new media, so a part of society may be excluded from online political discussion due to the "digital divide." While social media cannot replace face-to-face contact, they can be a useful tool to target young people deliberately, the age group most likely to be disengaged from politics. Young people aged 16 to 24 are more active users of social media services than other age groups, including creating blogs, posting content, or sending messages.

Social media can also assist with much more refined targeting of voter groups by effectively using blogs, tweets, text messaging, e-mails, or search engine advertising. However, experts consider that the critical edge comes in how voters' data are mined in order to produce "microtargeted" messages sent to particular groups of users during a campaign.

Analysts have also noted the increasing personalization of modern election campaigns. Social media reinforces that trend by emphasizing individuals and focusing on personalities and personal relationships. Tweets or Facebook updates can keep followers and friends informed about what the candidate is doing as part of the campaign. Photographs or videos of the candidate at events or speaking to constituents are posted on social media afterward to give a more personal and humanized view. Personalization is associated with a higher level of emotional appeal. Such aspects can make messages more likely to be shared with others. Tweets with more emotional content and appraisals of candidates and parties are more likely to be re-tweeted.

Many politicians use social media, mainly X and Instagram, as a private broadcast channel for one-directional communication; called the "homestyle" information provision strategy. While a politician certainly can enter a discussion with voters, this strategy has risks. Resources are required to keep up good interaction. Moreover, the chance of encountering people opposed to a candidate's position is much greater, and politicians need to be prepared to deal with these so-called "trolls."

Perhaps the most important aspect of social media is the "network" effect produced when someone who has seen a video, visited a page, or read a tweet passes on the same message or a reference to all their friends or followers. These "second degree" networks, the followers of followers, may represent weak social ties (Granovetter, 1973), but can be very large. The extreme case of this network effect is that of a campaign item that "goes viral," that is, is distributed or seen by large numbers of social media users in a short period. The results might be appealing but such amplification may be negative in some cases.

There are diverse opinions regarding the phenomenon of “echo chambers,” where messages get passed between like-minded people who are likely to vote for a given candidate or party. However, many point out that virtual political communities are, in many cases, heterogeneous groups where a diversity of points of view exists, and this provides fertile terrain for ideas to spread and for users to be convinced by someone they know rather than by a campaign speech or a party leaflet.

7.5.4 Social Media Campaigns Effectiveness on the Public Sphere

Not all analysts are enthusiastic about social media and its effect on politics and political campaigning. While this effect has been proven to be crucial in electoral campaigning and shaping the results, it is risky to assume that it has accomplished the task of mobilizing apathetic citizens into politics. Many highlight the capacity of social media to undermine serious deliberation, encourage populist rhetoric and celebrity politics, and erode responsible collective action. Arguably, the fundamental question is whether social media is effectively mobilizes those engaged online to become engaged "offline" and thereby reduces democratic deficits.

There are signs of increasing political activism on the internet and social media. Studies have found a positive correlation between political internet use and voter turnout. However, several experts remain skeptical. Some point to evidence that social media’s most active political users are those who are already committed to political causes. Others find that the internet seems less effective than other media at engaging the disengaged. Still, others characterize many social media users as “slacktivists,” that is, people who are happy enough to comment or re-tweet a political message, but who are unwilling to be otherwise engaged. A study of Facebook users showed that social media does not drive politically unengaged users to productive political engagement. It will certainly take some time for a more precise overview to emerge.

7.6 Case Study: The 2016 US Presidential Election

Social media played a significant role in shaping the events leading up to, during, and after the United States presidential election 2016. It enabled people to interact more with the political landscape, controversies, and news surrounding the candidates involved. In contrast with traditional news platforms, such as newspapers, radio, and magazines, social media allows people to share, comment, and post below a candidate's advertisement, news surrounding the candidates, or articles regarding the candidate’s policy. This accessibility, in turn, would greatly influence the events that ultimately led to its outcome.

Candidates would often use multiple social media accounts, such as YouTube, Facebook, X, Instagram, and Snapchat, and depending on the digital architecture of each platform, they would post, create, support videos, link to news articles, and challenge other candidates via fact-checking, discrediting, and response. On the other hand, users could share, like, or comment on these actions, furthering the candidates’ outreach. By doing so, candidates and users both would influence and change people’s views on a specific issue. With candidates using different combinations of these actions, they built a unique communication style with the public, influencing their portrayal in the news, and their accounts. As a result, they ultimately aided in voter mobilization and electoral impact. Researchers from Stanford have found that 62% of US adults got their news on social media and that people are more likely to believe in news favoring their choice of candidate, especially if they have ideologically segregated social networks.

The topics of discussion for the candidates throughout the campaign were political, economic, healthcare, education, environment, foreign politics, immigration, criminals, and domestic issues. However, with social media the candidates, both Republicans and Democrats, could expand their “field of operations” beyond the broadcast debates. In one instance, former Florida Governor Jeb Bush and former Secretary of State Hillary Clinton feuded over economic and educational policy in a series of tweets. In another, Hillary Clinton and Donald Trump feuded over Obama's endorsement of Hillary Clinton and the deletion of X accounts.

Overall, these and many other events deployed in the social media sphere contributed to the outcome of the 2016 election by endorsement, controversy, or other exhibits providing discussion for political discourse.

Trump's 2016 micro-targeting social media strategy made political history. He is the fifth person in American history to become president while losing the nationwide popular vote. Trump's provocative tweets have been heavily discussed and disseminated, constantly dominating X feeds at all hours, every day. Trump was mentioned in 6.3 million X conversations and has been retweeted many more times than any of his political opponents (Barbaro, 2015). Trump also tried a new publicity channel by hosting an Ask Me Anything (AMA) session on the popular forum, Reddit. This free-for-all questioning was a risk, with most users being white, educated, middle class users with good incomes and only 19% identifying as conservative. However, Trump's candid participation on Reddit boosted the *r/The_Donald subreddit* thread to the front page through algorithms, acted like a pro-Trump meme machine and was ranked among the most active communities with over 785,000 subscribers. Trump's Instagram account *@realdonaldtrump* had 17.3 million followers in 2020. He won the Instagram game because his aggression and lack of political correctness compared to his more contrived political opponents appealed to the Instagram millennial audience's idea of being authentic and transparent.

Trump's digital director worked with dedicated Facebook employees to maximize Facebook tools such as Engagement Custom Audiences to upload existing contact lists of Trump supporters who would be receptive to a certain ad. The tool also allowed advertisers to target Facebook users who had interacted with Trump's posts for fundraising and has successfully gotten $2-$3 in contributions for every dollar spent, accumulating to millions of dollars raised in the first few weeks.

Many scholars assume that Donald Trump has reinvented the presidential function on social networks, with his slogan "Make America Great Again" transformed into #MakeAmericaGreatAgain with its acronym #maga. Campaigners were able to connect to his campaign through discursive hashtags. This created a winning political organization. According to an analysis, links between hashtags and white supremacist groups in the UK and the US were discovered in late November 2016, and these findings helped to show how hashtag social networks unified Trump's support (John, 2019).

Trump's slogan was so important that in April 2020, more than 70 different hashtags with this slogan were created by Instagram users. More than 2.2 million users follow the first one. Hashtags have become a dissemination strategy for politicians, especially during presidential campaigns. In order to win the election, to have more supporters, and to make himself known to the general public and the world, Trump used social networks and Instagram. In July 2017, he said: "My use of social media is not presidential—it is MODERN DAY PRESIDENTIAL."

Trump's election campaign contained many other digital innovations, most of which were introduced then. With lower overall costs, Trump has proven to be a major operator of digital tools for promoting himself, such as Facebook, over his rival Hillary Clinton (Ward, 2018). Google, Facebook, and X have played a key role in Trump's campaign by supporting him and guiding his campaign. Their involvement became apparent in many cases, such as the banner on YouTube on Election Day or Trump's embrace of Facebook Live. Trump's campaign was based on live presentations through digital media, giving it a modern and authentic character in contrast to Clinton's image, which appeared on television and seemed old-fashioned and distant (Persily, 2017).

Trump's digital campaign was mainly based on three factors: the marketing company Giles-Parscale, the micro-targeting company Cambridge Analytica, and the digital team of the Democratic Party. Brad Parscale, who had knowledge of online services and had previously worked for Trump's businesses, decided to use Facebook to influence the public. The company Cambridge Analytica had worked for Brexit and Ted Cruz's election campaign. Trump's campaign has targeted 13.5 million voters in 16 states, especially in the Midwest.

Jared Kushner, Trump's son-in-law, who has strong ties to notable tech investors and CEOs, also played a role in the campaign by taking on a very Silicon Valley approach. He incorporated geo-location tools to plot location density for voters concerned about specific issues like infrastructure, immigration, or healthcare.

However, Facebook was significantly criticized for its role in the US presidential elections in 2016, because of its targeted advertising system. "Facebook reminders" were sent to people to remind them to register to vote or vote in general. However, there is always a dark side to a story. In this case, it was viral the fact that Russia somehow shaped voters' behavior for Trump to be elected. Based on Solon O. and Siddiqui S., Russia-backed content reached almost 126 million American citizens on Facebook during and after the elections in 2016. Facebook claimed that around 120 fake Russia-backed pages were created, and more than 80,000 posts were directed to 29 million Americans, who afterward shared these posts and reached a greater audience. (Blunden & Cecil, 2018). This example shows the huge impact that Facebook pages can have on citizens without even knowing if they are real, but just because a "message" reaches them.

Furthermore, Google discovered 18 YouTube channels linked to the Kremlin's disinformation campaign. These were all done with Gmail accounts. Also, X found 2,752 accounts linked to Russian operatives. All these led to Facebook's announcement in April 2018, that the company was exploited by governments wishing to manipulate public opinion (Blunden & Cecil, 2018).

It is evident that new technologies dynamically evolve in the political landscape, posing new challenges in political processes. Both benefits and risks co-exist, requiring more and more expertise from all involved sides to implement politically successful procedures and to avoid severe implications that eliminate democratic values, at the end of the day.

7.7 Misinformation and Disinformation

At the end of the previous paragraph, some samples of malicious use of social media have been outlined. This section analyzes two major related issues: Fake news and the bots.

7.7.1 Fake News

The introduction of Web 2.0 allowed people with no technical skills to post texts and multimedia content online; WordPress, YouTube, Soundcloud, and Spotify are some services. Over the last decade, social media platforms have allowed content creation, publishing, sharing, and commenting. This way, creators and consumers of information, news, and ideas can connect directly and interact. Now, not only professionals of this kind but simple users as well can create similar content, thereby making the internet a network with a huge variety of ideas, information, and services, where content can be published through rudimentary websites or more sophisticated social networking platforms, offering thus endless possibilities for enrichment and feedback from users. Unlike the traditional process, the content being exchanged cannot be controlled or quality assured. Publications are products that go through the rigorous stages of editing and publishing and are made available for public scrutiny, as opposed to being the creations of professionals. The cost of entering the market and producing political content on social media is extremely minimal. This fact increases the appearance of small-scale strategies, which fake news producers adopt in many cases. Fake news can easily become part of social media users' everyday lives because they are constantly viewed on phones and news feed windows (Allcot & Gentzkow, 2017). As a consequence, social media has gained a bad reputation over the years as it has become a means of spreading false news. In research commented by the European Parliament on false news and the role of new technologies, the results showed that readers came across fake news at a ratio of 42% through visits to social media and 22% through search engines. On the other hand, regulated media had only 10% of social media visits and 30% of search engines.

The term “newsfeed” on social media platforms indicates how platforms favor certain news and guide users in selecting and reading selected news. As stated before, a Facebook algorithm decides what users see on their pages and what they do not. The reasoning behind this practice is to improve the user experience, show information that users find interesting and appealing, and keep them interested in using the site, maximizing their interaction with the service. Because advertisers support these services, the goal is to maximize the relevance and number of ads shown. The positive impact of viewing a post reflects users' interest in a page, posting performance, user feedback, and recent results. It is worth noting that similar methods of processing through algorithms are also applied with the aim of, for example, distributing content to minors, preventing copyright infringement, and combating illegal activities. While all platforms take similar steps regarding potentially illegal content (intellectual property issues, adult content only), there is a different approach to political reinforcement.

The Cambridge Dictionary defines fake news as "false stories that appear to be news, spread online or use other media, usually created to influence political opinions or as jokes." According to analysts, adding "as a joke" to this definition seems rather inappropriate and refers to the satirical type that has always spread false stories as jokes. However, in those cases, "the joke" could easily be traced back to well-known publishers who do not hide their names and intentions, and their readers enjoyed reading these stories (Martens et al., 2018). The US Collins Dictionary defines false news as "false, often impressive, information disseminated under the guise of news reporting." The term "false" again denotes the distinction between true and false news by verifying events. The literature reports that the definition of false news is difficult because it is often applied to three separate categories:

- News created or "invented" to make money or defame others.
- Reality-based news is "distorted" to fit a specific agenda.
- News that people do not feel comfortable with or disagree with.

Still, fake news can be categorized according to different characteristics as to the source of the news, the content (real or false views), the method of dissemination (targeted advertising, social networks), and the intent (to influence the election, to divide and cause dissatisfaction or make money).

Recently, the term "fake news" was added to the media vocabulary, and according to Google Trends, the phenomenon was silent for many years until the US presidential election in November 2016, when its search frequency increased abruptly. The general public then began to be heavily occupied by deliberate distortions of the news in order to influence the political landscape and aggravate societal divisions. Following the 2016 election in the United States, a study showed that:

- 62 percent of US adults got news on social media (Gottfried & Shearer, 2016).
- The most popular fake news stories were more widely shared on Facebook than the most popular mainstream news stories (Silverman, 2016).
- Many people who see fake news stories report that they believe them (Silverman & Singer-Vine, 2016).
- The most discussed fake news stories favored Donald Trump over Hillary Clinton (Silverman, 2016).

Social media has become the significant enablers and conduits of fake news. About 47% of Americans use Facebook as the dominant source of information. Moreover, there has been evidence that Russia manipulated all the major internet platforms during the 2016 US election (Gottfried & Shearer, 2017). Fake news coexists with other information disorders, such as disinformation or misinformation. Most of the time, they are associated with topics like health and politics. Especially nowadays, fake news is used widely as a political weapon aiming to manipulate the masses. People are concerned about fake news because it is confusing and

because it may indicate interference by unjust or hostile factors (e.g. suspicions of Russian actors trying to influence the US election) and undermine social and political cohesion in several countries (Martens et al., 2018).

Although fake news has always existed in some form or another throughout history, it is becoming more and more recognized as a serious issue facing society as a whole. Fake news is linked to the way information is produced and disseminated and the role it plays in today's time as an instrument of influence and persuasion. Communication technologies allow news to be transmitted quickly. Based on this assessment, one could argue that fake news is not the root of the problem but rather a symptom of deeper problems affecting politics and information.

False news is not all new, but deep fake news is indeed unprecedented. Due to the ability of digital technology to falsify audio and video media in a way, deepfakes present a product that appears convincing beyond doubt and distorts reality with the intention of misleading. In these reproductions, real people say and do things they never said or did, making lies more realistic and difficult to detect.

According to analysts, digital forgery is increasingly realistic and persuasive, and "profoundly false technology" is at the forefront of this trend. This technology uses machine learning algorithms to insert faces and voices into real-life video and audio recordings and creates realistic representations of digital "cloth." Deep fake news technology has features that allow it to be quickly and widely disseminated most convincingly. Deepfakes have features that ensure their dissemination and, into the hands of unfair users, may spread and reach global audiences. The revolution in the distribution of images, audio, and video (original or not) has changed the distribution model through innumerable platforms facilitating global connectivity. Thus, deepfake and false news are powerful tools against trustworthy and accurate information, undermining public safety and democracy while sowing the seeds of social unrest and dividing society through acts of violence and other disruptive behaviors. So, the problem is getting worse and the public is facing new, more aggressive forms of misinformation and exploitation while the risks to democracy and national security are increasing.

The solution is a new system of safeguards. Nowadays, platforms attempt to face this novel challenge in several ways. For example, on the one hand, Facebook announced that it would change its algorithm to assure users of the “quality” of the platform’s content. On the other hand, X announced that it would block some accounts that spread misinformation. Technically speaking, platforms can inform users about the quality of the source they are using by providing signals incorporated into the algorithmic rankings of content. This could be accomplished using bots or cyborgs. However, bot developers are always expected to be one step ahead of any software robot in the foreseeable future. Fake news can spread out with the help of social bots (automated accounts impersonating humans), which detect users' likes, shares, and most usual searches. Facebook estimates that approximately 60 million social bots are infesting its platform and were responsible for a large amount of political content during the 2016 US campaign, while some of these bots were also used to influence people in the 2017 French election.

7.7.2 Bots

7.7.2.1 Definition

Software robots, or bots, have existed since the early days of computers. One of the most well-known categories is chatbots, envisioned by Alan Turing after World War II. However, artificial intelligence has been developed through the years and, as a result, bots have shown remarkable progress. Every new technology gets abused, and social media is not the exception. Many of these bots nowadays are designed to harm, steal information and manipulate.

A “bot” (short for robot) is a software application built to carry out automated repetitive tasks like pre-scheduled posting on social media. No human is needed to activate or command a bot to perform the preassigned tasks. Every bot action is automated; most of the time, it is even human-like. The overall schedule and behavior of bots are human-like also. Although bots can post, for example, every few seconds, their activity emulates human activity: whatever a person does in the morning, day and night; acting, working, sleeping.

Bots can act like web crawlers, spiders, or spider bots, indexing content from all over the web, or chatbots, an application that simulates human conversations too facilitate customer service (Chapter 15). On the other hand, they can be malicious by violating rules. They can crack passwords, spam content, scam and swindle, harvest personal data and perform illegal online activities. Social bots operate on social media, demonstrating human-like behavior, imitating human users, scanning, chatting, liking, following, posting, searching, and interacting with datasets, software, regular (human) users, and other bots. Some have a clear-cut political “command”: to promote a political agenda and influence public opinion.

Unavoidably, this phenomenon affects the whole society on several levels. Politics is a field that social bots largely affect. For instance, in some cases, robots support a specific candidate, influencing potential voters. As a result, society loses its democratic character, and the public gets manipulated. Recently, more specifically, in 2010 in the United States, this kind of abuse was detected during the midterm elections. Some robots supported specific candidates via X and sent fake news to websites.

In the modern political landscape, armies of automated accounts, which are designed to look like those of real social media users, game the algorithms to:

- push certain narratives,
- boost the popularity and prestige of a political party or candidate,
- share false or misleading information to undermine political dissidents, opponent politicians and movements,
- share hate speech, racism, discrimination,
- polarize,
- promote distrust and undermine democratic processes,
- shut down free speech, suppress content, and diminish activist voices,
- use personal data for political gain.

The rise of political bots has influenced politics with a new form of propaganda within the political sphere: computational propaganda. Computational propaganda refers to a phenomenon of online political manipulation through illegitimate interferences aiming to “disrupt or influence democratic processes.” It is the deliberate spread of misinformation over social media through automation, Artificial Intelligence (AI), algorithms, and human online behavior. Automated propaganda occurs on social media platforms such as Facebook and X, and its main actors are political bots, trolls, MADCOMs, and cyber attackers. All of them have particular goals aligned with a political cause. Trolls are real people who produce content, spread propaganda, threaten, bully, and harass other users whose ideas differ from theirs or their sponsors. MADCOMs are machine-driven communications that generate text, audio, and video content to bully, threaten, or engage users in political discussion. Cyber attackers spear phish or attack on the Internet of Things (IoT) to access confidential data or perform DDoS attacks to paralyze websites, companies, or even governmental actors.

Bots do not only reproduce fake news and disinformation. They also try to influence public opinion about a person or a movement by reproducing factual information irrelevant to the subject in question, information that aims to divide and curb attention towards a certain subject. It also aims to build trust so that the targeted audience simultaneously absorbs fake news and non-factual information along with the real.

7.7.2.2 Bots Across Countries

In this new era of politics, the army of bots has been deployed in several countries throughout the world: China, Australia, Russia, the United Kingdom, the United States, Iran, South Korea, Turkey, Spain, Greece and India. It is estimated that bots make up over 60 percent of all online traffic.

In the United States of America, according to X Audit, "at least 30% of the followers of both candidates were bots" in the 2016 elections. One fifth of all tweets during the TV debates (3.8 million tweets) were posted by 400,000 automated accounts and there is evidence that pro-Trump bots garnered the most attention and influence among human users.

In the rapidly developing society of Brazil, in 2016 (the year of municipal elections and the impeachment of former President Dilma Rousseff), according to Symantec, a multinational cybersecurity firm, Brazil hosted the eighth highest number of bots globally, while the Spamhaus Project, an international organization that monitors networks and global spam activity, claimed that Brazil was fourth in number after China, India and Russia in the BRICS list, the top 10 worst botnet countries, with 485,133 bots on 17 May 2017.

In Venezuela, a Twiplomacy study found that the former President, Nicolas Maduro, was the third most influential world leader on X. However, it was odd that his tweets were liked ten times less, probably because bots were involved. As Cuban dissident Yusnaby Perez also affirmed, as many as 2,500 accounts retweeting Nicolas Maduro were automated.

In India, all major political parties have deployed bots to boost the followings of their leaders on social media, to troll opponents on X, and to inflate hashtag rankings. It was reported that Indian Prime Minister Narendra Modi got 280,000 followers in one day and that "nearly half of Bharatiya Janata Party (BJP)'s Narendra Modi's followers seem suspicious."

In Spain, the situation has been different; in a study on the 2019 Spanish general election, social bots represented less than 1% of total users. However, their effectiveness was quite alarming since they easily managed to engage human influencers and have them retweet or share their content with hundreds of thousands of followers.

According to an investigation held by the Associated Press and the Oxford Internet Institute, an army of bot accounts fueled China's rise on X. These government-sponsored bots were retweeting Chinese diplomats aiming to transmit their agenda to hundreds of millions of people covertly. In 2018, X suspended more than 5,000 suspected state-backed accounts that were spreading covert Chinese propaganda around the world and banned another 200,000 related accounts.

According to X, 7,340 pro-Erdogan accounts were created and operated by the youth wing of Turkey's ruling AK Party. These accounts were taken down in 2020, whereas in 2019, according to a study of the *École Polytechnique Fédérale de Lausanne*, more than 19,000 unique keywords were used in astroturfing by least 108,000 bots.

In Greece, in research during the Thessaloniki International Fair in September 2018, where the grand debate about the *Prespa Agreement* of June 2018 regarding the name of North Macedonia was the burning issue, in a total of 3,698 accounts (12.87%), 476 bots were located.

7.7.2.3 Ethics and Regulatory Context of Bots

Unquestionably, the objective of using political bots is to influence and manipulate voters. Their resemblance to humans and their aim to appear as real users to the targeted audience by mimicking human behavior reveal an indubitable intention to deceive. Thus, it is clear that bots degrade the democratic values of freedom of speech, transparency, truth and consensus, equality, justice, and respect. The increase in the use of bots in the public sphere jeopardizes democracy. Together with other computational propaganda techniques, bots

distort reality to create an illusion of consensus. An ideal democracy cannot be present in a technological world where robots imitating humans manufacture consensus. An ideal democracy cannot be present in a technological world where robots imitating humans manufacture consensus. Bots can influence, deceive, and persuade thousands of people, messing with free will. However, for democracy to coexist with that amount of political manipulation and covert propaganda seems impracticable.

Needless to say, even if the deception behind bots' actions is exposed, the effects they can have can be irreversible. Thus, as bots are becoming more popular and bot technology grows, their punctual detection and regulation seem to become a sine qua non for the prosperity of modern democracies.

Bot accounts may have many followers, or they may have none, may follow a high number of accounts, or just a few, depending on the purpose they are working for. These can be indications of bot presence, but they do not suffice. As time passes, creators make bots more complex, harder to detect, and even more complicated to regulate.

Social bots have become a challenge in recent years, against which computer scientists have not yet developed antibodies. This vulnerability allowed software robots to influence the masses unconditionally. While filtering algorithms were used to detect them, the absence of methods to derive representative samples of bots combined with the extraordinary number of humanlike bots made this process more challenging.

Today, several countries and institutions have developed systems that understand and identify bot-patterned social media accounts using quantitative and qualitative methods and machine learning. COMPROP, the Computational Propaganda Research Project of the Oxford Internet Institute of the University of Oxford, is a tool that combines empirical findings with algorithms, automation, and human computer interaction to understand and analyze political bots. Botometer and Botslayer, applications developed by the Observatory on social media at Indiana University, use machine learning and algorithms to detect bots. BotOrNot, a service that detects bots based on over a thousand features, has served more than one million automated account detection requests since 2014.Technological progress in bot detection is on the rise, but the impact of bots could also be limited through enhanced digital media literacy and awareness. Knowledge of bots and the tools to identify and critique forms of computational propaganda can protect social media users from being manipulated and deceived.

As the risks increase, media platforms can establish and enforce standards and good practices, build rigid policies, and impose penalties for non-compliance in order to regulate bots. In July 2018, in pursuit of halting bots, X suspended nearly 70 million accounts that demonstrated bot-like behavior.

In politics, in order to annihilate the opponents who employ bots, political actors, unable to deal with the illicit means they face, will eventually respond with more bots, as Nicolas Maduro of Venezuela has been quoted as saying, “If lies come through Twitter, we are going to strike back through Twitter.” The world is standing on the threshold of a contemporary war of bots. This war can bring chaos, cacophony, polarization, and radicalization, misinformation, hatred, and distrust in the virtual world of the internet, which is a big part of modern people’s lives. A Code of Conduct for political campaigning and strict legislation like California’s Bot Disclosure Law, according to which a bot must disclose when it is used to "incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election” could prevent this virtual chaos by promoting a more responsible and legitimate use of bots in politics and ensuring that all bot actions comply with the best possible practices.

7.7.2.4 The Case of AKP Trolls

On the 28th of May 2013, a group of environmentalists concentrated in Taksim Square of Istanbul, Turkey, in order to protest against the government’s plan to cut down trees and destroy the Gezi Park to construct the “Taksim Military Barracks,” a shopping mall and a mosque. The police responded by using violence against the

protestors, and the issue quickly gained the public's attention. The people were in favor of the environmentalists and the maintenance of the Gezi Park and condemned the police's brutality. The following day, Turkey's Prime Minister stated that the construction according to the government's project, would continue and characterized the protestors as "spoilers." That fact intensified the conflict between citizens and government and unified the Turkish public since demonstrations started to occur in squares of various Turkish cities for the public to show its support for the Gezi Park movement (Dermihan, 2014).

An outcome of the Gezi Park protests was the formation of a cyber troop consisting of 6,000 agents whose occupation was to shape public discourses, increase the popularity of the AKP, create content in favor of the party, and encourage other social media users to attack people who express their opinion against AKP's policies. The above cyber troop is commonly known as AK Trolls, and the state finances it. People first heard about it in 2013, but it became even more known after a tape saw the spotlight, in which the President's daughter, Sumeyye, was saying to his advisor that she would ask for help of their "trolls" in the campaign she was organizing (Bozkurt, 2019). In some cases, AK Trolls express criticism not only towards their opponents but also towards members of the AKP who do not follow the party's line. For instance, in the 2014 elections, when the AKP's majority in parliament was lost, President Erdogan forced Ahmed Davutoglu, the Prime Minister then, to resign. The tool that helped to extract power from Davutoglu was the group Pelican Declaration, a team of the AK Trolls (Saka, 2020).

The AK Trolls use a variety of strategies in order to control online content, spread false information, and harass people who express their disbelief and disagreement with the government's actions. The primary means of their activity is X, due to its flexibility and its multiple functions, thanks to whom people can follow, tweet, re-tweet, and create hashtags. One of the most practiced AK Trolls' techniques is the targeting of individuals and especially the harassment of users, who make statements against the government or post news that contradict with the ones that the government spreads. This is also known as "social lynching". It usually it starts when a pro-government figure or a journalist post something neutral or negative about an anti-government person. Then trolls and X bots start to create hashtags and threats against that person (Sakas, 2018). Most often, the people who become targets are journalists, especially those excluded from the mainstream media, activists and members of other political parties. Sezgin Tanrikulu, a Turkish attorney and Republican People's Party member, is an example of this case. He pursued the AK Trolls' legal punishment after they attacked him on X, but they still continued to verbally abuse him online. Another more extreme incident is Nevsin Mengü, an anchorwoman at the Turkish CNN who was responsible of covering the attempt of a coup d'état in 2016 and at a point expressed her concerns about the AKP's effect on democracy. This provoked the reaction of the government's supporters. More precisely, it all started when a pro-AKP profile with no particular influence posted a tweet against her which led to trolls attacking her online. This shows how powerful X is since a low-profile user managed to get the attention of pro-government politicians and journalists and start a hate campaign against her (Nyst & Monaco, 2018). The easiest targets for trolls are everyday people. By threatening and attacking them, trolls can make them quit social media, thus eliminating their participation in online public discourses (Karatas & Saka, 2017).

In addition to the AK Trolls' strategies, another one is the disclosing personal data such as phone numbers, addresses, and other private information. In these cases of hacking the AK Trolls immediately after gaining access to the account of an anti-government user, they post apologizing messages towards Erdogan, expressing their regret for criticizing his actions. The next step is leaking the user's messages, multiple postings similar to leaked messages by trolls and X bots and creating hashtags in order to enter the trending list. For instance, in 2016, the X account of Ismail Saymaz, a journalist known for revealing facts about the government, was hacked by AK Trolls, and his conversations were leaked. The pro-government trolls made posts and memes on X referring to some of his conversations with other female partners. They attempted to hurt his public image by giving the impression that he was being inappropriate with other women (Karatas & Saka,

2017). According to the International Press Institute (IPI), in 2016, over 20 accounts of anti-government journalists were hacked and their personal information spread throughout the Internet, making it possible for everybody to see (Shearlaw, 2016). The AK Trolls have a specialty in their activity. There are trolls responsible for propagating the government's news, others who expose anti-government journalists, and other who post misleading videos of military content to manipulate public opinion in favor of the government's actions.

7.7.3 Russia, US, and Europe

US agencies have confirmed that the Russian government interfered in the 2016 US presidential election to harm the campaign of Hillary Clinton, boost the candidacy of Donald Trump, and increasing political discord in the United States. Russia's covert activities were first publicly disclosed by members of the United States Congress on September 22, 2016, confirmed by the United States Intelligence Community on October 7, 2016, and further detailed by the Director of National Intelligence office three months later. According to US intelligence agencies, the operation was ordered directly by Russian President Vladimir Putin. Former FBI director Robert Mueller led the Special Counsel investigation into the interference from May 2017 to March 2019.

According to Attorney General William Barr, who wrote a letter about the Mueller investigation's findings, Robert Mueller determined that Russia had interfered in the election primarily in two ways; firstly through disinformation and social media campaigns, and secondly through computer hacking and strategic release of information. For Mueller's investigation into links between Trump associates and Russian officials, Barr wrote that Mueller did not find that Donald Trump's presidential campaign conspired with the Russians in the Russian interference.

It is believed that the way this influence took place was through a "troll farm", which created thousands of social media accounts that impersonated Americans supporting radical groups, planning and promoting rallies, and reached millions of social media users between 2013 and 2017. According to criminal indictments by the Special Counsel, those messages and activities spread distrust towards the candidates and the political system in general, for example, by discouraging African Americans from voting or by motivating conservative voters wary of Trump.

In 2016, during the election campaign, fake news became President Trump's favorite phrase. As mentioned in the beginning, the term refers to fake political news transmitted by dubious partisan war media for speculation (Sarlin, 2018). In the months leading up to the presidential election, news websites and Facebook pages drew attention to the production of utterly fictional articles as Pope Francis shocked the world, backing Donald Trump for President, defaming readers' prejudices. In FYROM, teenage businessmen built a cottage industry with fake news sites that made fake publications for President Obama and Hillary Clinton, raising much revenue. Based on research findings in 2016, over 27% of adults visited an article about a website that favored Trump or Clinton that had been identified as a false information center (Sarlin, 2018).

Russia has understood the fundamental conflicts of American society. Racial segregation is the most divisive issue. Russia's goal was simple enough: to use social media and the Internet to push these buttons as far as possible and to create more anxiety and polarization. However, they were not alone in the race; they tried to identify and exploit every issue they could find (Illing, 2018).

As mentioned earlier, in one of the first academic studies of fake news, researchers at Princeton, Dartmouth, and the University of Exeter estimate that about 25% of Americans visited a fake news site over a six-week period from the 2016 US elections. However, researchers also found that visits were very concentrated—10% of readers made 60% of visits. The researchers concluded that "fake news does not exhaust the intense news consumption."

"The distance was relatively long but not that deep," says Alexios Mantzarlis. "It's a big step to say that people are voting for it, making decisions based on this news." "To say that it poisons our democracy or that it won this type or the other type of an election, we need a lot more research to be able to say it" (Wendling, 2018).

From the information above it is concluded that there is strong evidence that misinformation is part of the Russian military doctrine and its strategy to divide and weaken the West (Boffey, 2018). Facebook, in particular, has been used extensively for these purposes, raising many questions about how it works and whether it is freedom of speech or targeted coverage of an event in order to influence against or in favor of certain entities.

Following Russia's informal participation in the US presidential election, the European Union was concerned about Russia's possible influence on the upcoming European Parliament elections. To prevent the US problem, the EU has launched a "war on misinformation" spread by the Kremlin to protect the European Parliament elections. “There is strong evidence that Russia is the main source of misinformation in Europe,” said Andrus Ansip, Vice President of the European Commission (Boffey, 2018).

Exposing citizens to large-scale misinformation, including misleading or fake information, is a major challenge for Europe. The European Commission has committed all stakeholders to a clear, integrated, and broad-based action plan to tackle the spread and impact of electronic misinformation in Europe and to safeguard European values and democratic systems (European Commission, nd). Facebook's assumption that there are between 60 and 90 million fake accounts representing 3-4% of the users on the platform, King said, and some of these accounts are the most active (Boffey, 2018), creates yet another reason to create a plan to prevent such news from spreading.

From 2015 onwards, the European Union is taking an active part in tackling misinformation. Following the European Council's decision in March 2015 to “challenge Russia's ongoing flood information campaigns”, the *East StratCom Working Party* on the European External Action Service (EEAS) was set up. This Task Force works with the relevant Commission services to focus on communicating EU policies effectively to the countries bordering on its east. These countries bordering on the EU have developed their overall media environment in recent years, including in support of media freedom and the strengthening of independent media. The EU should aim to address and raise awareness of the Kremlin's misinformation activities (Commission, 2018).

In 2016, the Common Framework for Combating Hybrid Threats was adopted, followed by the Joint Communication on Increasing Resilience and Enhancing Hybrid Threat Opportunities in 2018. The follow-up comes in April 2018, when the Commission presented a European approach and self-regulatory tools to tackle online misinformation, including the EU-wide Anti-Misinformation Code of Conduct, supporting an independent audit network, with facts and tools to foster quality journalism. Specifically, on October 16, the Code of Practice was signed by many companies such as Facebook, Google, X, and Mozilla, as well as by the professional association representing online platforms and professional associations representing the advertising industry and advertisers (Commission, 2018).

The European Commission posted a Press Release on 5 December, 2018, entitled: “*A Europe That Protects: The EU is stepping up action against misinformation.”* Impressive is the introduction of news that says it aims to protect democracy and public debate for the 2019 European elections and for national and local elections. For these reasons, the EU has implemented an Action Plan to step up efforts to tackle misinformation in Europe and beyond.

7.7.4 The Case of Cambridge Analytica

Cambridge Analytica was founded in 2013 by the billionaire entrepreneur Robert Mercer as a company that would deal with online marketing and consultancy. It is referred to as a company owned by Strategic Communication Laboratories (SCL) and headquartered in London. It is a company that works on behavior and communication research, and as a product, it provides the behavioral change of the target audience that has been selected (Ward, 2018). The company has worked with agencies such as the US Department of Defense and the UK, providing communications to counterintelligence operations in Afghanistan, the Middle East, and North Africa. Cambridge Analytica also provides consumer and political behavior changes as a service (Ward, 2018). Cambridge Analytica first appeared in the media with its involvement in Ted Cruz's 2016 campaign. Reports on Cruz's nominations to the company prove her involvement. It later appeared to have been involved in the *Leave.EU* campaign in the referendum on the UK's exit from the EU, the so-called Brexit. When the company's work on Cruz's campaign ended, it took over Donald Trump's campaign. By the end of the year, the Trump campaign had successfully conquered the White House and paid Cambridge Analytica nearly $6 million (Ward, 2018). During the election, most believed in the victory of Hillary Clinton as she made great use of new technologies while at the same time having full coverage from the traditional media (Persily, 2017). Trump's victory was unexpected, so the media sought to understand the process of victory. Therefore, Cambridge Analytica's involvement in his campaign was investigated. Articles that indicated social media's interception of personal data to support Trump's campaign appeared. The company has denied spying on personal data, which is contradicted by statements made by Alexander Nix, the company's CEO, about its methodology (Ward, 2018).

The Cambridge Analytica scandal erupted in March 2018 when *The Guardian* and *The New York Times* revealed that the company had illegally harvested 50 million Facebook profiles to target digital political advertising in the US election and Brexit referendum. Only thereafter, Facebook clarified that the number of profiles involved was about 87 million users and informed that the types of data (such as likes, followed pages, locations, news feed, and messages) were pretty accurate and detailed for the company's identification of the right profiles to sponsor the most suitable and persuasive contents.

The company's practice was to mine social network users' data to trace a sort of psychometric profile that can draw out people's habits and behaviors. This online marketing strategy targets consumers with products that align with their interests. Therefore, this company has implemented a more sophisticated algorithm that was able to "micro-target" users: by monitoring their behavior online, political micro-targeting operates to send to users personalized advertising that suits their preferences and attitudes, thanks to the information collected while surfing the net.

The precursor of this digital technique was developed for Netflix in 2006 to improve the program's features. On the same line, in 2013, a researcher at Cambridge University, Michale Kosinski, released an article on the capacity of Facebook likes to predict (with 85 to 95% accuracy) personal attributes like "sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender" (Kosinski et al., 2103). One year later, another academic of the same university, Aleksandr Kogan, built an app called *thisisyourdigitallife*, in which 270 thousand users were attracted to take a personality test and agreed to give data for academic use to his company Global Science Research (GSR), just in collaboration with Cambridge Analytica. The tests were taken through Facebook login, and thanks to Facebook's old policy, the information of the test-takers friends was also collected.

At this stage, on the one hand, the inadequacy of Facebook's policy on the guarantee of privacy can be noticed, and, on the other, the course of events that led Cambridge Analytica to this data acquisition. With regard to the first point at that time, Facebook's security was weaker, and the system permitted access to

friends' profile data without agreement: this "error" was solved by Mark Zuckerberg, and the GDPR was implemented in 2018 in Europe. However, Kogan had violated the Terms of Use, in which Facebook notes the prohibition to share data with any third-party company, in this case Cambridge Analytica. For the record, this volume of data has allowed the company to improve its micro-targeting technique and present itself as the best on the market for any campaign. Indeed, the statistical model developed by Kogan has been evaluated as accurate in guessing political affiliation and voting behavior, which allowed them to broaden their market.

In light of Christopher Wylie's statements, it may be possible to assume that Cambridge Analytica was not interested in academic or marketing purposes. However, it has aimed to collaborate with parties during elections to support their rise to power by managing online campaigns. This scenario is based on the evidence of the net of Mercer's relationships with important politicians, the company's involvement in some elections, such as Trump's 2016 and Mexico's 2018 election, and its unethical digital strategy that had boosted the spread of fake news.

According to Cadwalladr's investigation, an intricate web of power is delineated in this affair and "Cambridge Analytica is one point of focus through which we can see all these relationships in play" (Cadwalladr, 2020).

A digital communication company hired by the "*Vote Leave*" party was the Canadian *AggregateIQ*. It is a mysterious company, unknown to the public, that signed away its intellectual property (IP) the same year of the US primary elections and sold it to Robert Mercer (the founder of Cambridge Analytica). At this point, the complicity of Cambridge Analytica in the Brexit referendum is evident, which constitutes an additional involvement in the political landscape besides the Trump and Mexico 2018 elections.

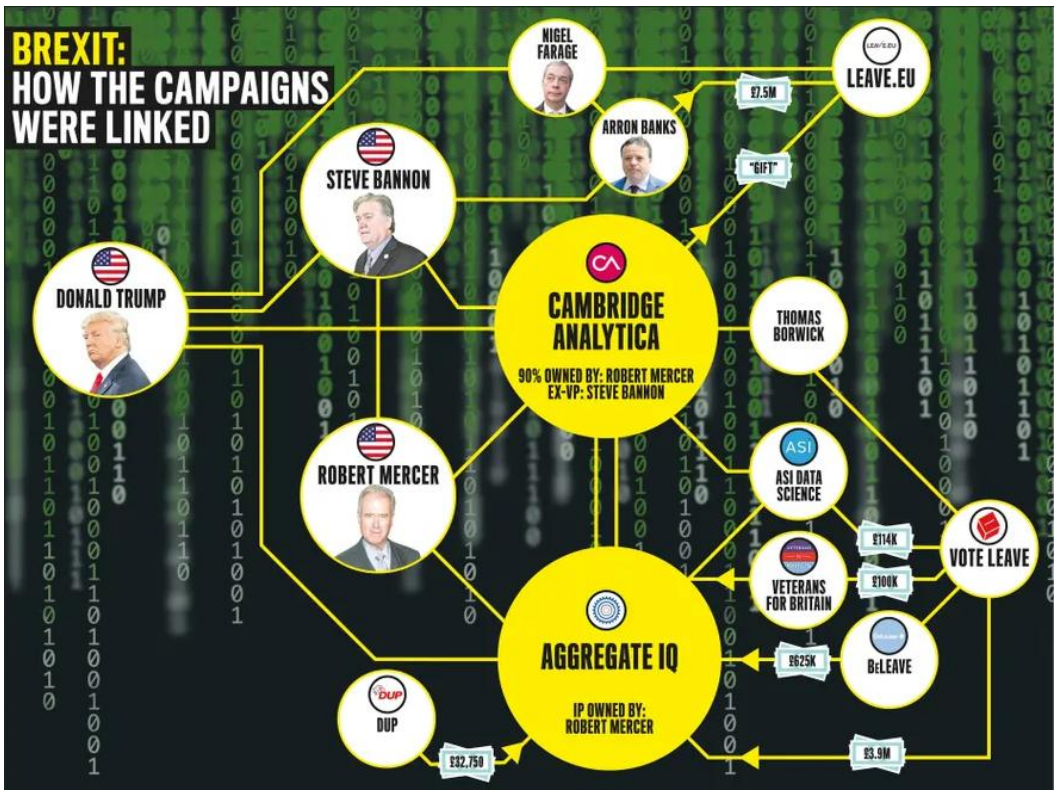


Figure 7.3 *Brexit: How the campaigns were linked. (Source: https://www.theguardian.com, Photographs: James Melaugh/Danielle Campbell/The Observer, 2017)*

A fundamental detail in this story is introduced by some statements made by an ex-Cambridge Analytica employee who argued that the company works with psychological warfare techniques used by the military to effect mass sentiment change: "It brought psychology, propaganda, and technology together in this powerful

new way" (Cadwalladr, 2020). Considering this potential insight, the micro-targeting model can soon become a method to find the "persuadable" voters and show them emotional trigger content to convince them to vote for the advertiser-political party. Irrespective of this model's military or digital marketing background, its success, and implications are undeniable, especially if the social media platform used is not institutional and the contents are not controlled: fake news, misleading messages and materials that have been spread without any control. This can be considered a new degree of propaganda and mass manipulation.

Regarding the case of the Brexit referendum, the peculiar political landscape of the UK needs to be taken into account because it has enabled the country to investigate this case further. In 2000, the *Electoral Commission* was instituted in the UK as an independent body that supervises elections and controls political finance to ensure an honest and democratic country. The electoral law imposes spending limits for the campaigns, and, specifically during a referendum, all the expenditure needs to be recorded and reported to the Electoral Commission, even the ones coordinated between more parties or non-parties campaigners. After the scandal broke, the Electoral Commission led an investigation "on whether one or more donations—including services—accepted by *Leave. EU* was impermissible" (Watt, 2020). Evidence shows that Vote Leave had spent £3.9m for the online campaign with *AggregateIQ*, and other affiliated *Leave* campaigns, *BeLeave*, *Veterans for Britain* and the *Democratic Unionist* party with £757,750 (**Figure 7.3**). During a *Channel 4* interview, Shamea Sami, a young volunteer in the pro-leave campaign, declared that an imposition from above urged them to invest money in *AggregateIQ*. It may be plausible to believe that the main party, Vote Leave, has played the groups of people involved in the affiliated Leave campaigns. The Electoral Commission found the party guilty of breaching the electoral law and fined it £61,000. The Information Commissioner's Office has conducted another institutional investigation into the possible illegal use of data. In conclusion, following with Carol Cadwalladr, these connections and relationships between billionaires and men of power may really suggest a "first step into a brave, new, increasingly undemocratic world" where billionaires' companies lead disinformation and fake news, thanks to unregulated platforms like Facebook, and where citizens become the product and subjects.

7.8. Digital Diplomacy: Twiplomacy, and Instaplomacy

The craft of diplomacy remains, to this day, an integral part of foreign policy. Traditionally designated as the formal communication channel between state actors, diplomatic activity has experienced notable alterations. The technological progress in Information and Communication Technologies (ICTs) has undoubtedly affected this practice, as well as countless other sectors of human activity. These advancements have influenced how information circulates hence transforming economic, political, and social landscapes across the planet (Adesina, 2017).

The adoption of digital means has not only introduced new tools but also an additional plane of communication. The availability of devices that facilitate easy access to the Internet has greatly increased the number of users. It has favored the inclusion of various audiences, that were previously left outside the discourse.

Connectivity and interactivity have become the main traits of the new media and its communication activity (Alvarez, 2017). Social media platforms' interactivity has enabled two-way communication between citizens, organizations, state, and non-state actors. The application and use of these tools gave rise to the term e-diplomacy or digital diplomacy as a distinct form of diplomatic practice. The appearance of these virtual communication channels does not mean that conventional modes of diplomacy have lost their relevance or primacy in international relations (Adesina, 2017). However, governments have certainly acknowledged their utility and usefulness (Yepsen, 2012), along with the threats that they may pose (Yepsen, 2012). Their interest and fear can be easily justified by the notion that social media has been credited or blamed (Yepsen, 2012) for

various incidents like the Iranian Green Movement in 2009, the 2009 Moldovan protests, and the Egyptian Revolution of 2010 (Yepsen, 2012). Speaking of the Egyptian Revolution, it can be boldly stated that social media was broadly used during the Arab Spring, aiding information distribution and protest organizations (Adesina, 2017).

On the other hand, the opportunities of those social media platforms are a serious concern for many governments, and their subsequent adoption of these new electronic means is no surprise. Ministries of foreign affairs (MFAs), embassies, and diplomats of various countries have already established a solid presence on social networking sites (Kampf et al., 2015). The overwhelming majority of this presence is found mainly on two sites, Facebook and X. AS such, this investigation will focus exclusively on analyzing the prospects of diplomatic functionaries in that area of the Internet.

Considering the incidents described in the previous sections of this chapter, it is easy to understand that social media has affected and changed diplomacy in general. Postmodern diplomacy is known as digital diplomacy, which is a public democracy using new information and communication technologies as a tool for strengthening diplomatic relations between international actors (Rashica, 2019). It allows us to “practice democracy without the limits of time, space, and other physical conditions” (Van Dikj, 2001). Digital diplomacy is an essential foreign policy for a country that wants to advance its goals, extend its international reach, and influence people.

The term Twitter diplomacy, also known as "Twiplomacy" or "hashtag diplomacy," refers to the use of the social media website X by heads of state or leaders of intergovernmental organizations (IGOs) and their associated diplomats to conduct diplomatic outreach and public diplomacy. It may also refer to the use of X and other social media sites by government agencies and officials to engage with the public, disperse information, and even leverage global influence. The term emerged from an August 2012 report from Geneva-based public relations firm *Burson-Marsteller*, which studied world leaders’ tactics using X and attempted to outline how social media can bridge the gap between these leaders and the public they serve. From these statements and the examples listed in the previous paragraphs, it is evident that X has finally made it to undertake several roles in diplomatic communications, from cordial announcements of bi-lateral cooperation to terse exchanges and diplomatic jabs, as well as more casual posts.

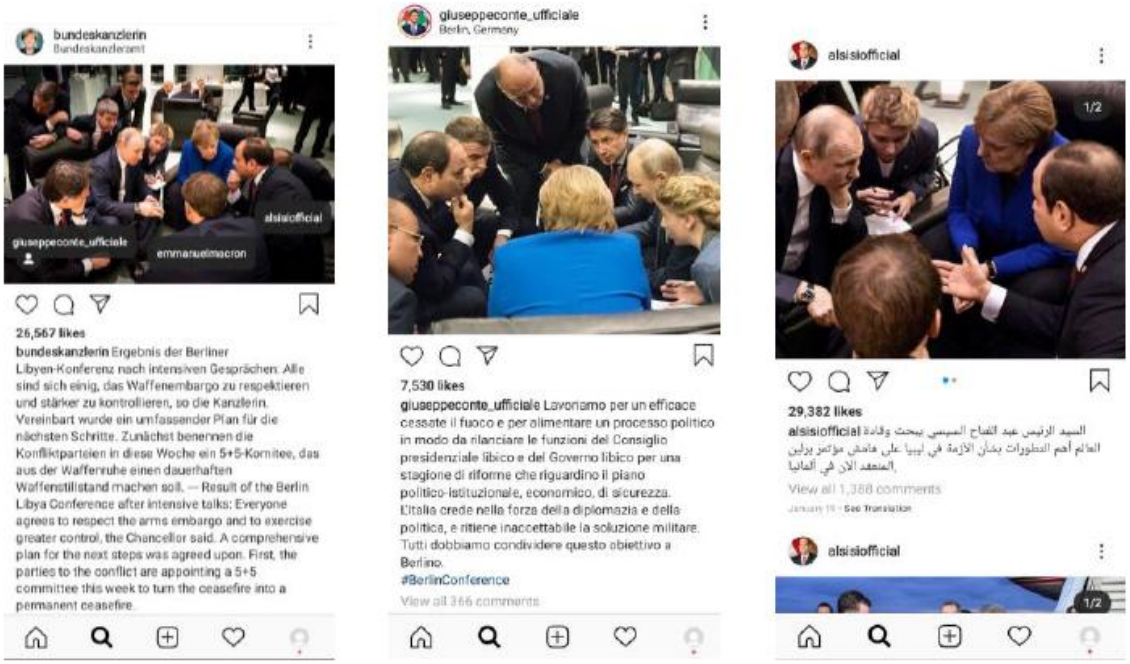


Figure 7.4 *Photos posted on Instagram by leaders during the Berlin conference in Berlin, January 2020. (Source: https://www.instagram.com/, 2020)*

In recent years, another form of digital diplomacy has emerged: Instaplomacy, where diplomacy is "more visible and more visual" (twiplomacy.com, 2018). Thus, Instagram has changed international relations for governments (Adesina, 2017), embassies, consulates, governmental and non-governmental organizations, and ministries, such as ministries of foreign affairs. This is part of the globalization process, where the world's nations are intensifying their interdependence in political activities and systems.

Diplomats are constantly negotiating something, be it political, social, economic, or environmental issues. They seek to solve problems, make decisions, and find action plans. In a visual and clear way, Instagram makes it possible to show the citizens and the world meetings and exchanges between diplomats. On the 19th of January 2020, the conference on the conflict in Libya took place in Berlin. The main countries involved came together to negotiate, restart the peace process, and avoid a civil war. It was also to stop the political confrontations and rivalries in this state. After this meeting, Angela Merkel (*Germany (@bunderskanzlerin*), Guiseppe Conte (Italy *(@giuseppeconte_ufficiale*)), and Abdel Fattah al-Sissi (*United Arab Emirates (@alsisiofficial*)) all three published a photo, with different angles, where we can see different countries represented by their leaders (**Figure 7.4**). The German Chancellor even used one of the important communication elements on social media, a tagging. Mentioning other participants allows users and targets to be redirected directly to other diplomat accounts and to keep easier tabs on the world leaders.

Instaplomacy is reinforced by stories, where "world leaders meet, greet, and tag each other" (Twiplomacy.com, 2018). Diplomats can illustrate the good relations between their countries and each other. This can be highlighted by the meeting between French and Italian Presidents Emmanuel Macron and Giuseppe Conte on the latter's profile and between the German Chancellor Angela Merkel and Cyril Ramaphosa (*@cr17siyavuma*), the President of South Africa. In both stories, a fraternal embrace can be seen. Also, between the President of Senegal, Macky Sall *(@macky_sall*), and the Prime Minister of Canada, Justin Trudeau *(@justinpjtrudeau*), a post showed them walking beside each other, with an added text: "*The friendship between our two countries is strong and thriving*" (**Figure 7.5**). These two strong words could show the cooperation between the two countries and what the politicians wished to convey to their citizens.

Figure 7.5 *Screenshots of posted stories where diplomats meet in Berlin, January 2020. (Source: https://www.instagram.com/, 2020)*

On Instagram, world organizations' accounts make it possible to disseminate and make important information, news, and developments more accessible in a clear, attractive, and entertaining way. The European Commission (*@europeancommission*), the European Parliament (*@europeanparliament*), the Council of the European Union (*@councilofeuropeanunion*), and the Development & Cooperation of European Union *(@europeaid*) share the actions carried out and decisions taken by European organizations. Other aims and objectives could be strengthening and promoting European identity, integration, social cohesion, and social interaction.

Through this platform, Europe would show cooperation, interactivity, and solidarity between its member states, not only in the political area but also in the economic, social, and environmental spheres. Instagram has also been a platform to show, present, and promote a country's image to others (Manor, 2016). The French government's account for foreign affairs (*@francediplo*) once put in its profile picture an image representing the symbols of the French Republic: the flag with its colors and the head of Marianne, national personification representing the values and the motto of France "*Liberty, equality, fraternity.*" In the description, it is written "French Ministry for Europe and Foreign Affairs". In addition to the emoji of the flag of France, there is also the flag of Europe to emphasize its participation and integration within Europe (Da Costa, 2019).

7.9 Conclusion

Social media has marked a new era in the political scenery, affecting fields such as campaigning and political participation. These online tools have widened the availability of citizen engagement and opportunities for politicians to interact with their constituents. The increasing use of these technologies has transformed methods of government communication in online and offline environments, trying to bring the new generation to the political foreground. Campaigns have moved from an interpersonal amateurish stage of campaigning through the eras of the dominance of television to a hypermedia era where new tailored tactics have emerged. In the modern age, the gap between centralized and local is narrowing. Interpersonal communication, even face-to-face communication, can occur despite millions of miles. There are new ways to be social, which paradoxically involve being simultaneously isolated and connected. In modern politics, being social involves benefits and risks that need careful consideration. It also requires new skills which are moving into the electoral arena. However, what is referred to as new media does not work in isolation with old media,

and the hybridization and merging of platforms creates a new communication ecosystem where influence is dispersed, and consistency is hard to attain. There are many challenges as humanity moves to the online environment where awareness of all potential perils must constantly be in the portfolio of contemporary digital citizens.

References

Adesina S., and Olubukola, 2017. "Foreign policy in an era of digital diplomacy." *Cogent Social Sciences* 3 (1).

Adesina O.S., 2017. "Foreign policy in an era of digital diplomacy." *Cogent Social Sciences*, volume 3, issue 1., Available at: https://www.tandfonline.com/doi/full/10.1080/23311886.2017.1297175 [Accessed: 25 April 2020].

Alvarez A., 2017. "Does Twitter move diplomacy closer to the people? An analysis of US Embassies' Twitter presence across the globe." Texas State University.

Barbaro M., 2015. "Pithy, mean and powerful: How Donald Trump masters Twitter for 2016." *The NY Times*.

Bekafigo M. A., and McBride A., 2013. "Who Tweets About Politics?: Political Participation of Twitter Users During the 2011 Gubernatorial Elections." *Social Science Computer Review*, https://doi.org/10.1177/0894439313490405

Beyer J., 2014. *Expect us, online communities and political mobilization*. United States of America, Oxford University Press.

Bleiberg J., and Darrell M., 2015. "Political polarization on Facebook." Brookings. Available at: https://www.brookings.edu/blog/techtank/2015/05/13/political-polarization-on-facebook/ [Accessed 15 May 2017].

Blunden M., and Cecil N., 2018. "Facebook identifies 'political influencers' to spread ads to their friends online." Available at: https://www.standard.co.uk/news/world/facebook-identifies-political-influencers-so-it-can-target-ads-to-their-friends-online-a3892416.html [Accessed 15November].

Boffey D., 2018. "EU raises funds to fight 'disinformation war' with Russia." [online] *The Guardian.* Available at: https://www.theguardian.com/world/2018/dec/05/eu-disinformation-war-russia-fake-news [Accessed 6 September 2019].

Bosch T., 2021. "Twitter activism and youth in South Africa: the case of #RhodesMustFall." [online] Taylor & Francis. Available at: https://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1162829?journalCode=rics20 [Accessed 30 June 2015]. Available at: https://www.tandfonline.com/doi/abs/10.1080/1369118X.2016.1162829?journalCode=rics20 [Accessed 12 December 2021].

Brady H., Verba S., & Schlozman K., (1995). "Beyond SES: A Resource Model of Political Participation." *American Political Science Review*, 89(2), pp. 271-294. https://doi.org/10.2307/2082425

Cadwalladr C., 2020. "The Great British Brexit Robbery: How Our Democracy Was Hijacked." [online] *The Guardian*. Available at: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [Accessed 24 April 2020].

Carpenter C.A., 2010. "The Obamachine: Technopolitics 2.0." *Journal of Information Technology & Politics,* Volume 7, 2010 - Issue 2-3: YouTube and the 2008 Election Cycle in the United States.

Clarke A., 2010. *Social Media Political Uses and Implications for Representative Democracy*. Library of Parliament, Background Paper.

Clement J., 2020. "Instagram: distribution of global audience 2020, by age group." Available at: https://www.statista.com/statistics/325587/instagram-global-age-group/ [Accessed 20 April 2020].

Coëffé T. 2017. "Abonnez-vous à des hastags sur Instagram." Available at: https://www.blogdumoderateur.com/suivre-hashtags-instagram/ [Accessed: 25 April 2020].

Colona T.W., 2012. "Social Media and the advancement of America's Soft Power by public diplomacy." Washington, D.C, Georgetown University, Master, Available at: https://repository.library.georgetown.edu/bitstream/handle/ [Accessed 20 May 2020].

Commission E., 2018. "A Europe that Protects: The EU steps up action against disinformation." [online] Europa.eu. Available at: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_6648 [Accessed 6 September 2019].

Conover M., Ratkiewicz J., Matthew F., Gonçalves B., Menczer F., and Flammini A., 2011. "Political Polarization on Twitter." *Fifth International AAAI Conference on Weblogs and Social Media*.

Cornfield M., 2004. "The internet and campaign 2004: a look back at the campaigners." Available at: http://www.pewinternet.org/files/old-media/Files/Reports/2005/Cornfield_commentary.pdf.pdf [Accessed 15 May 2017].

Cozma R., 2013. "John H. Parmelee and Shannon L. Bichard. Politics and the Twitter Revolution: How Tweets Influence the Relationship Between Political Leaders and the Public." *Mass Communication and Society*. 16. pp. 460–463. https://doi.org/10.1080/15205436.2013.778286

Da Costa A., 2019. "What are Emoji? How and When to Use Them." groovypost.com, Available at: https://www.groovypost.com/howto/what-are-emojis-how-and-when-to-use-them/ [Accessed: 25 April 2020].

Davies R., 2014. "Social Media in Election Campaigning." Members' Research Service, European Parliamentary Research Service, Briefing.

Dezelan T., and Vobic I., 2016. "(R)evolutionizing Political Communication through Social Media." University of Ljubljana, Slovenia, February 2016,

Domonique J., 2016. "How Social Media Is Changing Political campaigns." *Global Risk Insights*.

Donaldson A., 2016. "The soft power of Twitter." Available at: https://www.britishcouncil.org/research-policy-insight/insight-articles/soft-power-twitter [Accessed 20 May 2020].

European Commission (n.d.). "Fake news and online disinformation - Digital Single Market - European Commission." [online] Digital Single Market - European Commission. Available at: https://ec.europa.eu/digital-single-market/en/fake-news-disinformation [Accessed 6 September 2019].

Farrell H., 2008. "Introduction: Blogs, politics and power: a special issue of Public Choice." Available at: http://www.henryfarrell.net/publicchoice.pdf [Accessed 15 May 2017].

Financial Times, 2019. "Why US politicians are turning to Instagram ahead of 2020 election." ft.com., Available at: https://www.ft.com/content/737d2428-2fdf-11e9-ba00-0251022932c8 [Accessed: 18 April 2020].

Gottfried J., and Shearer E., 2017. "Americans' online news use is closing in on TV news use." Pew Research Center, Available at: https://www.pewresearch.org/fact-tank/2017/09/07/americans-online-news-use-vs-tv-news-usehttps://www.pewresearch.org/fact-tank/2017/09/07/americans-online-news-use-vs-tv-news-use/ [Accessed 15 November 20].

Granovetter M.S., 1973. "The Strength of Weak Ties." *American Journal of Sociology*, Vol. 78, No. 6 (May, 1973), pp. 1360–1380.

Halim H., Mohamad B., Dauda S., Azizan F., and Akanmu M., 2021. "Association of online political participation with social media usage, perceived information quality, political interest and political knowledge among Malaysian youth: Structural equation model analysis." *Cogent Social Sciences*, 7(1). Available at: https://www.tandfonline.com/doi/full/10.1080/23311886.2021.1964186 [Accessed 11 December 2021].

Heinmans J., and Timms H., 2018. *New Power*. Great Britain, Macmillan.

Illing S., 2018. "How Russia pioneered fake news." [online] *Vox*. Available at https://www.vox.com/world/2018/4/5/17172754/russia-fake-news-trump-america-timothy-snyder [Accessed 6 February 2019].

John H. Parmelee and Nataliya Roman, 2019. "Insta-Politicos: Motivations for Following Political Leaders on Instagram." Available at: https://journals.sagepub.com/doi/full/10.1177/2056305119837662 [Accessed: 10 April 2020].

Jung Y., Tay A., Hong T., Ho J., and Goh Y.H., 2017. "Politician's Strategic Impression Management on Instagram." *50th Hawaii International Conference on System Sciences*. Available at: https://scholarspace.manoa.hawaii.edu/bitstream/10125/41420/1/paper0271.pdf [Accessed: 15 April 2020].

Kahne J., and Middaugh E., 2012. "Digital media shapes youth participation in politics." *Phi Delta Kappan*, 94(3), pp. 52–56. Available at: https://journals.sagepub.com/doi/abs/10.1177/003172171209400312?journalCode=pdka [Accessed 10 March 2019].

Karatas D., and Saka E., 2017. "Online political trolling in the context of post-Gezi social media in Turkey." International Journal of Digital Television, 8 (3), p. 383–401 [online] Available at: https://*doi*.org/10.1386/jdtv.8.3.383_1 [Accessed 17 January 2019].

Kosinski M., Stillwell, D., and Graepel, T., 2013. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the National Academy of Sciences*, [online] 110(15), pp. 5802–5805. Available at: https://www.pnas.org/content/110/15/5802 [Accessed 26 April 2020].

Kuhn P., and Crew A., 2006. "Best of blogs." Available at: https://books.google.gr/books?hl=lv&lr=&id=u10dqlBdE-8C&oi=fnd&pg=PT33&dq=best+of+blogs&ots=neBXfNz4-G&sig=PyGJX0Ds_KcHBqCbXZOevQji5dI&redir_esc=y#v=onepage&q=best%20of%20blogs&f=false [Accessed 15 May 2017].

Lilleker D.G., and Thierry Vedel T., 2013. Chapter 19: "The Internet in Campaigns and Elections." Bournemouth University Research, Bournemouth University, United Kingdom.

Manor I., Segev E., and Kampf R., 2015. "Digital Diplomacy 2.0? A Cross-national Comparison of Public Engagement in Facebook and Twitter." The Hague Journal of Diplomacy. https://doi.org/10.1163/1871191X-12341318

Manor I., 2016. "What is Digital Diplomacy, and how is it Practiced around the World? A brief introduction," *The 2016 Annual Review of the Diplomatist Magazine*, https://www.researchgate.net/publication/310952363_What_is_Digital_Diplomacy_and_how_is_it_Practiced_around_the_World_A_brief_introduction [Accessed 25 April 2020].

Martens B., Aguiar L., Gomez-Herrera E., & Mueller-Langer F., 2018. "JRC Digital Economy Working Paper 2018-02: The digital transformation of news media and the rise of disinformation and fake news An economic perspective," April 2018, European Commission, Joint Research Center.

Nulty P., Theocharis Y., Popa S.A., Parnet O., and Benoit K., 2015. "Social Media and Political Communication in the 2014 Elections to the European Parliament." LSE Research Online, London School of Economics and Political Science Mannheim Centre for European Social Research (MZES) TNS Europe.

Nyst C., and Monaco N., 2018. "State Sponsored Trolling: How governments are deploying disinformation as a part of broader digital harassment campaigns." Institute for the Future. [online] Available at: http://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf [Accessed 17 January 2019].

Ott Brian, 2017. "The age of Twitter: Donald J. Trump and the politics of debasement." Critical Studies in Media Communication. 34. pp. 59–68. https://doi.org/10.1080/15295036.2016.1266686 Available at:

https://www.researchgate.net/publication/311892973_The_age_of_Twitter_Donald_J_Trump_and_the_politics_of_debasement [Accessed 20 May 2020].

Owen T., 2015. *Disruptive power*. United States of America, Oxford University Press.

Pastor S., 2020. "Could 2020 be the year where youth participation finally takes off?". [online] *CitizenLab's Blog*. Available at: https://www.citizenlab.co/blog/civic-engagement/could-2020-be-the-year-where-youth-participation-finally-takes-off/ [Accessed 29 October 2020].

Polat R.K., 2005. "The Internet and Political Participation: Exploring the Explanatory Links." *European Journal of Communication*, 20(4): 435–459. https://doi.org/10.1177/0267323105058251

Rashica V., 2019. "Digital diplomacy: aspects, approaches and practical use, European Perspectives." *International Scientific Journal on European Perspectives*, volume 10, number 1 (17), pp. 21–39, Available at: https://www.europeanperspectives.org/storage/24/DIGITAL-DIPLOMACY_Rashica.pdf [Accessed 25 April 2020].

Saka E., 2020. *Social Media and Politics in Turkey: A Journey through Citizen Journalism*, Political Trolling and Fake News, London: Lexington Books.

Sandlow S., 2021. "CIRCLE poll finds increased youth engagement, participation in 2020 election." *The Tufts Daily* [online]. Available at: https://tuftsdaily.com/news/2021/02/08/circle-poll-finds-increased-youth-engagement-participation-in-2020-election/ [Accessed 8 February 2021].

Sarlin B., 2018. "Fake news went viral in 2016. This professor studied who clicked." [online] *NBC News*. Available at: https://www.nbcnews.com/politics/politics-news/fake-news-went-viral-2016-expert-studied-who-clicked-n836581 [Accessed 6 February 2019].

Serafinelli E., 2018. *Digital Life on Instagram*. New Social Communication of Photography, Emerald Publishing, Available at: https://books.google.gr/books?id=UTdpDwAAQBAJ&printsec=frontcover&hl=el&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [Accessed 25 April 2020].

Shear M., 2019. "How Trump Reshaped the Presidency in Over 11,000 Tweets." Available at: https://www.nytimes.com/interactive/2019/11/02/us/politics/trump-twitter-presidency.html [Accessed 20 May 2020].

Shearlaw M., 2016. "Turkish journalists face abuse and threats online as trolls step up attacks." *The Guardian*. [online] Available at: https://www.theguardian.com/world/2016/nov/01/turkish-journalists-face-abuse-threats-online-trolls-attacks [Accessed 17 January 2019].

Silverman C., and Singer-Vine J., 2016. "Most Americans Who See Fake News Believe It, New Survey Says." *BuzzFeed News*. Available at: https://www.buzzfeednews.com/article/craigsilverman/fake-news-survey [Accessed 15 November 20].

Silverman C., 2016."This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook." *BuzzFeed News*. Available at: https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook [Accessed 15 November 20].

Small T.A., 2011. "WHAT THE HASHTAG? A content analysis of Canadian politics on Twitter," *Information, Communication & Society*. Volume 14, 2011 - Issue 6: Networking Democracy?: Social media innovations and participatory politics.

Solo A.M.G., 2014. "Political Campaigning in the Information Age." *Maverick Technologies America Inc.*, Available at: https://books.google.fr/books?id=FRSXBQAAQBAJ&printsec=frontcover&dq=Political+Campaigning+in+the+Information+Age&hl=fr&sa=X&ved=0ahUKEwjYwPfvyM7oAhUGxYUKHa5LBiAQ6AEIKDAA#v=

onepage&q=Political%20Campaigning%20in%20the%20Information%20Age&f=false [Accessed: 25 April 2020].

Stieglitz S., and Dang-Xuan L., 2012. "Social media and political communication: a social media analytics framework." *Social Network Analysis and Mining*.

Stieglitz, S., and Dang-Xuan L., 2013. "Social media and political communication: a social media analytics framework." Social network analysis and mining, 3(4), pp. 1277-1291. Available at: https://link.springer.com/article/10.1007%2Fs13278-012-0079-3 [Accessed 10 December 2021].

Strombach J., and Kiousis S., 2014. "Strategic Political Communication in Election Campaigns." Semantic Scholar.

Stromer-Galley J., 2014. *Presidential campaigning in the Internet age*. United States of America, Oxford University Press.

Twiplomacy.com, 2018. "World Leaders on Instagram 2018." Available at: https://twiplomacy.com/blog/world-leaders-instagram-2018/ [Accessed: 25 April 2020].

Vagianos D., Al Zoampie S., and Spettel S., 2019. "The Rise of Social Bots in Cyberpolitics: Convenience in Cyberpower Redistribution." *Cyberpolitik Journal*, 4(7), pp. 71–73.

van Dijk T.A., 2001. "Critical Discourse Analysis." In D. Schiffrin, D. Tannen, and H. Hamilton (Eds.), *The Handbook of Discourse Analysis*, (pp. 352–371). Oxford: Blackwell.

Watt H., 2020. "Leave.EU Under Investigation Over EU Referendum Spending." [online] *The Guardian*. Available at: https://www.theguardian.com/politics/2017/apr/21/leave-eu-under-investigation-over-eu-referendum-spending [Accessed 24 April 2020].

Yepsen E.A., 2012. "Practicing successful twitter public diplomacy: A model and case study of US efforts in Venezuela." Los Angeles: University of Southern California, pp. 1-48.

Zavadskaya M., 2015. "Spreading protest: social movements in times of crisis," edited by Donatella della Porta and Alice Mattoni, Colchester, ECPR Press, *Contemporary Italian Politics,* 7:2, 203–205, https://doi.org/10.1080/23248823.2015.1039245

Chapter 8 E-government

Abstract

In this chapter, the implications of Internet use in public administration and the resulting local or global organizational change which aims at the empowerment of democracy and the support of public policies, are presented. The set targets for the governance to remain useful, legitimate, transparent, and efficient are highlighted. The EU action plan is described, and special case studies of European countries where the various components of e-government have been successfully implemented are listed: UK, Netherlands, and Estonia. The latter is considered a pioneering country in establishing effective and multifaceted e-government services, and therefore, it is more thoroughly analyzed to show that its public sector's dependency on IT systems has greatly benefited the state. Vulnerabilities and weaknesses, which others have exploited at an international level, are also highlighted.

8.1 Introduction

The rise of electronic government (from now on e-government) in the public administration field was noticed at least twenty years ago (Brown, 2005; Grönlund & Horan, 2004). This concept was developed at the end of the 20th century and was based on the idea of implementing an e-commerce method into the public sector. This led to implementing services for public administration agencies on the Internet (Spremic & Vrzica, 2008), using it as a governance tool.

The electronic governance may have two types of use:

1. E-services, refer to the electronic delivery of information, programs, and services of municipalities or the government. These e-services are constantly available to the citizens on a 24/7 basis.
2. E-administration, refers to the electronic management of data and the support of cross-departmental information flow. E-administration focuses mostly on the back-office processes aiming to develop new ways of service delivery.

Information and Communication Technologies (ICTs) provide a wide range of opportunities and potential for the support and transformation of the Public Administration domain in several countries around the world, with Member States (MS) of the European Union (EU) being among them.

It must be specified that the term *e-government* refers to the systems used to implement the services mentioned above, whereas e-governance refers to the functionality. Consequently, e-government means the application of ICTs in government operations, as a tool to make a better government. E-governance, on the other hand, implies the use of ICTs in transforming and supporting functions and structures of the administration system.

The concept of governance (Cambridge Dictionary, n.d.) defines the means, structures, and tools used to manage and regulate a state, an institution (public or private), or an authority, thus achieving better results and goals in terms of administration. It is also a pillar that eases the decision-making process of a body or organization in terms of management (Institute of Governance, n.d.). On the other hand, governance refers to a framework of policies (economy, growth, innovation, logistics and environment) being implemented in a country or state to benefit the people. In other words, the term above illustrates a spectrum of good practices where a government interacts with its citizens and the citizens communicate their opinions towards their government using several online tools.

Considering the aspects and definitions above, electronic governance defines the services and the policies implemented for the benefit of citizens through online public services and platforms. E-governance is a double rotation system that facilitates the shareholders' interactions through a more immediate and less bureaucratic administrative path. It set up a framework for a better communication between governments, organizations, and citizens in all possible combinations, using online platforms that have been properly tailored to deliver a specific service (Belgian Development Agency, 2017).

According to the definition of the Digital Divide (chapter 5), not all countries are favored from E-governance. The Western world and the industrialized countries (e.g. MS of the European Union, USA, Israel etc.) were among the pioneers in adopting e-governance techniques. Poverty, lack of resources and infrastructure, low internet diffusion, unskilled personnel and authoritarian regimes are the main obstacles to implementing public administration online services (Schuppan, 2008). For this reason, e-governance can be envisaged as a Western world product and as a democratic evolution that occurred through technological progress, serving the needs of the citizens as a part of e-democracy.

After all, on many occasions, technology is regarded as a tool that governments can improve the services delivered to the citizens and regulate their performance (OECD, 2008). In this process, national public organizations preserve a great amount of information, competence, and knowledge, and their effective and

competent handling requires the abolition of frontiers, geographical distance, and the challenges of national bureaucracy (Karacapilidis et al., 2004).

8.2 The Evolution of E-governance

The theoretical framework of electronic governance hails from the theory of cyberspace and governance. The term cyberspace originated from the Greek word *κυβερνήτης/κυβέρνηση* (= governance), which means the ruler or the governor of a body. Cyberspace is a virtual field being created through networking internet channels, where human bodies can communicate, face and tackle problems and challenges caused by technological advancements in the field of the internet. Each person can deliver their values, virtues, norms and activities in this virtual space.

Baron de Montesquieu (De Montesquieu, 1748) states that a government has three powers: judiciary, legislative, and executive. E-governance is the implementation of the above branches on a daily form using IT means. The Gartner group (Noman & Hebbar, 2016) conducted a research study in 2000, to identify the evolution stages of e-governance. This research identified four stages (**Figure 8.1**) that had already driven the evolution of e-governance as it is known nowadays. The first stage refers to "*presence,*" where a government transmits information through websites, platforms, links to ministries and governmental authorities, archived files, and documents that are available to citizens online. In other terms, governmental data is “projected” online. The second phase is "*interaction*" between a government and its citizens, economic factors and the state. For instance, a government can create electronic tax service platforms where visual interfaces or downloadable applications implement tax services.

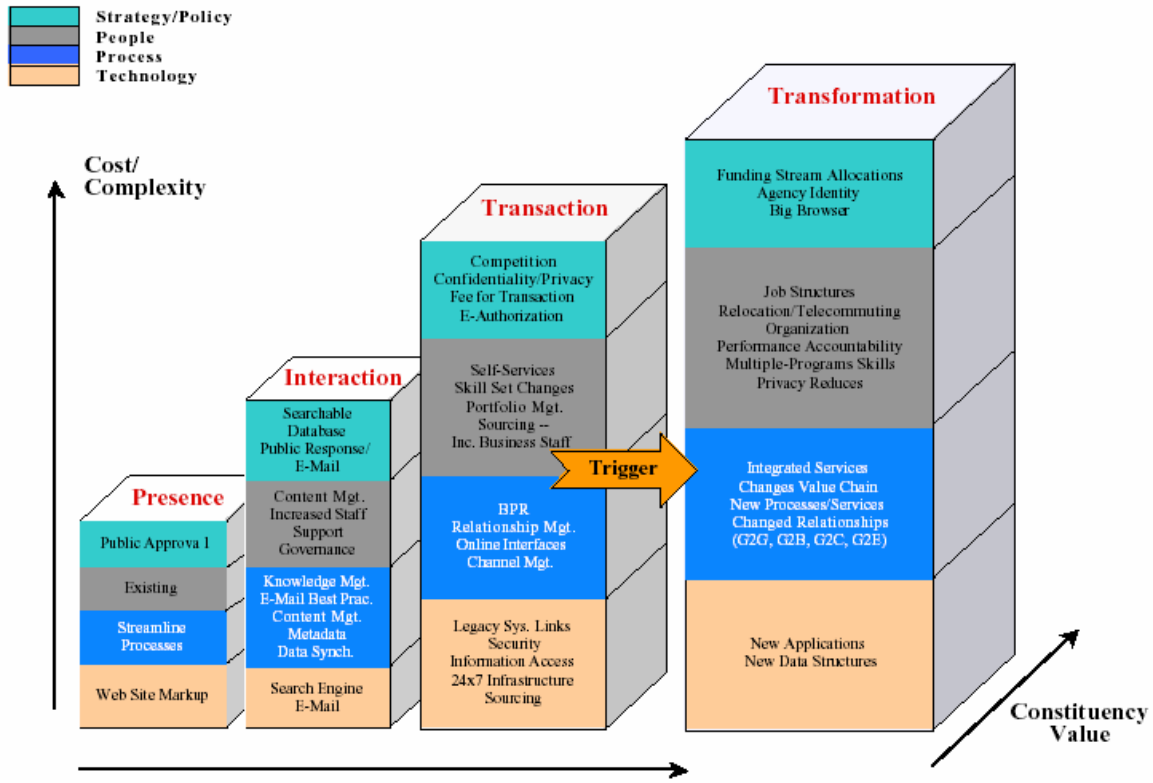


Figure 8.1 *Gartner’s Four Phases Model (Di Maio, 2003).*

The third stage, *“transaction”* allows citizens to execute their financial transactions online. They can pay their taxes online using credit/debit cards, etc. The final evolutionary stage of e-governance is the *“Transformation,”* where Projects are mature enough to introduce changes and reinvent the government’s

existing processes and functions. This transformation leads to further developments of e-governance and adds value to the system.

8.3 The Essence and the Main Types of E-government

In the previous paragraphs, it has been mentioned that e-government is a part of the New Public Management and involves the application of the private sector methods into the public administration sector (Grönlund & Horan, 2004, p. 718). E-government includes four main elements (Abu-Shanab & Bataineh, 2014; Baptista, 2005):

- The provision of digital services to the citizens and the entities,
- The improvement of the performance of governmental bodies and agencies,
- The provision of digital tools that promote and enhance democracy,
- The promotion of participation and social inclusion.

More specifically, e-government entails new techniques and practices while focusing on the electronic delivery of services in different public administration domains (Centeno et al., 2005). Many different definitions can be found for the meaning and the content of e-government. It has been explained as *"the delivery of government information and services online through the Internet or other digital means," as "using the internet and the world wide web for delivering government information and services to citizens, business and other government agencies," as "utilizing of information and communication technologies (ICT) for developing and improving the relationship between government, citizens, businesses and other government entities" or as "the use of information and communication, technologies particularly the Internet, as a tool for delivering better government services to the citizens, businesses and employees"* (Alshehri & Drew, 2010). Therefore, it is apparent that e-government constitutes a broad concept that describes the use and exploitation of ICTs in such a way that public administration can be transformed in order to promote the accountability, transparency, efficiency, effectiveness, and availability of public services (Ardielli & Halaskova, 2015).

Over the years, some types of e-government have been developed, depending on the participants of the digital services that interact with each other (Spremic & Vrzica, 2008). Therefore, the most important of them are the following (Spremic & Vrzica, 2008; Beynon-Davies, 2007):

1. The first type is the internal e-government, which is related to establishing of internal procedures within government agencies through ICTs. Moreover, it entails the management of the workflow and knowledge within the public administration.
2. The second type is the *Government to Citizens* (G2C or *administration to citizens* (A2C), which deals with the interaction between the agencies and the citizens, in which the citizens are treated as customers or clients.
3. The third type of e-government is the *Government to Business* (G2B), developed between governmental agencies and private sector entities.
4. The fourth type of e-government is the *Government to Government* (G2G), which deals with achieving intragovernmental collaboration and cooperation.
5. The fifth type of e-government is *Citizen to Citizen* (C2C). It is provided through modern web applications (e.g., social networks), which allow various citizens to communicate with each other from different levels and categories of society over the Internet.

Those types are depicted in the figure that follows (**Figure 8.2**).

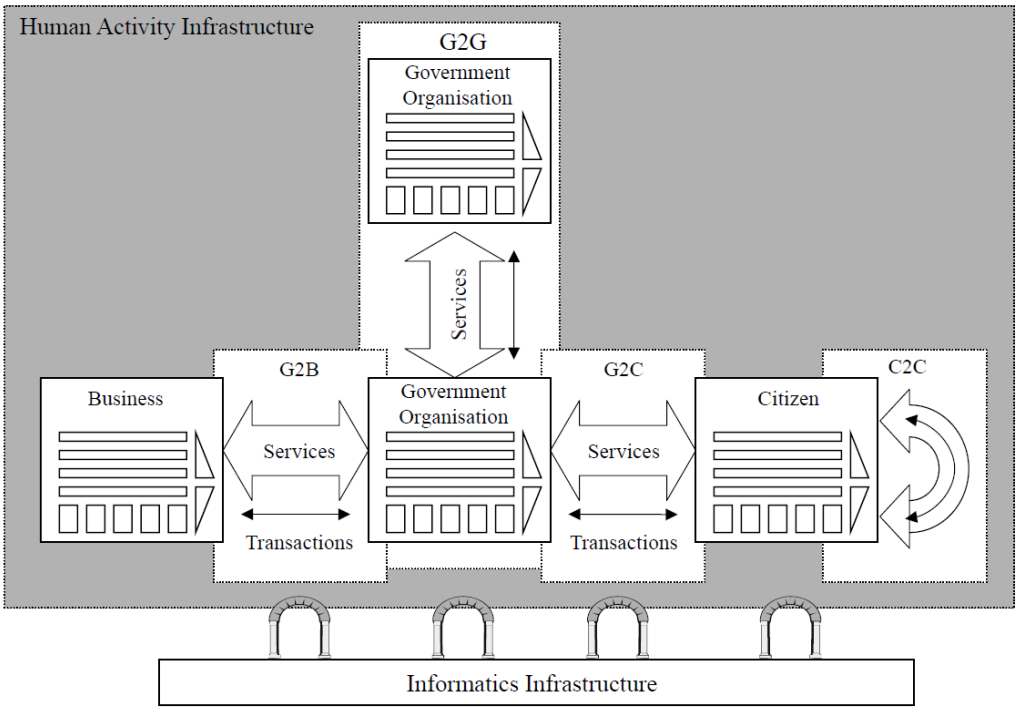


Figure 8.2 *Forms of e-government (Beynon-Davies, 2007, p. 13).*

G2C, G2B and G2G are more thoroughly analyzed in the following paragraphs.

8.3.1 Government to Citizen (G2C)

Government to citizen (G2C) aims to provide individuals with online access to information or services. Citizens should be able to find and access what they need quickly and easily. The e-government category focuses on interactions between the government and citizens, supporting transactions such as tax payments, driving licenses, or obtaining passports. Government to citizen interactions can allow citizens to be more informed about government laws, regulations, policies, or services. For the citizen, this e-government type can offer a huge range of information or services, including government forms or services, public policy information, employment or business opportunities, voting information, tax filing, license registration or renewal, payment of fines, and submission of comments to government officials.

8.3.2 Government to Business (G2B)

Government to business (G2B) aims to reduce burdens on businesses, provide one-stop access to information, and enable digital communication. Moreover, the government should reuse the data reported appropriately and use commercial electronic transaction protocols. The e-government category focuses on interactions between the government and various organizations, including businesses or nonprofits, supporting transactions such as contract bids, data collection, and grants. It involves selling government services and goods and procurement facilities, entailing benefits for businesses and governments. For businesses, government to business interactions can result in increased awareness of opportunities to work with the government, cost savings, and improved efficiency in transactions. For governments, government to business interactions offer benefits in reducing costs and increasing efficiency in procurement processes, plus providing new avenues for selling e.g. surplus items.

8.3.3 Government to Government (G2G)

Government to government (G2G) is the electronic sharing of data and/or information systems between government agencies, departments, or organizations. The goal of G2G is to support e-government initiatives by improving communication, data access, and data sharing. Several factors are driving local and federal governments to institute G2G initiatives. One of its themes is federal government legislation such as the Open Government Directive. Budgets and funding are also driving G2G initiatives. By sharing information and systems, governments can reduce IT costs, and government offices can be more efficient and streamline procedures, allowing citizens to access information over the internet. They may also qualify for grant funding, depending on the project. An example of a successful G2G project is the Northeast Gang Information System (NEGIS) in the US. States in the northeast of the US use NEGIS to share information about street gangs, including gang-related activities and gang intelligence. The system connects all the state police departments of the participating states, and the police departments transmit the collected information to other states' law enforcement and public service agencies.

8.4 E-government and Democratic Participation

The 21st century is characterized by the novel problems of political apathy and the loss of public confidence in constitutional functions. The public domain, in which political dialogue and deliberation take place, has been described by Jurgen Habermas as the *Public Sphere*. (Habermas, 1991). Habermas counterposes the old feudal public sphere with the newly emerged *bourgeois* public sphere. The former was restrained by secrecy and disenfranchisement, while the latter had three main characteristics: universal access, autonomy, and equal status to the opinion of each member. Within the public sphere, individuals express their arguments, use reason to judge each other's input and reach some form of deliberation or consensus.

The OECD identifies a lack of trust in the government as a factor that hinders the successful application of policies and the willful participation of citizens and businesses in economic recovery. To remedy the lack of trust, the *Organisation for Economic Co-operation and Development* (OECD) lists six possible tools:

- Reliability,
- Responsiveness,
- Openness,
- Better regulation,
- Integrity and fairness,
- Inclusive policy making.

Responsiveness, openness, and inclusive policy making can be addressed using modern technologies. By the time Habermas laid out the *public sphere* theory, the internet had yet to be invented, not even in the most rudimentary form. This means that the prospective applications of the internet were separate from his evaluation of how citizens can get together and discuss with each other. Even after the creation of the Internet, the medium would not satisfy the requirements of being labeled part of the public sphere if it were not for a set of new capabilities summarized in the term Web 2.0. This evolved stage of the World Wide Web perceives the network "*as a platform, spanning all connected devices [...] creating network effects through an 'architecture of participation' and going beyond the page metaphor of Web 1.0 to deliver rich user experiences*" (O'Reilly, 2005).

As analyzed in Chapter 7, citizens are no longer required to be information consumers in a one-way flow. They can contribute material and improve their collective experience of the web. All without the need for specialized technical knowledge. In other words, a user does not have to create a website to broadcast

their message to the world. They can utilize one of the hundreds of such existing applications and make their ideas, their audiovisual material, their data available for other users to view and respond to.

In the following two paragraphs, two types of available e-government platforms that enhance democratic participation are presented: Top-down government platforms and bottom-up non-profit platforms. Both have been conceived to implement the aspirations for an open political life through the internet. Two corresponding exemplar platforms from Greece are outlined.

8.4.1 Top-Down Platforms: The Case of OpenGov (opengov.gr)

Top-Down platforms are usually state sanctioned platforms, run by governmental agencies and on governmental budgets. With the diffusion of digital technology in all other aspects of their life, citizens grew the expectation of enjoying such an advancement in the activities of their government (Coleman & Blumler, 2009). To meet this demand, governments sought to design information portals or deliberation models that that the national or local government hosts to invite citizens to participate in the political process.

OpenGov (www.opengov.gr)is a representative project set up by the E-governance working group of the Greek Prime Minister's Office in 2009.It has been operated by the Greek Ministry of Administrative Reform and E-governance. It used to be the flagship of the G. Papandreou administration regarding the modernization of governance and including citizens in decision-making process. The platform initially had two main functions:

1. Displaying draft governmental bills for public deliberation. Deliberation is hardly the term, though, because all user comments are only advice that can be considered by the respective ministers who handle the draft bill. The platform provides information about all planned legislation, and allows for quick comments without a pre-existing registration. The access is again hindered, however, by the exclusion from the commentary of whichever articles the minister wishes to.
2. Publishing calls for job positions in government organizations and public institutions. This part is not connected with participation in governance, but it still contributes to transparency in how public job positions are staffed.

A side project of OpenGov was the platform of Labs.OpenGov (http://labs.opengov.gr/). The project worked as follows: A scientific committee was designating a topic for each period (cycle) and called for ideas. Each idea should identify a related problem and suggest a solution. The submissions were published and were subject to commentary and rating by the Labs.OpenGov users. After public deliberation, ideas were evaluated by the scientific committee and were categorized according to maturity. By 2016, the platform had completed five thematic cycles of submitting, evaluating and presenting ideas.

8.4.2 Bottom-up Digital Democracy: The Case of Vouliwatch (VouliWatch.gr)

The bottom-up type of online participation platform is administered by a non-governmental organization or other similar civil society entity (Coleman & Blumler, 2009). This bottom-up approach allows for many attempts with different focuses and characteristics. While many of them never gain momentum or fail to meet the financial and logistical needs of scaling up their platform, a few make the cut. Of course, as the domain of online democratic participation is a new one altogether, it is too early to judge if these platforms substantially impact on political life and the sense of inclusiveness by the citizens. Parliamentary observatories are a popular subcategory of these platforms. To increase accountability and transparency in the political system and encourage a broad participation in politics, the observatories host public discourse concerning a parliamentary institution. Depending on the availability of resources and materialization, parliamentary observatories can escape from being static repositories of information and become interactive spaces where citizens debate with one another and monitor their members of parliament.

Vouliwatch (VouliWatch.gr) is a parliamentary observatory run by an independent non-profit organization that aims to bring the citizens close to the workings of the Greek parliament. It began in March 2014 with a team of six young professionals who had observed similar projects abroad and wanted to introduce the model of parliamentary observatories in Greece. They employed the same company that had created the online information platforms *Diavgeia* and *OpenGov* for the Greek state. The result was considerably more interactive and user-friendly than the two applications above.

The website featured some static content, such as general information about the functions and regulations of the decision-making bodies (the Greek Parliament and the European Parliament). Users could browse the profiles of Greek MPs, filtered by district or party, or search directly for the MP that is of interest to them. The *Vouliwatch* editing team has been publishing various articles covering parliamentary activities and policies under discussion. A very interesting function of the platform has been the recording of parliamentary activities and votes of MPs.

Users could engage in the following parliament-related activities:

1. Ask questions to the MPs of the Greek Parliament or MEPs of Greece. This is followed up with a compilation of statistics, displaying the trends in citizen's questions and the MP's rate of response
2. Submit ideas for resolving common problems, discuss them, and rate other user submissions.
3. Compare the policy of the parliamentary parties on specific issues (Policy Monitor).
4. Undertake a quiz based on the information about the institutions available on *Vouliwatch*.

As a non-profit endeavor, *Vouliwatch* has been collecting funding donations and public grants. In the 16/03/2015–16/03/2016 period, 9% of the organization's budget had come from European Union projects, 59% from foundations and public grants, and 32% from private donations.

Public officials and MPs treat projects like *Vouliwatch* with a lack of confidence. The Greek political system is plagued by mutual distrust as citizens' confidence in public institutions collapses, and politicians are suspicious of every grassroots attempt as a possible platform for opposition. As the Chief Executive of *Vouliwatch* has stated (rejoin.gr, 2015), the members of the Greek parliament were reluctant to participate because they were wondering whether the project had some partisan agenda or whether their input would be distorted before being broadcast. This was coupled with the technological illiteracy of some older MPs, but this is gradually changing as a new generation of statesmen are elected and enter the parliament.

Despite these shortcomings, *Vouliwatch* has managed to gain publicity on the domestic as well as the international level. *Vouliwatch* has banded together with eight similar initiatives from other countries and created the *Parliament Watch Network*. The degree of interaction between MPs and citizens through submitted questions is constantly increasing.

8.5 The Benefits of E-government

From the very first conception of e-government, it was expected to bring a wide range of benefits; hence, it was considered an element of great significance in public administration. The anticipated benefits of e-government can be numerous: transparency of public administration, improvement of the services provided, augmented satisfaction of the citizens served, acceleration of the procedures, efficiency, and accountability, promotion of accessibility etc. (Centeno et al., 2005).

More specifically, e-government is a tool that can create a digital state and achieve the delivery of public services and the provision of information to the citizens through electronic ways and applications of the ICTs (Meiyantia et al., 2018, p. 2). On that basis, e-government has affected the delivery of public services in a significant way and has changed the environment of public administration (Brown, 2005). As such, many

benefits and opportunities are provided not only to citizens, businesses, and governmental entities (Centeno et al., 2005).

The governmental and public administration structures are reorganized, modernized, and improved. The processes are simplified through ICTs, which leads to better service for the citizens at a lower cost. This can be achieved through streamlining and the reorganization of the operating processes. The public performance of government agencies is upgraded and improved. The services are delivered effectively and efficiently despite long distances and towards all the customers. Through e-government, the service operations of the governments are economized and improved, and transactional costs are reduced while transparency is increased. Moreover, the time spent, effort, and costs of the customers are reduced (Alshehri & Drew, 2010). A well-founded public administration culture is developed that puts the clients (citizens and businesses) and their needs at the center of the interest and the procedures. Efficiency is acquired with the reduction of the cost. The value of the public administration is augmented, financial management is improved, effectiveness is achieved, and at the same time, the citizens have access to a great range of information on a 24/7 basis, leading to the participation of the citizens and their accessibility to procedures and information, and the enhancement of accountability, democratic values, transparency and openness (OECD, 2003).

As a result, there is an improvement in the quality-of-service delivery, which in turn improves customer satisfaction. New businesses are created, linked to the augmentation of work opportunities. Apart from that, the efficiency of the government is achieved and promoted in the field of data and information processing. There is a better understanding of the users' demands, leading to improved and seamless online services. Government agencies exchange ideas and information with one another, making it possible to build enormous databases that are used to continuously provide citizens and other entities with public services. All of the above, enhances citizens' trust in governments, democracy, and democratic procedures and processes. Consequently, good government practices are established (Alshehri & Drew, 2010). Therefore, it is easy to understand that e-government ensures efficiency, speed, and improvement of public services and achieves the competitiveness and modernization of public services (Centeno et al., 2005).

The following sections, examine the concept of e-government within the European Union. At the same time, its importance, the benefits it provides and the weaknesses and challenges for its implementation are outlined.

8.6 E-government in the European Union and the Member States

Since e-government is considered an area of great importance in the European Union, the European institutions have published many relevant documents from 2000 until today (ReSPA, 2018). Its importance lies in the fact that the EU has gone through many transitions of a social and economic nature due to its enlargement: cultural diversity, religious diversity, the aging populations, and the changing conditions of living, working and the consumption patterns. All these elements are a great challenge for delivering public services. Within the Single Market, with enhanced cooperation, new public services and innovative ways are required to deliver the existing public services. On that basis, e-government is considered the center of gravity of European public management's reform and modernization. Technology is used as an important tool for the modernization of structures and processes, for the improvement of the regulatory framework of public administrations and human resources structures, and in general, for the establishment of a culture of innovation concerning public administration. This means that public value is generated through e-government in the EU, and better governance is achieved. Public value includes the democratic, economic, social governance, and environmental roles of the national governments (Centeno et al., 2005). ICTs are regarded as a means to improve the public administration and services of the members by creating pan-European governance that lies in the creation of a network of the MS' administration (local, regional, and national) across

the Union and on the emergence of an integrated public space with a European character. On that basis, the concept of interoperability of the public services of the member states has risen (Misuraca et al., 2011).

For the reasons stated above, e-government was included in the political agenda in the Lisbon Strategy in 2000. It belongs to the European Information Policy and enhances the established information society (Ardielli & Halaskova, 2015). The most important initiatives for the public sector's modernization through e-government are the Action Plan for e-Government 2016-2020 and the European Commission Communication on the European Strategy for a Single Market. The main principles of those documents have been confirmed by Tallinn's Declaration in 2017 (Floria et al., 2019), while many MS have adopted strategies, action plans, and roadmaps in order to achieve the digitalization of their public administration system and to promote interoperability (Directorate - General for Informatics, 2019).

In the Action Plan 2016-2020, it is accepted that the main aims are (European Commission, 2016):

- The modernization of the public administration and the delivery of public services to European citizens and businesses.
- The enhancement and promotion of cross-border mobility.
- The facilitation of the digital interaction within the Union between the citizens-businesses and the public administration agencies.

Therefore, the Commission concludes that e-government must be developed in such a way that (European Commission, 2016):

- Digital services are ensured,
- The citizens and the businesses provide only once to a public administration their information,
- Inclusiveness and accessibility of the clients is ensured,
- Openness and transparency serve as the main principles,
- E-government will have a cross-border character in order to enhance the Single Market,
- Interoperability shall be guaranteed,
- Security and trustworthiness of the data and info is essential.
-

In 2018, the European Commission, examined the situation of e-government between the MS and has set three indicators for this evaluation: the online availability of services, the usability standards (support, help and feedback online) and how friendly the m-services provided are (European Commission, 2018). Some of the results are presented in the following figures.

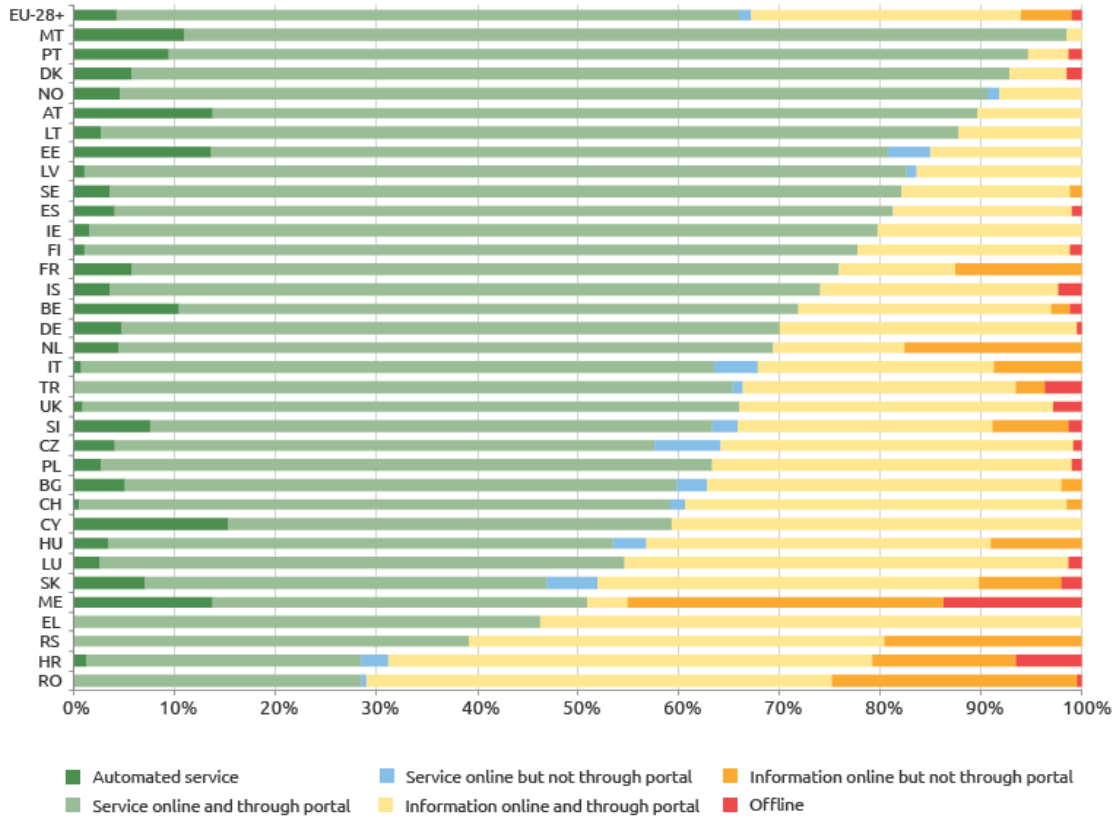


Figure 8.3 *Online availability of public services per member state average (2016-2017). (European Commission, 2018, p. 32)*

It can be understood (**Figure 8.3**) that different online availability levels can be found between the MS, while Malta, Portugal, and Austria provide more than 90% of the public services online. Portugal, Austria, Cyprus, and Estonia automatically provide more than 10% of the public services.

Figure 8.4 *Online availability of public services per MS (2016-2017 average) (European Commission, 2018, p. 35).*

In all the members, the results are satisfying for the online availability of public services (**Figure 8.4**), while up to almost 70% of the services online were national, up to 65% regional, and up to 49% local. The same satisfactory results are to be found in the usability of services (**Figure 8.5**).

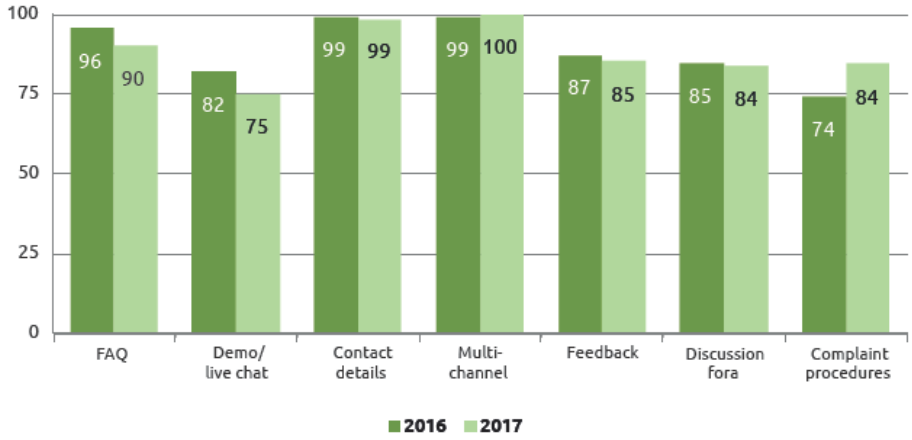


Figure 8.5 *Availability of online support (2016-2017) (European Commission, 2018, p. 37).*

Finally, the UK, Denmark, Iceland, Malta, Sweden, France, Belgium, and the Netherlands have set interesting examples for mobile friendly services (**Figure 8.6**).

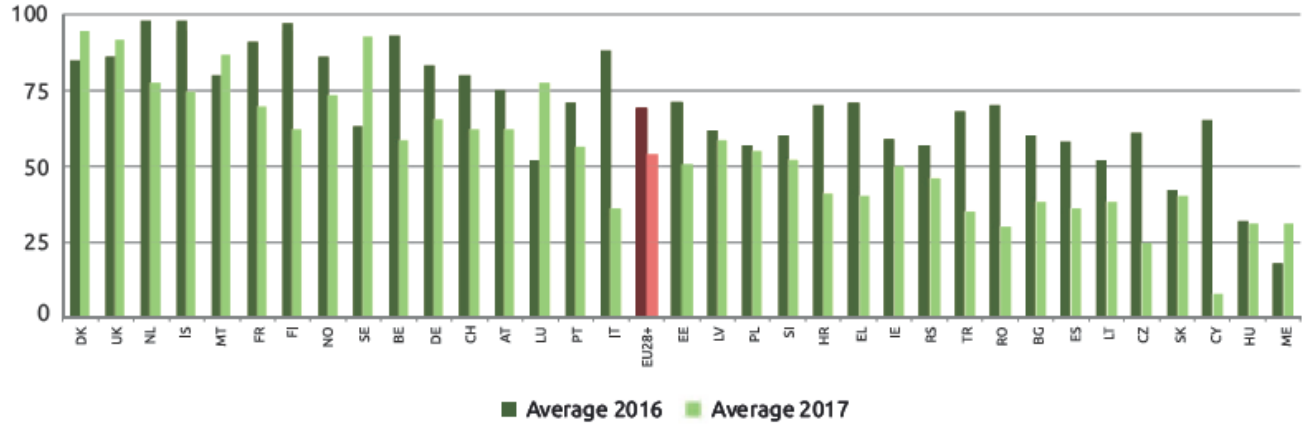


Figure 8.6 *Mobile friendliness 2016-2017 (European Commission, 2018, p. 38).*

From what has been stated above, e-government in the EU has reached an upgraded level. However, it cannot be neglected that many challenges can be observed that impede the full implementation of the Commission's Action Plan. Firstly, e-government requires a high level of collaboration and participation of the national public administrations of the MS, which takes place at a different pace (Karacapilidis et al., 2004). Creating and implementing a transnational e-government agenda is a difficult task, and it can be regulated firstly at a national level since the Union is not competent in the organization of governments and public administration of the MS (Baptista, 2005).

Firstly, there are infrastructure challenges that include the technological capabilities and challenges of a technological nature. The member states have different technological capabilities, while financial support and investments are required for the infrastructure acquisition. All the administrations must adopt a clear business and sustainable model to realize e-government and interoperability (Abu-Shanab & Bataineh, 2014).

Moreover, e-government at a national, and afterward, pan-European level must be achieved in a way in which knowledge has to be appropriately managed in what has to do with governance. At the same time, democratic procedures must be implemented with transparency, efficiency, speed, and effectiveness. In any case, the needs of the citizens and the businesses have to be taken into account since the citizens and the businesses constitute the clients of e-government. Moreover, it is important to incorporate several

intermediaries that will play a crucial role in both the services and the democratic processes. Finally, networking, coordination, and collaboration are required to promote a better form of governance. This means that e-government requires a knowledge-based, distributed, and networked system to succeed in the MS and in the EU (Centeno et al., 2004).

Unfortunately, the use of ICTs in the field of e-government in most of the MS is centered on promoting the efficiency and the quality of the services. It has not enhanced the democratic processes concerning the promotion of the political participation of citizens. Up to a theoretical level, e-government enhances the participation of the citizens, but in practice, this is not fully implemented. The same applies to policy formulation and the participation of the citizens. After all, good modern governance is not only about the quality of services but involves as well "*democratic and cooperative policy formulation, citizen and civil society involvement, transparent and participative implementation of policies, as well as continuous independent evaluation of their results, and accountability of public decision-makers so as to improve policy making in the future*" (Centeno et al., 2005). On that ground, it has been supported that in the context of the EU, this link between the e-government and improved governance, as explained above, has not been achieved.

On art from ICTs, political engagement and long-term strategies are crucial for e-government success. On many occasions, multiple ambitious and, in many cases, contradicting goals of e-government set out by the MS have been observed (Centeno et al., 2005). At the time being, there is a gap in the ambitions of the MS concerning e-government, leading to problems in implementing the pan-European e-government goal (Bershadskaya et al., 2013).

Furthermore, a crucial challenge is the interoperability issue and the standardization in the MS. Interoperability is not an easy task as the European Commission has stated: *"…the approaches and solutions for interoperability will differ, depending on the e-government services concerned and on the environment in which the services are implemented"* (Misuraca et al., 2011). Due to differences in the public administration concerning structure, culture, strategies, powers, and competences, along with procedures combined with different e-government platforms, interoperability can be jeopardized. Therefore, political engagement appears again alongside the need for structural transformation of the national e-governments. This requires a social transformation in the MS so all of them can understand the meaning and importance of creating a client-centered system that promotes democracy, efficiency, transparency, and accountability (Centeno et al., 2004).

Last but not least, it should be mentioned that budget issues, educational and training programs' differences, as well as the regulatory and legislative differences among the MS constitute a great challenge in implementing the EU e-government, emphasizing the need for harmonization and the provision of economic support (Bershadskaya et al., 2013; OECD, 2003).

8.7 Estonia: A Pioneer of E-governance

The country of Estonia is undoubtedly recognized as one of the global leaders in cyberspace and as one of the pioneers in developing governmental e-services. Even though it is most known for the breakthroughs in the field of cyber defense, which were initiated after the 2007 cyber-attacks (see Chapter 12), the country's digital transformation had already begun in the mid-1990s.

The following paragraphs provide an overview of the Estonian State's digital transformation, which includes the following:

- An analysis of the previous infrastructure that laid the basis for the digital solutions that were adopted.
- The legal context and the administrative characteristics of this effort.

- Four e-solutions the state has adopted that fall under the larger ecosystem of e-services.
- A summary of the overall process and the argument that led the country to use digital transformation to exert soft power.

8.7.1 The Road to E-Estonia: A Historical Overview

Estonia began investing in its Institute of Cybernetics as early as the 1960s.While similar institutes in other Soviet Republics focused on maths and engineering, the Estonian institute concentrated on computer programming. After it broke away from the Soviet Union in 1991, the country had to be rebuilt from scratch, and since the resources were poor, Estonians took advantage of the rising invention of that time: the Internet. Both the IT community and the political reformers were advocating in favor of utilizing the capabilities this invention offered; on the one hand, the IT specialists were interested in putting their knowledge into practice and, on the other hand, the political leaders were searching for means to achieve an efficient and minimal government. The contribution of these two agents came in terms of rulemaking and provision of services based on private sector developments. The former socialist country followed a more open model in terms of political development, and except for the foundation of tech companies such as *Skype,* the liberal economic regime and sound financial policies benefited the birth of the banking sector, which became an influential IT innovator by introducing Internet banking in 1996.

The first step seen as a great boost for developing country's information society was the "Tiger Leap" program. In 1996, Estonia took up the challenge of catching up with the West "*by updating local IT infrastructure and establishing computer skills as a priority in schools"* (e-estonia.com, n.d.). Even though the program emphasized on education, it was the first initiative largely supported by the state. Today's success lies in two building blocks: the Data Exchange Layer X-Road and the electronic Identity (eID). The preparations for these two started the same year by establishing the basic principles of the information society and creating the relevant infrastructure.

8.7.2 The X-Road

Estonia's "data backbone" is X-Road, a concept first introduced in 2000. Due to limitations to its financial resources, the government of Estonia needed a "central toolkit" to create all government institutions' information systems (Maarit et al., 2017). The first version of the X-Road (**Figure 8.7**) was named X-tee, and it was not a fundamentally new invention. Estonia harnessed then-existing technologies and applied them novelly in the state governance context (x-road.global, n.d.). The outcome of this innovative application of existing technologies was launched in 2001 and enabled the flow of data information between citizens, public institutions, and private companies. X-Road was vital for Estonia; without it the government would have to set up a Central Super Database or establish a company that would move data storage devices between municipalities and agencies across Estonia (x-road.global, n.d.).

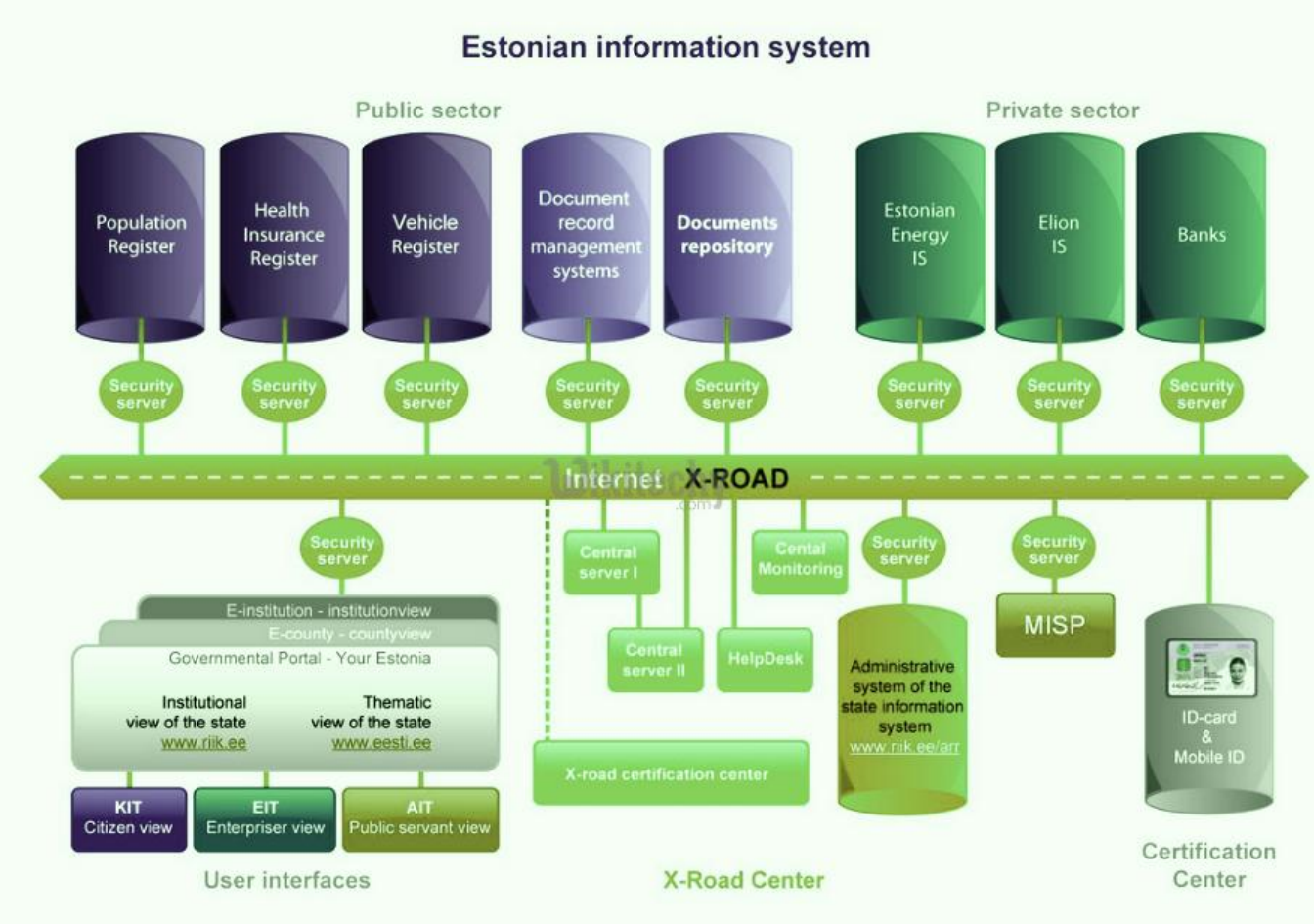


Figure 8.7 *X-Road (Goede, 2019).*

The three pillars of X-Road and its predecessor are data availability, integrity, and confidentiality. Data availability can be taken for granted if the platform operates properly. Moreover, the integrity of the data is guaranteed because each time data is transferred, all outgoing data is digitally signed and encrypted, and all incoming data is authenticated and logged (x-road.global, n.d.). Thirdly, confidentiality is safeguarded by limiting data access to those authorized people working within member organizations. Thus, it is a secure internet-based data exchange layer that facilitates the communication of different information systems. Moreover, X-Road functions upon the "once only" principle, which means that information is inserted only once in the platform, and when an institution needs access, it is retrieved from the information system where it is saved. One of the most important features of X-Road is its decentralized nature, as it does not have a monopoly over individual data repositories belonging to the institutions it hosts. (Vassil, 2016).

Substantially, X-Road is a platform where any state institution can extend their physical services into electronic ones. For instance, when an institution or a private company wants to develop an online application, they can apply to join the X-Road. Automatically, they are given access to a number of services that determine the vital components and the application design. Such services are client authentication, registry services, visualization environment, etc. Once an institution has access to the X-Road, it has to share its data with others if required. Particularly, institutions are encouraged to share their data in order to avoid the repetition of data. However, only via agreements with each particular data provider will an organization be able to access other members' data.

Organizationally, the X-Road Centre responsible for the well-functioning of the X-Road was established within the Estonian Informatics Centre, and up to the present, its operation is ensured by the central

government, primarily by the Estonian Information System Authority (Vassil, 2016). The X-Road is regulated by the X-Road Regulation (2003), a very laconic document that has been amended twice since its adoption. The first time was in 2008, when the amendments were introduced to the Public Information Act (2008), and the second in 2016, aiming to harmonize the new EU Directive on Trust Services and eID, known as eIDAS (Maarit et al., 2017).

8.7.3 E-identity

The second building block is developing a *"comprehensive system for electronic identification, authentication, and digital signature"* (Maarit et al., 2017). Estonia is said to have the world's most highly developed national ID card system.

Primary electronic identity comes with a physical ID card, a mandatory identification document in Estonia. A citizen's identity in Estonia is discerned with a personal identification number (PIC), which is also the core element of the country's identification system. The 11-digit PIC is printed on the physical ID card and stored on its chip, which carries embedded files. Therefore, it can be used to prove a person's existence in the electronic environment. Moreover, the ID card is based upon the so-called public key infrastructure. In principle, an encryption key pair is utilized: a public encryption key and a private decryption key. These two keys used for signing and authentication are protected with two respective PIN codes.

In addition to the physical ID card, mobile ID and E-residency cards are also issued. Mobile ID allows people to use a cell phone as a secure digital ID. Like the ID card, it can be used to access secure e-services and digitally sign documents, but it has the added advantage of not requiring a card reader. The system is based on a special mobile SIM card, which the customer must request from the cell phone operator. However, when one does not have this special SIM card, they can prove their identity online using the Smart-ID mobile application. Finally, the E-residency card is designed to fulfill the purposes of the E-resident concept the state adopted. E-residency is a government-issued digital identity and status that provides access to Estonia's transparent digital business environment (e-resident.gov.ee, n.d.).

Estonia's e-ID system is used for electronic signing, authentication, and the secure transfer of sensitive data. It is convenient for the user and cost-effective for the institution. Contrary to the development of the X-Road, the digital identity project, which started in 1997, was completed five years later. The involvement of private banks was pivotal in the success of the ID card. What helped a lot was that people soon realized that their banks preferred digital IDs for personal identification, that it was more secure and convenient, which motivated them to replace old identification methods with digital-IDs (Vassil, 2016).

8.7.4 Legal and Administrative Basis

A well-structured legal and policy framework is the founding prerequisite of any e-governance initiative. For Estonia, the development of an information society began in 1998 when the Parliament adopted the Principles of Estonian Information Policy. Also, the Government of the Republic elaborated and approved a follow-up to the document in 2004, and the principles were updated in 2006. In January 2007, the "*Estonian Information Society Strategy 2013*" entered into force. This was a *"sectoral development plan, setting out the general framework, objectives and respective action fields for the broad employment of ICT in the development of knowledge-based economy in Estonia"* (Estonian Information Society Strategy, 2013) within six years. For its implementation, several international and European directives were taken into account, notably the EU i2010 and E-government Action Plans. The document that accomplished that was named *"Digital Agenda for Estonia 2020",* which laid down the steps planned in the context of national ICT policy for implementing the vision of information society. This strategy was divided into two sub-fields: developing information society (including

promoting communications and state information system, e-governance and services, ICT skills, and the reputation of e-Estonia) and developing cyber security (Digital Agenda for Estonia, 2020).

Estonia did not create a specific ministry for the information society. The Estonian approach can be characterized as minimal because it views implementation as the alternative to writing new documents and adding layers to bureaucracy. Today, the Ministry of Economic Affairs and Communications is politically liable for developing the state information policy. It elaborates on the state's economic policy and development plans while drafting the respective legislation bills, in various fields: informatics, development of state information systems, research and development and innovation. The main actor who coordinates governmental ICT policy and information society policy is the Government CIO Office of the Ministry of Economic Affairs and Communications. The Office's strategic goal is to align the state IT policy actions and development plans in state administrative information systems. It comprises six teams: the Digital Service Excellence Team, the Legal Team, the Financing Team, the ICT Skills Team, the Cybersecurity Policy Team, the International Affairs Team, and the Govtech Team (European Commission, 2019).

8.7.5 E-Estonia Services

With 99% of public services available online, the UN has ranked Estonia among the elite countries with the highest *E-Government Develop Index* (United Nations, 2018). According to the latest Digital Government indicators, Estonia is above the EU's 27 average in terms of individuals using the internet to interact with public authorities and obtain information from them (Eurostat, 2020). With 99% of public services being offered online, Estonia is the most digital country in the world. Some of these services are listed in the following paragraphs.

8.7.5.1 Government Cloud

The creation of a government cloud was part of the e-solutions for the creation of an e-services ecosystem. The Estonian Government Cloud (**Figure 8.8**) was established to facilitate the state's ability to manage, deliver, and audit services in the government sector (e-Estonia, n.d.).

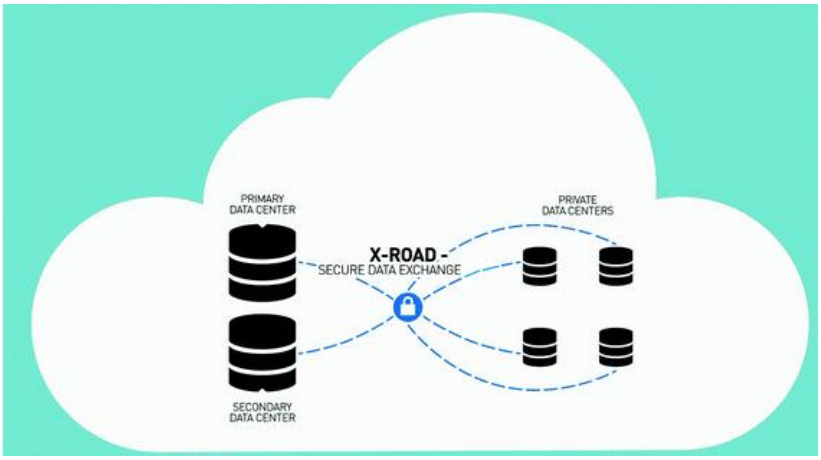


Figure 8.8 *Concept of Estonian Government Cloud and Data Embassies (Kotka & Liiv, 2015).*

The US National Institute of Standards and Technology (NIST) states that: "Cloud computing is a model for enabling a ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction." Simply put, everything is hosted on a collection of computers and servers that are accessible over the Internet or a private network, as opposed

to apps and data being hosted on a single computer. The solution aims to integrate *"…the existing siloed IT infrastructure of the Estonian public sector into a shared pool of resources*." The Estonian Government Cloud is delivered from a collaboration between the Estonian Government, represented by the State Infocommunication Foundation, and a consortium of private sector companies, including Cybernetica, Dell EMC, Ericsson, OpenNode, and Telia (e-Estonia, n.d.).

8.7.5.2 Data Embassy

The issue of security and integrity of vulnerable data has always been a concern because of the interdependent nature of the digital society the state has created. Thus, Estonia is highly dependent on the information systems and the data stored in them. The Estonian Government had an innovative plan to accommodate physical security requirements: creating a data embassy (Figure 8.9). Such embassies are servers situated outside the state's physical borders but are legally under its jurisdiction. Maintaining digital copies of key databases allows the management of data and information systems in a distributed manner.

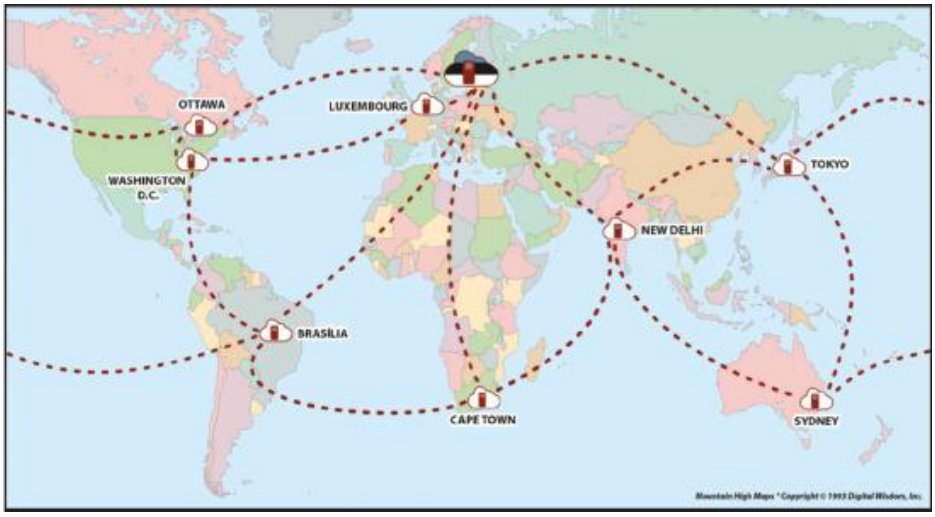


Figure 8.9 *How a network of Data Embassies might look in full operation (Robinson & Martin, 2017).*

Firstly, the cyber-attacks of 2007, when some Russian attackers took over 58 Estonian websites, including those of the government, put the security issue at the forefront. Secondly, the legal annexation of Crimea in 2014 brought the security issue to the surface. The response of the Estonian state came in 2017 when the first data embassy was created in cooperation with the authorities of Luxemburg. The Prime Ministers of the two countries signed an agreement that was the basis of the e-embassies framework. In other words, the government of Estonia has the right to own server resources inside Luxemburg's territory safeguard data backup and operate critical services. Furthermore, the partner state of Luxemburg guarantees that the embassy will be protected with the same legal guarantees as security servers in Estonia. The innovation also lies in the fact that it represents the first bilateral agreement to expand the Vienna Convention on Diplomatic Relations. For other countries to launch similar paradigms, the Estonian authorities have highlighted the importance of finding partner countries with which they share trust (OECD, 2018).

8.7.5.3 E-cabinet

E-cabinet is the Information System for Government Sessions in Estonia. It is considered a powerful tool used to streamline the decision-making processes of the Estonian government (e-Estonia, n.d.).

Up to 2000, the government sessions were held in the Government Session Hall of Stenbock House. The first attempt to implement technical solutions to this procedure was using stationary computer terminals

inside the Government Session Hall. Today, the session hall is free of stationary electronic devices, meaning that ministers can access the E-cabinet simply from their portable digital devices. In this way, ministers can view the proximate meetings, notify their colleagues, be updated in real time and even give preliminary votes regarding the topics on the agenda. The ones everyone with no objections accepts are adopted by default at the beginning of the session. The E-cabinet facilitates government meetings as it reduces paperwork and saves time; sessions in the past lasted approximately 4 hours, while today they last from 30 up to 90 minutes. Moreover, this system enables the "*secure digital signing of the government legal acts and other documents*" (Riigikantselei, 2020). Lastly, the e-cabinet is connected to another information system, the E-consultation system. The latter is designed to connect different government sectors, providing "*consulting draft legislation and other government instruments between the ministries as well as with the public*" (Riigikantselei, 2020).

8.8 Two Case Studies: The UK and the Netherlands

In the following paragraphs, two case studies of European countries are listed where various components of e-government have been successfully implemented: the UK and the Netherlands.

8.8.1 The UK

The UK is among the countries that have made excellent progress, a fact that the UN has recognized in the 2016 e-government Survey (United Nations, 2016), where the UK achieved the highest score on the e-government Development Index and the highest E-Participation Index. An overview of the history of e-government in the UK is given in bullets below:

- In October 1994, the CCTA (Central Computer Telecommunications Agency) created a website of the British government that could be used by Internet users and direct them to different websites.
- In November 1996, the British government published a brochure to inform its citizens. In the brochure, named *"Government Direct"* all e-government services were presented.
- In 1997, the British Prime Minister announced that by 2002, a high percentage of governmental interactions would be done electronically through computers and mobile phones.
- In February 1998, a report was published by the POST (Parliamentary Office of Science and Technology), explaining how the ICTs could provide a better provision of public services and ameliorate internal working.
- In 1999, a report was published under the title *"Modernizing Government Action Plan*", aiming to develop a single electronic getaway.
- In April 2000, the official e-governance strategy of the United Kingdom was announced. All government agencies should obtain the necessary electronic structure.
- After a few months, in December 2000, the official website of the British government "*UKonline.gov.uk*" was launched.
- Respectively, in December 2001, the "*E-policy Principles"* was published, which outlined all the online procedures to improve its effectiveness.
- At the end of 2002, the national strategy for local e-government started. The strategy aimed to transform the local services to provide greater ease and accessibility to the customers.
- After a year, in 2003, the government created a specific website only for businesses. The "*BusinessLink.gov.uk*" provided all the necessary information for owners and business managers.

- In 2005, a new document was published named "*Transformational Government-Enabled by technology*." The document stated how using public services electronically could improve the daily lives of citizens and businesses.
- At the end of 2006, the British government's website *"Directgov"* started to provide all the online public services using mobile phones.
- After a year, the British government realized that the official government sites had improved slightly since 2002. For easier access to the public and businesses, the government divided the information into two online websites, "*Directgov*" and "*businesslink.gov.uk*".
- In July 2008, a report was published named "Transformational Government Annual Report 2007", which included the latest developments of the year, aimed at improving the provision of public services to the citizens.
- The British government decided to focus on the evolution of e-government, and for this reason, in 2009, it announced that it would reduce public spending, but at the same improve time public services.
- The new "*UK Digital Champion*" was published in June 2010. Its purpose was to convince more and more citizens to go online to increase transparency.
- In January 2011, the first public sector directory was published. Also, the *Digital Continuity Framework* (part of the UK's *National Archives project)* was launched simultaneously to provide instructions regarding how to use their information.
- After several months, in December 2012, Minister Francis Maude announced that the new e-services would be faster and more convenient for the public, while by 2015 1.2 billion pounds would be saved from taxpayers.
- In May 2013, the Health Minister announced that until 2018, the National Health System (NHS) would go digital. A total of 260 million pounds would be used for this purpose.
- In April 2014, the Cabinet Office funded organizations that wanted to improve their data publication. ODUG (*Open Data User Group*) is the group that is responsible for collecting bids for funding.
- On the 1st of October 2015, the *UK Government Manifesto* was published by the *UK Government Civil Society Network*. Manifesto was a ten-month project. Its goal was to present the best open government ideas from the political parties and citizens. Some identified themes were Privacy, Citizen Participation, Open Data, Open Parliament and Court, Open Budgets.

The facts listed above highlight a constant trend for improving the usability and quality of the offered services, aiming to transform the relationship between the state and the citizens, offering services related to travel, vehicles, work and retirement, education and youth, residence formalities, family, health, or commerce. Businesses are also supported in fields of VAT and customs, start, and grow, selling abroad, staff, product requirements, environment, public products etc. Additionally, some tools offer greater opportunities for vertical communication with politicians and e-participation.

Table 8.1 gives an outline of some popular e-services offered in the UK.

Table 8.1 *Popular e-service platforms in the UK (own elaboration).*

Platform	Service
Gov.uk	The official website of the British government. It offers the businesses and citizens of the UK everything they need to know to have access to all the public services. The site began officially in 2012. Three hundred twelve agencies were transitioned to this site, and this transition officially ended in December 2014.
Data.gov.uk	Non-personal UK data available. It covers approximately 21,000 government datasets from 1400 local, and central government entities.
Gov.uk Verify	A website that verifies the identity of citizens.
Employee Authentication Service	It allows employees to access information safely. It shows how somebody can reuse existing technology and save costs for the local government.
Excellence Gateway	An online service for those who want to practice their learning skills in the UK. It promotes new teaching and learning skills. Moreover, methods of teaching and examples used can be shared among participants.
justice.gov.uk	Information about the legal system, regulations and administration of the country. The Criminal Justice Secure eMail, processes approximately 3.000.000 messages every month.
Universities and Colleges Admissions Service (UCAS)	A web system that gives applicants the possibility to apply online through the site for higher education in UK. Also, most university libraries offer online access to their library catalogue.
National Hospitality Service (NHS)	GP appointment, European Health Card issuing online etc.
Crown Commercial Service (CCS)	Combines direct buying, advice, and policy. These commercial services manage common goods and services across the government and improve the supplier. Furthermore, they provide services to the public sector, saving money for the taxpayer at the same time.

8.8.2 E-voting: The Case of the Netherlands

8.8.2.1 E-voting

The influence of cyberspace on politics, and especially on electoral contests, is becoming increasingly important. This is noted by human rights observers and international organizations specializing in democratic governance and elections. Their role is to document the correctness of the procedures and standards for conducting elections following democratic principles. According to the guidelines established by the UN, electronic voting systems and electronic files must comply with the rules for data management (UN General Assembly, 1990). The responsibility for the collection, accuracy, and transparency of the data of the electoral rolls lies with the authorized persons who act with legal procedures and store the data safely.

In 2017, the Council of Europe added additional principles to those of the United Nations, recognizing that Electoral Management Bodies (EMB) should be held accountable for e-voting and "*availability standards, reliability, usability and security of the electronic voting system*" (Council of Europe, 2017).

Although these rules have contributed significantly to improving the quality of electoral processes, they do not apply to the offline world and are constantly challenging cybersecurity in elections. There have been concerns about how cyberspace could affect the electoral process. Information and Communication Technologies (ICT), according to voters, the media, electoral experts, and politicians, involve risks related to falsification in terms of data, voter profiles, voting machines or registers, false news, and campaigns. Indicatively, countries such as Germany, which introduced electronic voting, have stopped using it. The ICTs, with their new possibilities, raise concerns for the security of the electoral process, as they make large-scale "attacks" possible and falsify voting and the election result. In so-called "digital democracies," where technology offers the opportunity to increase participation in democratic processes, protection against fraud becomes even more necessary. The 2016 USA presidential election is an example where massive voter fraud was reported to have occurred, which demonstrates how vulnerable cyberspace can be to external interference in the electoral process (Dominioni, 2018). The issue remains highly debated not only in the USA but globally and has caused major turbulence in the political developments in the country (Norris, 2017).

Electronic voting (E-Voting) means using electronic systems in one or more steps of the electoral cycle. According to the International IDEA Organization, electronic voting in the electronic steps of elections or referendums is related to the recording and/or counting votes. It concerns voting systems in controlled environments, in which voting takes place in an area supervised by election officials, such as the constituency (using means such as a punch card, visual scanning, and other), and in uncontrolled environments, which means that voting can take place anywhere outside a polling station, e.g., at home on a computer. Through the Internet, the voting data is transmitted to receivers through telephone or mobile networks; in this way, the voting results are disseminated in the public space, which can only be partially controlled by election officials (IDEA, 2011).

The debate over the costs, benefits, and risks of e-voting is well underway. Although already widely used, there is great skepticism about the above from civil society organizations, experts, and politicians. In some countries, such as Switzerland, introducing remote voting over the Internet is a highly convenient and practical solution due to their geography. Still others avoid any form of electronic voting, such as Norway, due to concerns about the security of the process and voting in national elections or referendums. According to experts, voting in a controlled environment that supports counting or recording voting is considered the least controversial form of electronic voting. It is used regularly in many countries (e.g., Brazil, USA, India, and Estonia). However, some countries have avoided or stopped using computers (e.g., Germany, Netherlands). In both cases, some arguments justify each side.

Electronic voting technology allows people with disabilities to vote on their own, easily, and secretly, and at the same time, increases the likelihood of low voter turnout as it encourages more voters to cast their ballots remotely. People who cannot visit polling stations (military and civilians living abroad) or people who do not speak the language can participate. The overall cost of running and managing the electoral process is reduced, and counting votes is faster and more accurate. At the same time, the election results are delivered more immediately (especially regarding complex electoral systems). Human error is almost eliminated, the results are more reliable, and the possibility of fraud while recording results is reduced, as human intervention is reduced.

On the other hand, information technology does not guarantee the complete elimination of errors, in which case the detection of errors is much more difficult to detect and the technical malfunctions to be treated compared to conventional procedures. The possibility of a fully digitized system failing to produce results due to a lack of natural backups makes alternatives difficult or impossible. Free and secret ballot becomes problematic, as registered voters do not have to go through a process of verifying their identity. An even greater risk is the possibility of third parties interfering (with hacking attacks) that threaten to cancel the process altogether. Finally, the high know-how requires high dependence on technical experts, while

according to others, the cost of purchasing and maintaining the electronic voting system makes this option unprofitable. An important campaign to train voters is needed, and the risk of losing public confidence in the election and referendum process is significant (ACE, n.d.).

8.8.2.2 The Case of the Netherlands

Electronic voting has been implemented by many MS using different techniques. In Estonia, for example, Internet voting culture is said to be diffused among the electorate and research has shown that e-voters are not likely to go back to offline voting (Vassil, 2016). The process there is simple and goes as follows: first, the voters need their digital identification card, a computer with access to the Internet and a smart card reader. Second, they must download the voting application and insert their PIN1 for the program to decide whether they have the right to vote. Afterward, the voters cast their vote, and verify their identity by entering their PIN2. Several security mechanisms protect the integrity of the vote and have to abide by the principles of the Estonian Electoral Committee. These principles, in short, set the time framework for the electorate to vote; they allow the voter to change their vote either online or in person at the ballot box on the Election Day, and prohibit the transfer of PIN codes to other people for voting. Also, the e-vote resembles the physical vote because it is secret, and one cannot vote on behalf of another. Software is used to check the voter's identity through a smartphone camera to prevent malware interference. Since 2005, Estonia has held nine elections online at the local, national, and European levels. However, systems implementing e-voting in combination with the "digital" circumstances and the surrounding digital culture cannot always guarantee success in advance, and procedures may be more complicated. An example is the case of the Netherlands, which is presented below.

In 2013, the Dutch authorities assigned the Electronic Voting Research Committee (Commissie - Van Beek) the task of assessing the need to re-introduce electronic voting in electoral procedures. Electronic voting was widely used in the Netherlands for thirty years until 2006 when it turned out that the voting machines used were susceptible to fraud and that voting secrecy could not be guaranteed. As a result, it was decided that voting and counting of votes should be done manually again in 2009. However, the manual voting and counting process was criticized as it takes a long time until the preliminary results are known, and polling station members make mistakes when counting. In addition, municipalities were increasingly finding it difficult to recruit polling station members due to the long working days and the heavy load. Finally, the ballot paper was found difficult or impossible to be used for large groups of voters, while persons with disabilities depended on voting with help or via a power of attorney.

The committee's task was to verify whether electronic voting fulfills provisions of the country's Elections Act. With this mandate, it collected information, discussed with various stakeholder groups (both supporters and opponents of electronic voting), enquired about the possibilities for electronic voting, and identified the costs of the process. The Committee focused on forms of electronic voting available in practice and investigated how other countries used electronic voting. Finally, it examined different voting and counting methods electronically and identified the risks and measures to cover those risks.

The committee found that in the current (manual) voting process, many people cannot vote independently, their votes become invalid unintentionally, or they vote for candidates other than those they intended. When counting the votes, mistakes are made, and overall, the burden on polling station members has increased since the introduction of manual counting, and inevitably, results are known late.

Based on this, the committee made a risk analysis of three different electronic voting methods and the current paper process. It was recommended that a vote printer and vote counter should be used. With that system, voters enter their choice on a computer that prints their vote on a ballot paper. Then, the voter puts the ballot paper into the ballot box, and after the vote, all ballots are counted electronically with scanning

equipment. This offered significant advantages, making voting more accessible to people with a disability; voters received feedback about the progress of their voting choice, fewer mistakes were made during counting, and the election result would be available faster. The votes should not be electronically stored but only printed and the committee proposed measures to limit eavesdropping as much as possible with random checks that the counting equipment is working correctly; it even considered the effect electromagnetic radiation would have on people. The committee recommended that all municipalities vote and count electronically with the same equipment and that a central organization be held responsible for storing, managing, maintaining, and preparing equipment for elections. Regarding costs associated with electronic voting and counting, they would largely be determined by the requirements of an electronic voting process and the measures necessary to ensure that voting takes place smoothly on the day of the elections.

In May 2015, the Minister of Interior set up an Expert Group for Electronic Voting and Counting in the polling station to investigate whether the Van-Beek proposal was feasible and to remove uncertainties, reduce complexity, and make a better cost estimate for e-voting (Kiesraad, n.d).

In May 2016, the Expert Group advised the minister to opt for the introduction of the vote counter. However, they were cautious about introducing a voting printer: "*The voting printer is a much more complex system that involves more risks.*" The Expert Group report recommended issues such as vote counter security, random checking of electronically counted ballot papers, and storage, management, and maintenance choices. Essentially, that expert group advised only including a vote counter and not a vote printer, because a printer could be hacked and print other voices than wanted (in practice people often do not check what is on their printed ballot paper).

The government has also indicated that there were still questions to be answered, such as whether the proposed method increased the accessibility of the voting process for voters with a visual impairment, or if there were possibilities for eavesdropping, "compromising radiation" and what checks were required on the correctness of electronic counting. It also assessed that the cost still needed to be determined.

In August 2017, in a communication sent by the Ministry of Interior and Kingdom Relations to the President of the House of Representatives, the results of the inquiry made by the Electoral Council were presented for the suggestions of the Van Beek committee and the Expert Group. In this document, it was mentioned that the decision-making on the introduction of the voting printer and voting counter will have important legal, organizational, and financial consequences to elections; "*the risks, due to cyber threats, for the election process just recently increased. In view of this, it is not opportune for a resignation cabinet to take final decisions on this*" (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2017). With this, the decision on the feasibility of introducing the e-voting equipment was passed on to the following cabinet. The Electoral Council emphasized that all variants of voting and counting involved risks. Therefore, assessing the acceptability of residual risks and comparing them with the existing system was unnecessary.

In an article published in July 2018 on a credible news site with the title "*Waarom stemmen we in 2030 nog niet elektronisch*?" the writer explained that "the red pencil" (as is the manual voting and counting called in the Netherlands) remains for the time being. The discussion about electronic voting and counting still holds on. Elections were held for the first time in 1966 with a voting machine, and the Netherlands continued to use voting computers in elections for decades. However, over the years, the technical possibilities increased, and the threats, for example, from hackers. That is why the country re-introduced the "analog" system in 2009, with a red pencil and paper ballot, which is still used. Employees of a polling station now count all votes cast manually. Each agency has its system. This method is prone to errors, and votes must be recounted in several cases, leading even to a new distribution of seats.

At the same time, in other sectors, new digital techniques continue to follow each other rapidly. So, many people wonder: "*If I can file my tax return online, why can't I vote?"* The article's author reminds us that

"If your tax return is manipulated, a system will beep somewhere and you will receive a letter on the mat." This is not the case with elections, though, as nobody should ever know what you are voting for, not even the government, thanks to secret voting. The voting secrecy is so delicate that a discussion about snapping a selfie with your completed ballot surfaced in 2014. Voting covertly increases the difficulty of identifying electronic voting fraud. "For comparison, if your bank detects a 'suspicious' transaction with your credit card, your bank can contact you or block your card. This is because internet banking is not anonymous, such as voting. In elections involving electronic voting, someone can break into the system, manipulate the votes, and then erase their tracks."

As the US elections in 2016 showed, it is now clear that state actors have the intention and capacity to interfere in our elections through digital means.

So, based on the above, one wonders if there is a safe way to vote electronically. Blockchain, the technique behind Bitcoin, is often mentioned in this context. Blockchain is a digital ledger containing the accounts of every economic transaction ever made. For example, with Bitcoin, you can find where and to which accounts money is transferred. For the time being, in the Netherlands, authorities are only experimenting with new ballot papers and a vote counter, and according to computer security, much depends on the implementation. If mistakes happen with the counting machines, the paper ballots can always be counted manually again.

As the Minister of Interior of that time pointed out, *"everything is laid down in the Elections Act. If you want to change something, you have to do experiments first and then implement a change in the law. We do everything step by step. And that is also important, because it is really about our democracy"* (de Joode and Schellevis, 2018).

8.9 Conclusion

Implementing successful e-government in a country is essential for promoting each public administration system's efficiency, accountability, effectiveness, transparency, and success. For modern democracies, new challenges emerge, such as the security of transactions and accessibility to services. The digital environment cannot (yet) guarantee security in the processes of e-governance, particularly in key functions such as voting, posing the risk of compromising the secrecy of votes and interfering with political preferences in shaping and expressing the true will of citizens.

As times change and technology progresses, it is important, on the one hand, to keep abreast of new types of managing public life and, on the other, to respect the core values of participatory democracy. Essentially, the new means digital technology offers do not abolish traditional forms of democracy but complement them. At the center of the discussion of the above lies the recognition that cyberspace and in real life governance in apply the same principles and aims.

Within the EU, the importance of e-government is even greater due to the function of the European Single Market and the need to simplify all the procedures between the MS. The cross-border character of the activities within the EU indicates the urgency of implementing the pan-European vision of e-government.

Up to the present, in most of the member states, e-government is partly or fully implemented. However, there are differences between the pace of each MS, proving that some challenges must be overcome to realize the European Commission's Action Plan and fully exploit the opportunities and benefits provided by the ICTs. These difficulties must be managed under the MS's steadfast direction and active participation in politics. Simultaneously, the majority stem from structural variations among the MS, economic factors, and technological and legal constraints.

References

Abu-Shanab E. A., and Bataineh L. Q., 2014. “Challenges Facing e-government Projects: How to Avoid Failure?” *Int. J. Emerg. Sci.*, 4(4), pp. 210–217.

ACE n.d., “Electoral Knowledge Network, E-Voting.” Available at: https://aceproject.org/ace-en/focus/e-voting/benefits-risks-and-costs [Accessed 20 May 2020].

Aldrich D., Bertot J.C., McClure C.R., 2002. “E-government: initiatives, developments, and issues.” *Government Information Quarterly, 19.*

Alshehri M., and Drew S., 2010. “Implementation of e-government: Advantages and Challenges.” *IASKE E_ALT Conference Proceedings*, pp. 79–86.

Anon., 2020. European Commission Official Website. [Online] Available at: https://ec.europa.eu [Accessed 31 March 2020].

Anttiroiko A.-V. (ed.), 2008. *Electronic Government: Concepts, Methodologies, Tools, and Application*. New York - London: IGI Global.

Ardielli E., and Halaskova M., 2015. “Assessment of E-Government in EU Countries.” Issue 22, pp. 4–16.

Baptista M., 2005. “E-Government and State Reform: Policy Dilemmas for Europe.” *The Electronic Journal of E-government*, 3(4), pp. 167–174.

Belgian Development Agency, 2017. “Belgian Development Agency "E-Governance." [ONLINE] Available at: https://www.enabel.be/sites/default/files/d4d_info_sheet_e-governance_version_2.0.pdf [Accessed 7 May 2019].

Bennett O., 2009. Electronic Government (e- Government). House of Commons.

Bershadskaya L., Chugunov A., and Dzhusupova Z., 2013. “Understanding E-Government Development Barriers in CIS Countries and Exploring Mechanisms for Regional Cooperation.” EGOVIS/EDEM, pp. 87–101.

Beynon-Davies P., 2007. “Models for e-government. Transforming Government: People,” *Process and Policy*, 1(1), pp. 7–28.

Brown D., 2005. “Electronic government and public administration.” I*nternational Review of Administrative Sciences*, 71(2), pp. 241–254.

Cambridge Dictionary. (no date). Cambridge Dictionary "governance." [ONLINE] Available at: https://dictionary.cambridge.org [Accessed 17 April 2019].

Castells M., 2009, *The Rise of the Network Society: Economy, Society and Culture*. v.1: The Information Age: Economy, Society and Culture, Wiley-Blackwell.

Centeno C., van Bavel R., and Burgelman J.-C., 2005. “A Prospective View of e-Government in the European Union.” *The Electronic Journal f e-Government*, 3(2), pp. 59–66.

Coleman S., and Blumler J. G., 2009. *The Internet and democratic citizenship: Theory, practice and policy*. Cambridge: Cambridge University Press, p. 90, p. 117.

Coleman S and Blumer J. G., 2009. *The Internet and democratic citizenship: Theory, practice and policy.* Cambridge: Cambridge University Press.

Council of Europe, Council of Europe CM-Rec, 2017. Appendix I, sec. VIII, Strasbourg.

Curtin G.G., Sommer M.H., & Sommer V.V., 2003. *The World of E-government*. The Haworth Press, pp.261-263.

de Joode E., and Schellevis J, 2018, "Waarom stemmen we in 2030 nog niet elektronisch?" *NOS*. Available at: https://nos.nl/artikel/2240863-waarom-stemmen-we-in-2030-nog-niet-elektronisch.html [Accessed 7 January 2020].

De Montesquieu, 1748. *Complete Works*. *The Spirit of Laws, Book III.* Vol. 1. 4 vols. https://oll.libertyfund.org/titles/montesquieu-complete-works-vol-1-the-spirit-of-laws

Di Maio A., 2003. "Traditional ROI Measures Will Fail in Government." Gartner Group. Note Number AV-20-3454.

Di Maria E., and Micelli S. (eds.), 2005. *Online Citizenship - Emerging Technologies for European Cities*. New York - London: Springer.

E-Estonia, 2020. "Government Cloud." Available at: https://e-estonia.com/solutions/e-governance/government-cloud/ [Accessed May 6, 2020].

e-Estonia, n.d. "X-Road®." Available at: https://e-estonia.com/solutions/interoperability-services/x-road/ [Accessed 7 May 2020].

e-Estonia, 2018, "Government Cloud: Infrastructure as a Service," Available at: https://e-estonia.com/government-cloud-infrastructure-service/ [Accessed May 10, 2020]

e-Estonia, 2020. "E-Cabinet." Available at: https://e-estonia.com/solutions/e-governance/e-cabinet/ [Accessed 5 May 2020].

E-estonia.com, 2015. "We have built a digital society and we can show you how." [ONLINE] Available at: https://e-estonia.com [Accessed 5 May 2020].

e-Residency, n.d. "What Is E-Residency? How to Start an EU Company Online." Available at: https://e-resident.gov.ee/ [Accessed 11 May 2020].

E-Residency, 2015. "We have built a digital society and we can show you how." [ONLINE] Available at: https://e-resident.gov.ee/ [Accessed 11 May 2020].

Estonian Information Society Strategy, 2013. [ONLINE] Available at: https://www.yumpu.com/en/document/read/42978481/estonian-information-society-strategy-2013-european-centre-for [Accessed 22 May 2020].

European Commission, 2016. *EU eGovernment Action Plan 2016-2020 Accelerating the digital transformation of government* (COM(2016) 179 final), Brussels: European Commission.

European Commission, 2017. *eGovernment in the European Union*. Brussels: European Union Publications.

European Commission, 2018. *eGovernment Benchmark 2018-Securing eGovernment for all*. Brussels: European Union Publications.

European Commission, 2014. "E-government in the United Kingdom." Retrieved from: https://joinup.ec.europa.eu/collection/egovernment/epractice

European Commission, 2016. "E-Government in the United Kingdom." Retrieved from: https://joinup.ec.europa.eu/

European Information Society – E-Government, n.d. Available at: http://europa.eu.int/information_society/soccul/egov/index_en.htm [Accessed 10 April 2020].

Eurostat 2020, "Individuals Using the Internet for Interacting with Public Authorities." Eurostat Information Society Information, Eurostat, March 25, 2020 [ONLINE]. Available at: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15eiandlang=en [Accessed 5 April 2021].

Floria, A., Burcea, S., and Folescu, C., 2019. "Challenges encountered in the use of electronic services in the public administration from EU Member States - A Comparative Study," s.l.: ACZ Consulting.

Fountain J.E., 2001. *Building the Virtual State: Information Technology and Institutional Change*, Brookings Institution Press.

Goede M., 2019. "E-Estonia: The e-government cases of Estonia, Singapore, and Curaçao." *Archives of Business Research*, Vol.7, No.2, pp. 216–227.

Government of the Republic of Estonia, 2018. "Digital Agenda for Estonia 2020." Available at: https://www.mkm.ee/sites/default/files/digitalagenda2020_final.pdf [Accessed 12 June 2020].

Grönlund Å., and Horan T. A., 2004. "Introducing e-Gov: History, Definitions, and Issues." *Communications of the Association for Information Systems*, Volume 15, pp. 713-729.

Habermas, J. 1989. *Civil Society and the Political Public Sphere*. Cambridge: MIT Press.

Habermas J., 1991, *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. MIT Press.

Hacker Kenneth L., and van Dijk J., 2000. *Digital Democracy: Issues of Theory and Practice*. 1st ed. SAGE Publications.

Hague B. N., and Loader B., 1999. *Digital democracy: Discourse and decision making in the information age*. Psychology Press.

Hardy A., 2020. "Estonia's Soft Power through Technology." *E-International Relations*.

Heeks, R. 2006, *Implementing and Managing eGovernment. An International Text*. (pp. 1–7). SAGE Publications.

Herzog S., 2011. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security*, Vol. 4, No. 2, Strategic Security in the Cyber Age, pp. 49–60.

Hindman M., 2008. *The myth of digital democracy*. Princeton University Press.

IDEA, 2011. *International Policy Book, Electronic Voting Introduction: Basic Estimates*. Available at: http://www.idea.int/publications/introducing-electronic-voting/ [Accessed 15 April 2020].

IFES, 2018. Cybersecurity in Elections: Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies, Available at: https://www.ifes.org/sites/default/files/2018_heat_cybersecurity_in_elections.pdf [Accessed 15 March 2020].

Institute of Governance. (no date). Institute of Governance "What is Governance?" [ONLINE] Available at: https://iog.ca/ [Accessed 25 April 2019].

Kalvet T., 2012. "Innovation: a factor explaining e-government success in Estonia." *Electronic Government, An International Journal*, Vol. 9, No. 2, pp. 142–157.

Karacapilidis N., Loukis E., and Dimopoulos S., 2004. "A Web-Based System for Supporting Structured Collaboration in the Public Sector." In R. Traunmüller (ed.), *Electronic Government - Third International Conference*, EGOV 2004 - Zaragoza, Spain, August 30 - September 3, 2004 Proceedings. Berlin - Heidelberg: Springer - Verlag, pp. 218–225.

Karamagioli E., Staiou E. R., Gouscos D., 2018, "Can Open-Government Models Contribute to More Collaborative Ways of Governance?" In: Open Government. Springer New York.

Kiesraad, n.d. "Rood potlood en elektronisch stemmen." Available at https://www.kiesraad.nl/verkiezingen/tweede-kamer/stemmen/rood-potlood-en-elektronisch-stemmen [Accessed 20 March 2020].

Kitsing M., 2010. "An Evaluation of E-Government in Estonia." Impact Assessment conference at Oxford University.

Kotka T., I., and Livv I., 2015. *Concept of Estonian Government Cloud and Data Embassies*. Springer International Publishing Switzerland, pp. 149–162.

Kreiss Daniel, 2016. *Prototype Politics: Technology intensive campaigning and the data of democracy.* New York, Oxford University Press.

Maarit S., Leonsk N., and Trechsel A.H., 2107. "Two Countries/Two Decades/ Two Outcomes: A Brief Comparison of e-Government Solutions in Estonia and Switzerland." Zurich: *xUpery*.

Martin K., Robinson N., 2017. "Distributed denial of government: the Estonian Data Embassy Initiative." *Network Security*, Volume 2017, Issue 9, September 2017, pp. 13–16.

Meiyantia R., Utomo B., Sensuse D. I., and Wahyuni R., 2018. "e-Government Challenges in Developing Countries: A Literature Review." *The 6th International Conference on Cyber and IT Service Management* (CITSM 2018).

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2017. "Aan de Voorzitter van de Tweede Kamer der Staten-Generaal, uitkomsten marktuitvraag stemprinter en stemmenteller." Available at: https://www.kiesraad.nl/binaries/kiesraad/documenten/kamerstukken/2017/kamerbrief-rapportage-onderzoek-haalbaarheid-stemprinter-en-stemmenteller/kamerbrief-rapportage-onderzoek-haalbaarheid-stemprinter-en-stemmenteller/kamerbrief-rapportage-onderzoek-haalbaarheid-stemprinter-en-stemmenteller/kamerbrief+rapportage+onderzoek-haalbaarheid-van-stemprinter-en-stemmenteller%27.pdf [Accessed 15 April 2020].

Ministry of Economic Affairs and Communications, 2007. "Estonian Information Society Strategy 2013." Available at: https://www.yumpu.com/en/document/read/42978481/estonian-information-society-strategy-2013-european-centre-forhttps://www.yumpu.com/en/document/read/42978481/estonian-information-society-strategy-2013-european-centre-for- [Accessed 12 April 2020].

Misuraca G., Alfano G., and Viscusi G., 2011. "Interoperability Challenges for ICT-enabled Governance: Towards a pan-European Conceptual Framework." *Journal of Theoretical and Applied Electronic Commerce Research*, 6(1), pp. 95–111.

Noman A.M., Hebbar C.K, 2016. "E-GOVERNMENT DEVELOPMENT MODELS: CONCEPTS OVERVIEW." *International Journal of Latest Trends in Engineering and Technology,* Special Issue SACAIM, pp. 115–120.

Norris P., 2017. "Could massive voter fraud have occurred in the 2016 US presidential election?" *Electoral Integrity Project blog*, Available at: https://www.electoralintegrityproject.com/eip-blogs/2017/2/2/could-massive-voter-fraud-have-taken-place-in-the-2016-us-presidential-election [Accessed 17 May 2020].

O'reilly T., 2005. Web 2.0: compact definition. http://radar.oreilly.com/2005/10/web-20-compact-definition.html [Accessed 15 April 2016].

OECD, 2018. "Case Study: The World's First Data Embassy-Estonia." *Embracing Innovation in Government: Global Trends*. UAE.

OECD, 2003. *The e-Government Imperative*, Paris, France: OECD Publications Service.

OECD, 2008. "Future of e-government AGENDA 2020." *OECD Leaders Conference*," The Hague - Netherlands: OECD.

OECD, 2016, "Trust in Government." [ONLINE] Available at: http://www.oecd.org/gov/trust-in-government.htm [Accessed 15 October 2020].

Pederson K., 2016. "e-Government in Local Government: Challenges and Capabilities." *Electronic Journal of e-Government*, 14(1), pp. 99–116.

Pippa Norris, Richard W. Frank, and Fernandez Martinez, 2014. *Advancing Electoral Integrity.* Oxford: Oxford University Press.

Prins J.E.J., 2007. *Designing e-Government*. New York, NY: Kluwer Law International, pp. 165–183.

Reddick C. G. (ed.), 2010. *Comparative E-Government*. New York - London: Springer.

rejoin.gr,.2015. «Η δημοκρατία στην εποχή του vouliwatch». [ONLINE] Available at: https://www.rejoin.gr/synentefxeis/1923-h-dhmokratia-sthn-epoxh-tou-vouliwatch [Accessed 5 September 2016].

Research and Development Section for e-Government in the EU Information Society and the European Commission, 2013. "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions," European Union Security Strategy Cyberspace, Brussels.

ReSPA, 2018. "Regional Comparative eGovernment study." s.l.: Regional School of Public Administration.

Riigikantselei, 2020. "Organisation of the Work of the Government." Government Office of Estonia, [ONLINE] Available at: https://www.riigikantselei.ee/en/organisation-work-government [Accessed 4 May 2020].

Riigikantselei, 2020. Government Office of Estonia, n.d., "Organisation of the Work of the Government." Available at: https://www.riigikantselei.ee/en/organisation-work-government [Accessed 6 May 2021].

Robinson N., Keith Martin K., 2017. "Distributed denial of government: the Estonian Data Embassy Initiative." *Network Security*, Volume 2017, Issue 9, Available at: https://www.sciencedirect.com/science/article/pii/S1353485817301149 [Accessed 10 May 2020].

Samuele Dominioni, 2018. "Protecting Electoral Integrity In Cyberspace: The US Mid-Term Elections In 2018." ISPI Centre on Cybersecurity.

Schuppan T., 2008. "E-Government in developing countries: Experiences from sub-Saharan Africa." *Government Information Quarterly 26* (2009), pp. 118–127. Available at: https://doi.org/10.1016/j.giq.2008.01.006

Sierzputowski, B. 2019. "The Data Embassy under Public International Law." *ICLQ*, vol. 68, January 2019, pp. 225–242.

Spremic M., and Vrzica H., 2008. "Comparative Analysis of e-Government Implementation Models and Progressive Services." *WSEAS Transactions on Business and Economics*, 5(5), pp. 260-269.

Tapscott D., 1999. *Growing Up Digital: The Rise of the Net Generation*, 1999, McGraw-Hill.

U.N. 1948. "Universal Declaration for Human Rights, Paris." Available at the site of the Office of the United Nations High Commissioner for Human Rights.

U.N. General Assembly, 1990. "Guidelines for the Regulation of Computerized Data Files." Available at: http://www.refworld.org/pdfid/3ddcafaac.pdf [Accessed 10 May 2020].

United Nations, 2016. "United Nations E-Government Survey 2016. [ONLINE] Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016 [Accessed 15 April 2019].

United Nations, 2018. "United Nations E-Government Survey 2018, Economic and Social Affairs." New York [ONLINE]. Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2018-Survey/E-Government%20Survey%202018_FINAL%20for%20web.pdf [Accessed 5 May 2021].

Vassil K., 2016. “Estonian E-Government Ecosystem: Foundation, Applications, Outcomes.” Institute of Government and Politics University of Tartu, no. World Development Report 2016.

Veebel Viljar. “E-Democracy in the European Union: Lessons from Estonia.” Foreign Policy Research Institute, Baltic Bulletin, February 13, 2018. https://www.fpri.org/article/2018/02/e-democracy-european-union-lessons-estonia

X-Road® Data Exchange Layer n.d. “X-Road® History.” https://x-road.global/xroad-history [Accessed 2 May 2020].

Chapter 9 E-commerce and E-business

Abstract

In Chapter 9, the interlinked terms e-Commerce and e-Business are defined. It describes how firms' digital transformation corresponds to the realignment of technology and business models to engage digital customers more effectively at every touchpoint in the customer experience lifecycle. Moreover, the internet's contribution to establishing commercial transactions is presented, where buying and selling goods, services, and information is electronically implemented. It is explained that e-Business is a broader term than e-Commerce which points out how the Internet is changing the way companies do business, the way they relate to their customers and suppliers, and the way they view functions such as marketing and logistics. The B2B, B2C, and C2C models are presented, and M-Commerce is introduced, which holds significant and exponentially increasing merit in the global marketplace. Finally, the role of social media in shaping consumers' purchasing behavior is analyzed.

9.1 Introduction

Electronic commerce (e-commerce from hereafter) describes how transactions occur over electronic networks, mainly the Internet. It includes electronically buying and selling goods, services, and information. Furthermore, other than buying and selling, it is also about electronically communicating, and collaborating. It can also be used as a source of information to compare prices or look for products before purchasing online or at a traditional store. Although there has been a severe recession in the world economy in recent years, e-commerce has grown rapidly, impacting a significant portion of the world and affecting businesses, professions, trade, and people.

Only two base-level technologies were involved in supporting the e-commerce explosion: computing and communications. Both have been developing exponentially in terms of performance and reduction in cost. It is now well known that computing system performance per dollar doubles every 18 months. It has been doing so for two decades and will likely continue for at least 15 years. By the end of this period, computers will be more than 1000 times more powerful than today's machines for the same price. Today, communication networks using advanced technologies like optical fiber carry orders over intercontinental distances. The reduction in operational costs is truly dramatic, and we are only at the start. The message for businesses is simple: Within a couple of decades, they will have access to affordable networks of effectively infinite carrying capacity and computers with unimaginable processing power.

One very important contribution to the development of e-commerce in recent years is the continuous phenomenal growth of social networks and the trend toward conducting electronic commerce with mobile devices, changing dramatically commercial areas such as travel, banking, fashion, and transportation.

9.2 A Theoretical Framework of E-Commerce

E-commerce first appeared in Europe and the US in 1998. However, e-commerce processes were launched in 1970, representing an electronic data exchange for business purposes like sending certain business reports (e.g., an order). In general, e-commerce can be considered any form of economic or business activity via electronic connections (Nanehkaran, 2013). E-commerce is the sale and purchase of products and services via the Internet. More specifically, it is a more complex system of security, data management, and communication that is linked and interconnected to exchange information about the products and services provided and available for purchase. How it is structured can be divided into three categories: Infrastructure, Services, and Structures. More specifically:

- **Infrastructure** has everything to do with the infrastructure on which e-commerce operates, such as the hardware and software necessary for its implementation. Databases are extremely important because they are where all the necessary information is stored and organized offering communication channels between merchants and consumers.
- **Services** provide the ability to seek information about future trading partners, negotiate with them, and finally reach an agreement establishing a business.
- **Structures** have to do with the immediate availability of products, services, and information to customers and partners. They also provide the opportunity to cooperate and exchange information both within and outside the business to coordinate with the marketplace itself and the chain of supply and support (Nanehkaran, 2013).

In this way, traditional trade as we know it has developed quite rapidly, giving the opportunity and space for e-commerce to grow and evolve, while modernizing the way traditional trade has been working for centuries.

E-commerce offers many opportunities, such as developing mutual and tight partnerships between partners to create innovative products and services that will facilitate customer satisfaction and improve the

relationship between the business and the customers. Moreover, the opportunities offered by electronic commerce have a huge impact and can help establish international partnerships between multinational companies to organize various marketing campaigns. Nowadays, there are countless products and services on the internet that can be purchased by customers around the world, such as clothes, books, travel tickets, electronic devices, software, etc. In this way, these economic and business activities become profitable, which positively affects countries' economies as they generate revenue while reducing the costs of services and business (Temizel, 2009).

E-commerce has become a powerful tool for businesses and companies in order to explore the marketplace and spread their economic activities worldwide, while providing enormous benefits for the global and local economy.

9.2.1 E-Commerce Attributes

From what has been stated above, e-commerce stands for the technology-mediated commercial exchanges between parties (individuals or organizations) and the electronically based intra or inter-organizational activities that facilitate such exchanges. The following attributes characterized it:

- It is about the exchange of digitized information between parties. This information exchange can represent communication between two parties, coordination of the flow of goods and services, or transmissions of electronic orders. These exchanges can be between organizations or individuals.
- It is technology-enabled. E-commerce is about technology enabling transactions. Web browsers offer perhaps the best-known of these technologies enabling customer interfaces.
- It is technologically mediated. Furthermore, e-commerce is moving beyond technology-enabled transactions to technology-mediated relationships. What is different in e-commerce is that the transaction is mediated much less through human contact and more by technology—and, in that sense, so is the relationship with the customer. The place where the buyers and sellers meet to conduct business is moving from the physical world marketplace to the virtual world. Hence, the business' success rests on the screens and machines that manage customers and their expectations. That is a big difference compared to when all transactions involved human interaction.
- It includes intra- and inter-organizational activities that support the exchange. The scope of electronic commerce includes all these online activities that directly or indirectly support marketplace exchanges between customers, suppliers, partners, competitors, markets, and how they operate internally in managing activities, processes, and systems.

9.2.2 E-commerce and E-business

E-business is sometimes used as another term for the same process. However, it is more often used to define a broader process of how the Internet is changing the way companies do business, how they relate to their customers and suppliers and how they view such functions as marketing and logistics.

Sometimes, the terms e-commerce and e-business are used interchangeably. E-commerce is a term used to describe transacting businesses over the Internet. E-business involves the fundamental reengineering of the business model into an Internet based networked enterprise. The difference between the two terms is how an organization transforms its business operations and practices using the Internet. E-business can include any process a business organization conducts using the Internet, including internal processes such as employee services and training.

Compared with e-business, e-commerce is relatively easy to implement because it involves only three types of integration:

1. **Vertical integration** of a front-end website application to an existing transactions system.
2. **Cross-business integration** of a company with customers, suppliers, or intermediaries such as web-based marketplaces.
3. **Integration of technology processes** for order handling, purchasing, or customer service.

E-business is more difficult to implement because it involves four types of integration:

1. Vertical integration between web front- and back-end systems.
2. Lateral integration among a company and its customers, business partners, suppliers, or intermediaries.
3. Horizontal integration among e-commerce and Enterprise Resource Planning systems (ERP).
4. Downward integration through the enterprise for integrating new technologies with redesigned business processes for E-business.

The message here is clear: Successful companies will early and effective adopters of integrated solutions across "*heterogeneous platforms,"* and between organizations, different functional units and applications, within a secure customer-facing environment. This requires the development of architectures that can work in a distributed and heterogeneous world together with a cultural adjustment where traditional, safe, inwards-looking design and entrepreneurial, rapid development and deployment approaches can work together in mutual respect. The cultural shift may be the more difficult for the two.

E-business requires technical integration as well as cultural integration for its success. It is possible to follow e-business development through a number of strands:

- **Retailing**: This is exemplified by Internet retailing via a Web site, emphasizing the presentation to customer and less attention to back-office functions. Delivery of this service depends on transmission channels to the home and suitable domestic terminals.
- **Enterprise business systems**: The first electronic systems were used to run in-house operations for a limited range of functional units. Little thought was initially given to connecting them and even less to making some of their functionality available online. Recent developments have concentrated on component-based architectures that achieve this integration without replacing existing systems. Once information exchange becomes desirable across organizations and between organizations and their customers, consistent definitions of terms become critical and analyzing market information becomes of great value.
- **Operational security:** Exposure to online trading soon alerted businesses to the need for better security measures to protect against theft or sabotage.
- **Customer support:** the rapid increase in call center activity, predominately voice-telephony, with computer-hosted scripting of standard procedures.
- **Maintenance operations:** They have also followed a traditional path of physical visits, but automated methods are also implemented.
- **Warehousing/logistics:** These also need to be integrated into the end-to-end supply chain, having been largely left to their own devices.
- **Marketing:** Professional skills in marketing and sales campaigning are being applied to the new online sales channels.

9.2.3 E-commerce Categories

As in the case of e-government (Chapter 8), there are several types of e-commerce, which can be:

1. **Business-to-Business (B2B):** A transaction between two or more businesses that involves online wholesaling in which companies sell products and services to other companies. This includes purchasing and procurement, supplier management, inventory management, channel management, sales activities, payment management, and service and support. Major players like *FreeMarkets*, *Dell,* and *General Electric* may be familiar names. However, some exciting emerging consortia combine the purchasing power of traditional competitors such as GM, Ford, and Chrysler, which jointly created *Covisint*. Similar initiatives are under way with industry groups, including pharmaceuticals, commercial real estate development, and electronic subcomponents.
2. **Business-to-Consumer (B2C):** A form that refers to exchanges between businesses and consumers, such as those managed by *Amazon*, *Yahoo*, and *Charles Schwab and Co*. B2C transactions can include the exchange of physical or digital products or services and are usually much smaller than B2B transactions.
3. **Consumer-to-Consumer (C2C) or Peer-to-Peer (P2P):** A business model that helps consumers directly trade with each other while online (Ohene-Djan, 2008). Exchanges involve transactions between and among consumers. These exchanges can include third-party involvement, as in the case of *eBay*. Other operations that support peer-to-peer activity include *Owners.com, Craigslist, Gnutella, Monster,* and *Lavalife*.
4. **Consumer-to-Business (C2B):** Consumers can band together to present themselves as a buyer group in a consumer-to-business relationship. These groups may be economically motivated, such as demand aggregators, or socially oriented, such as cause-related advocacy groups like *SpeakOut.com*.
5. **Mobile Commerce (M-Commerce):** It was coined in 1997, and its purpose is basically "*buying and selling goods and services, using online banking and carrying out bill payments and money transfers through it*" by using devices like cell phones or tablets that connect wirelessly (Kütz, 2006). It is estimated that by 2022, the number of customers adopting mobile banking and mobile commerce services will increase to 2 billion, and banks and companies are investing more and more in improving mobile applications to improve security and customer satisfaction (Hadad, 2013).

Indeed, mobile shopping popularity is constantly on the rise, with customers increasingly using their mobile devices for various online shopping activities. According to a March 2016 study regarding mobile shopping penetration worldwide, 46 percent of internet users in the Asia Pacific region and 28 percent of those in North America had purchased products via a mobile device, whether a smartphone or tablet computer. As of the third quarter of 2017, desktop PCs still accounted for most of global e-retail orders but smartphones were the number one device for retail website visits (Statista, 2018).

Some authors argue that the perspective of a single e-commerce chain is likely to emerge. This chain will be a superset of the categories noted above. Therefore, it is increasingly important to think of a single demand-and-supply chain that can be most accurately characterized as initiating with end-customers and rippling backward through a supply chain to the eventual raw-materials producers. Moreover, the chain can also ripple through the P2P to C2B exchanges. For example, let us consider the purchase of the Harry Potter book at *Amazon.com*. The sale of these books can ripple throughout the e-commerce categories listed above. For the first time, thousands of consumers bought the most recent Harry Potter book through *Amazon*. This purchase triggers an electronic exchange between *Amazon* and the publisher to request more books. This order forces the publisher to print new copies. The new copies trigger orders of paper products, shipping materials (from cardboard suppliers), and ink. Meanwhile, consumers may be able to "demand aggregate" through public websites or corporate bulk-purchase rates. Finally, after the books are read, they can be sold on *eBay*. Thus, it could be argued that the categories of e-commerce are not distinct but rather intimately linked in a broader network of supply and demand.

9.3 E-commerce Consequences

As stated above, technological developments open up enormous business opportunities, although new complex problems arise and must be solved technically. Some of them are:

Geographical Freedom

Certain parts of a trading organization are free from location restrictions. An online store exists solely in cyberspace and is not limited by physical space or property availability. Customers can come from anywhere, which can be considered an advantage. Trading globally certainly increases potential market size, although it sometimes has the potential to increase the complexity of the transaction regarding the place of origin, the governing rules there, etc. In other words, there can be a major impact on the complexity of marketing and logistics. This implies that e-business requires better integration of back-office processes.

But No Hiding-Place

Geographical freedom affects not only the vendor but also the customer who can access e-shops anywhere in the world. This can apply cost and quality of service pressure to the traditional vendor. It may also give rise to a new breed of organizations that can provide broker functions between multiple suppliers and customers, broking on availability, price, interpretation of requirements, and specifications.

Temporal Freedom

A 24/7-day company that shifts its operational base around the clock is heralded as an example of the new opportunity for trading on instant gratification and overtime-independent automation. This can raise a demanding requirement for a company's processes that should operate flawlessly without downtime, a condition that is sometimes difficult to fulfill. There is also a need to provide human cover over a similar span as an exception handling procedure for where things have gone wrong or simply have become too complicated where artificial intelligence algorithms (e.g., chatbots) have not been effective enough to handle such situations. In this case, people must be scheduled to operate call centers at appropriate skill levels, and the centers themselves, in many cases working on an outsourcing basis overseas should handle workload over the diurnal traffic variations.

Freedom to Customize

To meet a "*giving customers what they want*" strategy, there must be a precondition that one knows what they want. Electronic trading provides an almost unique way of acquiring and processing that information. Each transaction with a customer can be recorded, and customer profiles, likes and dislikes are obtained and stored for future use, most of the time, with their consent. Additionally, customers can even be encouraged to construct (virtually) complex online products out of a kit of parts. Technology makes this possible in two ways: first, by removing the need for expensive human support and, secondly, by efficiently transferring this specification to the manufacturing arm without failure or other costs.

Collaboration in Distributed Enterprises

Suppose communication and computing can provide very low-cost ways of passing moving images and voices of geographically dispersed people. In that case, it can do the same with the high volumes of data required to support manual or automated tasks. Companies can concentrate on what they are good at, seamlessly interacting with other organizations with different areas of excellence to create an end-to-end virtual enterprise.

Low Transactions Costs for Payments

Automated and error-free processing of payments can significantly reduce transaction costs to customers and suppliers alike.

In general, electronic commerce has significantly improved the efficiency of economies, enhanced their competitiveness, improved the allocation of resources, and promoted long-term growth.

9.4 E-commerce Impact

9.4.1 Economic and Consumers' Behavioral Changes

The impact of B2C e-commerce on the buyers' behavior has been significant. In the past, when consumers wanted to make purchases, they had to set aside time to shop during certain hours or get informed through catalogues sent to them by ordinary mail. Today, many consumers can use their computers, smartphones, or other portable electronic devices to get informed and shop online. Store hours, geographic restrictions, or mailing lists no longer restrict buyers and sellers in the e-commerce retail trade. With a few simple clicks, they can access various goods and services 24 hours a day, seven days a week, and all year round.

The characteristics of retail e-commerce merchandise have also changed significantly over the fifteen years. In 2000, computer hardware was the most common type of merchandise sold over the Internet. Today, the variety of merchandise is extremely diverse, and shoppers can buy almost anything online. Online shoppers have benefited in other ways. The growth of e-commerce retail sales has reduced consumers' search costs and placed downward pressure on many consumer prices. However, this has led to a substantial decrease in small companies operating in specific industries when they are less involved with e-commerce. Larger businesses, such as retail book outlets, new automobile dealerships, and travel agents can compete more in this new market environment.

The extremely rapid growth of e-commerce retail sales has additionally provided a major boost to residential parcel delivery services, especially after the pandemic burst of Covid-19. This is because online merchandise purchases involve some form of residential delivery by a third-party vendor, such as a freight or postal service. Consequently, there are considerable synergies related to B2C parcel delivery and heavier freight volumes.

9.4.2 Change in Firms' Business Models, Organizations and Market Structure

E-commerce has transformed the marketplace by changing the firms' business models, shaping relations among market actors, and contributing to changes in market structure. Given the dynamic nature of these processes, there is a need for a continuous monitoring of the electronic marketplace. Cybertraders play a catalytic role for companies that are entering electronic markets. Key market players contribute to the evolution and diffusion of e-commerce by spreading e-commerce applications in sectoral and national contexts. An analysis of the role of e-commerce players in different national contexts, and governments' role in leading and encouraging e-commerce solutions is always required.

Electronic commerce's open and global nature has increased market size and changed market structure in terms of the number and size of players involved and how players compete on international markets. The extent to which firms can re-organize in the electronic environment depends on the flexibility and adaptability of the workforce. The task of business re-engineering, taking into account the emerging forms of work organization in electronic markets and the process of "*up-skilling*" workers and redefining their functions in electronic environments, is vital. The digital transformation of firms is more thoroughly analyzed in the following paragraphs of this chapter.

A novel aspect of e-commerce is the emergence of virtual communities in social networks. Firms must investigate the role of virtual communities in shaping new relations and shifting market power among suppliers and consumers. This topic is thoroughly investigated in **Chapter 15**.

E-commerce favors streamlined business processes, flat organizational hierarchies, continuous training and skills acquisition, inter-firm collaboration, and networking. All these elements contribute to a favorable environment for innovation and improved performance.

The changes introduced to the firm's models by e-commerce entail a list of benefits that are distinctly presented in **Table 9.1**.

Table 9.1 *The benefits of e-commerce to firms.*

E-commerce benefits to firms	
Global reach	Rapid location of customers and/or suppliers at a reasonable cost worldwide.
Cost reduction	Lower cost of information processing, storage, and distribution.
Facilitation of problem solving	Enables solving complex problems that have remained unsolved.
Supply of chain improvements	Reduced delays, inventories, and costs.
Business always open	Open 24 hours-a-day/7-days-a-week/365-days-a-year; no overtime or other costs.
Customization/personalization	Enables orders to be made to customer preference.
Ability to innovate, use of new business models	Facilitates innovation and enables unique business models.
Lower communication costs	The internet is cheaper than communicating via telephone.
Efficient procurement	Saves time and reduces costs by enabling e-procurement.
Improved customer service and relationship	Enables direct interaction with customers, and better Customer Relationship Management (CRM).
Small and medium-sized enterprises (SMEs)are encouraged to compete.	E-commerce may help small and medium-sized enterprises or companies to compete against larger companies by utilizing special business models.
Lower inventories	Inventories can be minimized using customization.
Lower cost of distributing digital products	Delivery online can be up to 90% cheaper.
Provide competitive advantage	Enables innovative business models.

9.4.3 Customers' Perspectives

Internet shopping has added value to customers as it enables them to purchase products from anywhere in the world and compare prices in the global market to get the best bargain while having access to a wide range of products. When e-commerce was introduced, people needed clarification about the service level they would receive. Since then, many laws have come into place regarding online activity, allowing e-commerce

organizations to provide excellent services as if they were in a high street store. Customer perspectives on security issues and the ease of using e-commerce websites have also changed. Most of the people who were once hesitant to use credit cards online, now trust online payment methods.

Many products become available online before they are in physical stores, and many people use sites such as *Amazon* to pre-order the latest tech gadgets so that they acquire them as soon as they are released. The ease of price changes should also be highlighted. Pricing changes based on demand, which can be seen by how airlines offer ticket prices based on the number of flights that have already been booked. Typically, early booking allows for purchasing tickets at a lower cost, and prices can change dramatically as demand increases. Similarly, items' prices decline based on the shelf life of an object and many items are sold at discounted prices when new season ranges are introduced.

Another interesting issue is that businesses with online and physical presence give customers more confidence when shopping online because they can visit the store to return items or complain about goods they have purchased online. They can also visit the physical store and try before buying more expensive items, whereas they can order smaller items online. It is common for big retailers to integrate a physical presence with an online presence.

9.4.3.1 Benefits

There are many benefits to consumers when shopping online, some distinctly listed in **Table 9.2**. Online shopping means shopping anytime from the comfort of one's home and having shopping items delivered. This can become extremely important for people living in remote rural areas, people with disabilities or isolated people, especially in the special circumstances that the Covid-19 pandemic has introduced. People can shop whenever they want thanks to anytime access, which is a feature that physical stores hardly ever provide. Prices can be lower as e-commerce companies offer internet discounts because they can run their business at a lower cost as staffing costs are minor compared to having a physical presence.

Table 9.2 *The benefits of e-commerce to Consumers.*

Benefits to Consumers and Society	
Inventory	Wide range of retailers, products, and styles to choose from.
Ubiquity	Enables purchases to be made at any time from any place.
Self-configuration	Enables self-customization of products.
Search for bargains	Use of comparison engine.
Real time delivery	Enables download of digital products.
Enable telecommuting	Ability to work or study at home.
Social interaction	Via social networks.
Find unique items	Using online auctions, collectible items can be found.
Comfortable shopping	Enables shopping at one's leisure without interference.

Enable telecommuting	Facilitates work at home, resulting in less traffic and pollution.
Increased standard of living	Allows purchasing more and cheaper goods/services.
Bridging the digital divide	Allows people in rural areas and developing countries to use more services and purchase desired items.

9.4.3.2 Drawbacks

One of the main drawbacks of e-commerce has always been the payment security. As highlighted earlier, many people lack trust when shopping online due to possible credit card fraud. Additionally, stored customer data can be stolen by companies' servers, raising private data security issues. Another drawback when shopping online is the inability to assess quality and fit without having access to the product. The fact that someone cannot try before buying does deter many consumers. Another disadvantage is that many e-commerce companies rely greatly on delivery services, meaning that many consumers mistrust shopping online when they require a product at a certain time, such as a birthday gift. E-commerce companies need to be confident that they are using a reputable delivery company, as the longevity of their business may depend on this.

Furthermore, a negative aspect of e-commerce organizations is that they can have a negative impact on employment. Running a warehouse does not necessarily require employing sales staff; delivery management staff is reliant alone. Less staff is needed to process 1.000 orders online than across a number of physical stores, increasing company profit but minimizing employment opportunities.

Finally, a negative aspect of e-commerce is that it causes some form of divide. In the developed world, consumers have access to 24/7 goods and services. In contrast, in countries with underdeveloped infrastructure and minimal internet access, the same opportunities are not available, increasing the digital divide on a global scale. 9.5 Statistics

Based on one of the leading statistics organizations in the world (Statista), some interesting data can outline the most recent e-commerce trends globally. **Figure 9.1 presents** the online shopping frequency of internet users in the United States in March 2017.

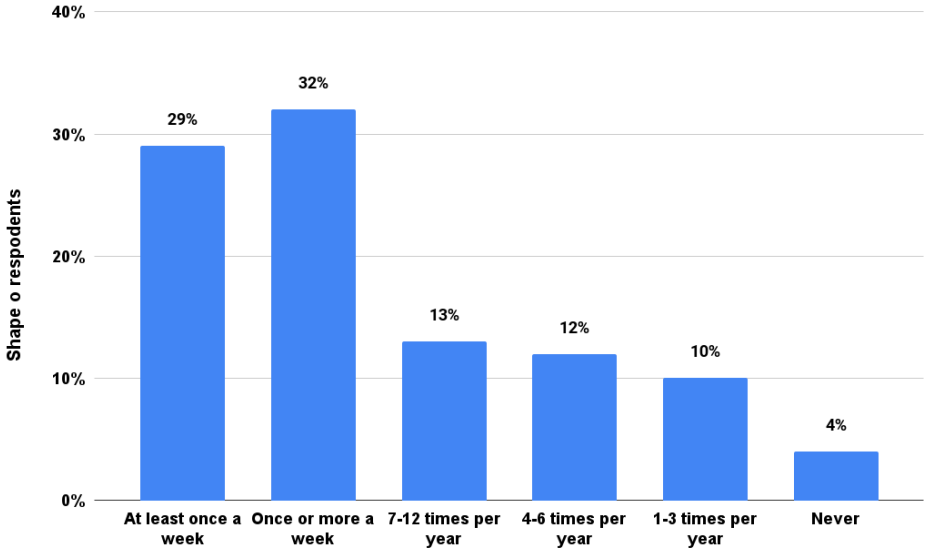


Figure 9.1 *Online shopping frequency of internet users in the United States as of March 2017 (Statista, 2017).*

In the same year, an estimated 1.66 billion people worldwide purchased goods online, and 32 percent of respondents stated that they purchased them online at least once monthly. Global e-retail sales amounted to 2.3 trillion US dollars, and projections indicated a growth of up to 4.48 trillion US dollars by 2021 (Statista, 2017).

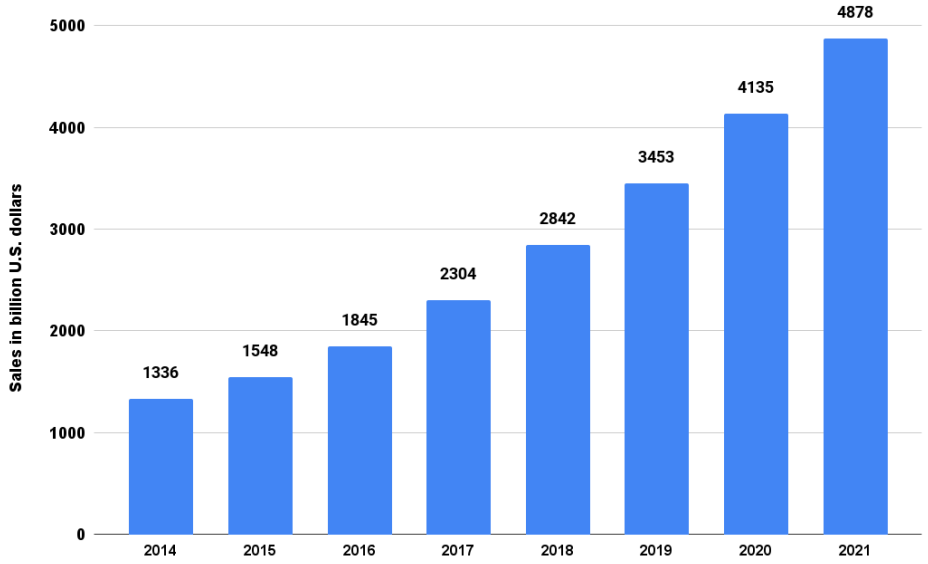


Figure 9.2 *Retail e-commerce sales worldwide from 2014 to 2021 (in billion USD) (Statista, 2017).*

Figure 9.2 gives information on retail e-commerce sales worldwide from 2014 to 2021. In 2017, retail e-commerce sales worldwide amounted to 2.3 trillion US dollars, and e-retail revenues were projected to grow to 4.88 trillion US dollars in 2021. The top 3 online stores' revenue amounted to almost 100 billion US dollars in 2017. Online shopping is one of the most popular online activities worldwide, but the usage varies by region. In 2016, an estimated 19 percent of all retail sales in China occurred via the internet, but in Japan, the share was only 6.7 percent. Back then, Desktop PCs were the most popular device for placing online shopping orders but mobile devices, especially smartphones, were catching up (Statista, 2018).

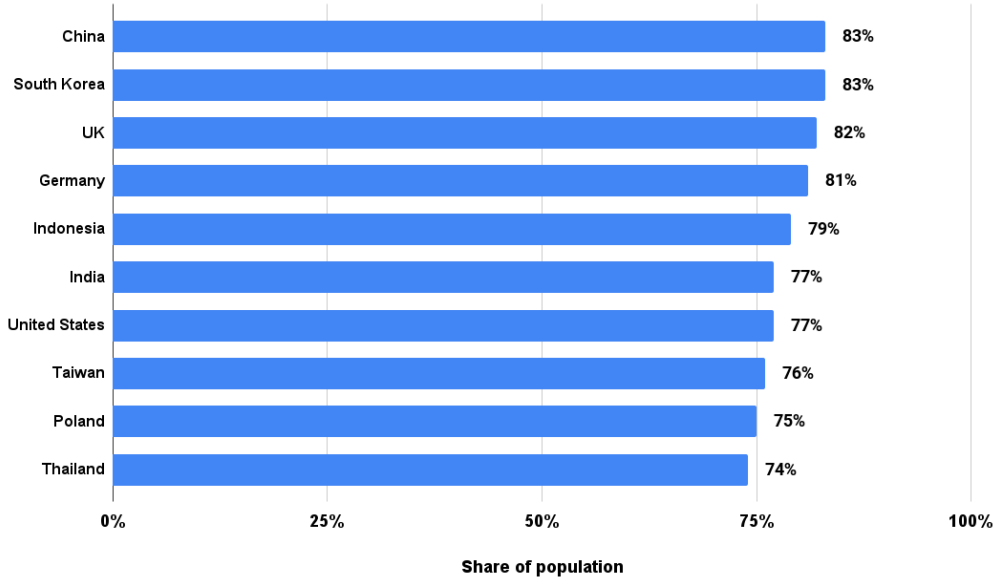


Figure 9.3 *Global markets with the highest online shopping penetration rate as of 2nd quarter 2017 (Statista, 2017).*

Figure 9.3 shows the global markets with the highest online shopping penetration rate as of the second quarter of 2017. During this survey period, it was found that 81 percent of the online population in Germany had bought a product online during the last month of this period. As of the second quarter of 2017, the average value of online shopping orders worldwide via desktop was 136.77 US dollars. Smartphone and tablet purchases lagged with an average order value of 100.75 and 108.18 US dollars, respectively.

In 2015, retail e-commerce sales in the United States amounted to 340.6 billion US dollars and were projected to grow to 543.95 billion US dollars in 2019. Despite the advantages of the already established e-commerce markets, online retail in Asia is catching up. Malaysia ranks first in retail e-commerce compound annual growth rate (CAG) from 2016 to 2021, with a projected growth rate of 23.7 percent. India ranks second with a projected e-retail CAGR of 23 percent.

9.5 The Process of the Digital Transformation of Firms

In literature, the digital revolution is considered the most significant change for enterprises since the Industrial Revolution. The Nasdaq crash highlighted this this in April 2000 (-39,3%!) due to the dot-com bubble, which became the dot-com crash after it exploded. According to IBM Chairman and Chief Executive Officer Louis V. Gerstner Jr., *"the collapse of the dotcoms was not a failure of e-business. It was an overly narrow approach to e-business."* Another reason could have been the lack of agreement about the terms used in the e-commerce sector (Jewels & Timbrell, 2001).

This was the first alarm signal indicating that businesses were not ready to enter the digital era. In the next paragraphs, there will be an attempt to go through the following issues:

- What is the digital transformation,
- What are the stages to reach digital maturity,
- What is the current situation of companies, and in particular European companies, towards their digitization,
- What are the differences between B2B and B2C marketing when it comes to digitalization,
- What are the challenges and opportunities for companies when facing digital transformation.

9.5.1 Digital Transformation

According to the Cyprus Institute of Marketing's Academic Director, digital transformation "*is defined as the realignment of new investment in technology and business models to more effectively engage digital customers at every touchpoint in the customer experience lifecycle."* In order to implement efficiently the digital transformation, businesses must innovate and operate in new ways (Kkali, 2018).

Charles Darwin once said, *"It is not the strongest of the species that survives, but the one that is best able to adapt to the changing environment in which it finds itself."* Thanks to this famous quote from this reputable biologist, it can be comprehended that digital transformation is no longer a choice or an opportunity for firms. However, it is necessary if they want to survive in the digital era we live. (Kkali, 2018).

The website *ResearchAndMarkets.com* gives another definition: digital transformation *"refers to the integration of digital technologies such as artificial intelligence, machine learning, cloud computing, big data, and analytics, mobility and social media into all areas of the businesses, to fundamentally change how the businesses operate and deliver high value to their customers."* It is also pointed out that the digital market weighs 290 billion US dollars and should reach 665 billion by 2023 (Research and Markets.com, 2019).

According to a study done by MIT scientists, the four levels that a business should go through in order to attain digital maturity are the following (Bonnet et al., 2012):

1. **Beginners:** Companies that can use some basic digital tools but they do not manage to use more advanced technologies.
2. **Fashionistas:** Those businesses are trying hard to implement new technologies but do not coordinate them properly so they fail to maximize their benefits.
3. **Conservatives:** They adopt prudent behavior when it comes to new technologies and opportunities; they prefer to focus on their vision and strong governance.
4. **Digirati:** They combine a strong will to invest in new technologies and opportunities and a careful governance that allows them to benefit from digital transformation.

According to current estimations, the distribution of companies between the four levels of digital maturity is given in **Figure 9.4** (Kkali, 2018).

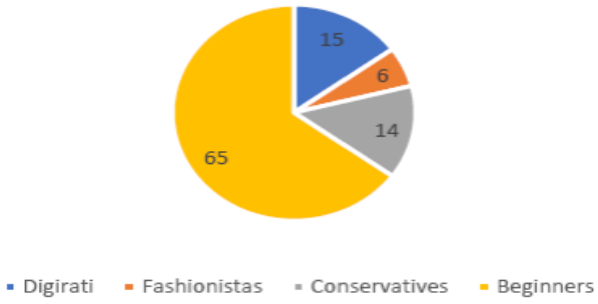


Figure 9.4 *Distribution of businesses between the four levels of digital maturity in % (Kkali, 2018).*

9.5.2 Digital Transformation of Businesses in Europe

As it is outlined in **Figure 9.5**, northern countries in Europe were the most advanced in terms of digital transformation in 2018. Indeed, Denmark, Finland, Ireland, Sweden, and Belgium constituted the top five. Greece was in 24th place among 28 EU countries. Regarding the red color of the sticks ("business digitization"), this is, in fact, the percentage of companies using new technologies (electronic information sharing, Radio Frequency Identification (RFID), social media, e-invoices and cloud solutions) in their daily management. The blue part of the sticks is about SMEs (small and medium-sized enterprises) and their behavior towards e-

commerce (the percentage of SMEs selling online, e-commerce turnover as a percentage of total turnover of SMEs, and the percentage of SMEs selling online cross-border) (European Commission, 2018).

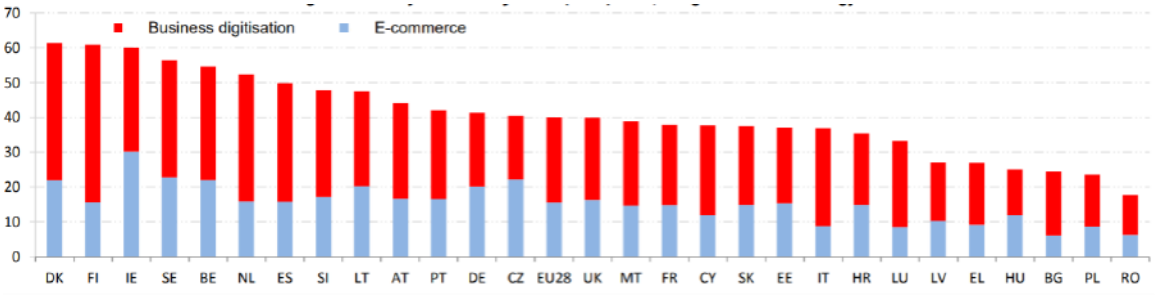


Figure 9.5 *Digital Economy and Society Index (DESI) 2018, Integration of Technology (European Commission, 2018).*

The European Commission has created a set of 10 criteria to assess the digitization situation in each country. These criteria are as follows:

- internet for at least 50% of persons employed,
- fast broadband (30 Mbps or above),
- mobile internet devices for at least 20% of persons employed,
- a website or homepage,
- a website with sophisticated functions,
- social media, sharing supply chain management data electronically,
- the use of Enterprise Resource Planning (ERP) software packages,
- the use of Customer Relationship Management (CRM),
- e-commerce web sales accounting for over 1% of total turnover,
- B2C web sales of over 10% of total web sales.

Figure 9.6 shows the percentage of firms in each country possessing between 10 and 12 (red), between 7 and 9 (light blue), between 4 and 6 (grey), and between 0 and 3 (dark blue) of these criteria in 2017. Again, the northern countries (Finland, Denmark, Netherlands, Sweden and Belgium) made the top five. Greece was still in the 24th position, with more than half of its enterprises attaining a very low level of digital evolution (using between 0 and 3 of the criteria listed before).

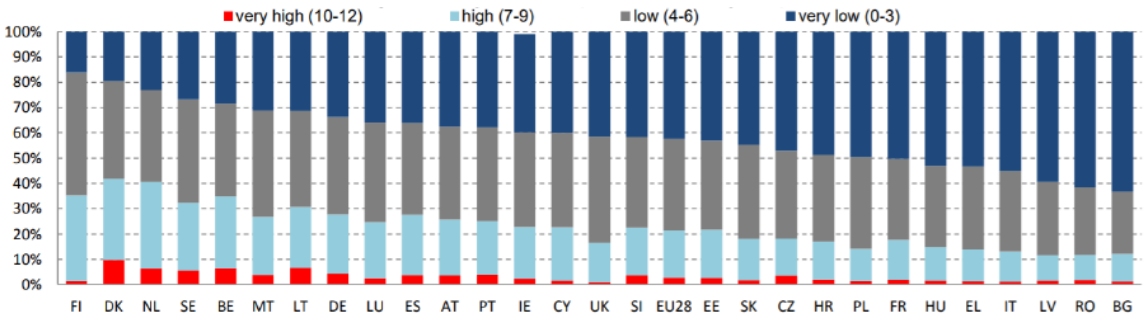


Figure 9.6 *Digital Intensity Index 2017 (% of enterprises by level) (Source: Eurostat).*

There are two main types of e-commerce: the classic web-sales and the Electronic Data Interchange (EDI) - type sales. The latter technology allows data transfer between two computer systems through a dedicated channel and using defined standards without human intervention. Therefore, sales can take place via this EDI technology. In 2017, the percentage of the firm's turnover in the EU that came from EDI-type sales was 12%

while web sales were only 7%. Of those web sales, 4% were from business-to-business or business-to-organization B2BG and 3% were from B2C activities (European Commission, 2018).

9.5.3 The Real Difference Between B2B and B2C

As already stated, B2B e-commerce is "*the use of Web-based technologies to buy, sell or exchange information between two or more companies. B2B transactions can take place directly between companies or through a third party (an intermediary) which helps match buyers and sellers*" (Jewel & Timbrell, 2001). B2C is "*a term describing the communication between businesses and consumers in the selling of goods and services.*" And when the Internet features are now fused, it becomes "the use of Web-based technologies to sell goods or services to an end-consumer." In this last definition, the term "end-consumer" is very important because it avoids any potential confusion between B2C and B2BAfter all, the second B in B2B also means consumer to a certain extent (Jewel & Timbrell, 2001).

It must also be underlined that some businesses can operate in both sectors, B2B and B2C, e.g., an insurance company that can sell insurance products to private individuals (B2C) and other companies (B2B). Consequently, they need to implement different marketing strategies depending on their operating sector. This comparison demonstrates the need to understand the differences between B2B and B2C types of e-commerce.

When operating in a B2B environment, the first concern should be understanding the potential buyers and how they operate. Usually, in B2B transactions, the return on investment (ROI) is crucial for the customer, so it is important to send them the most effective message on how a product or service can help them save time, money, or resources (Lake, 2019). On the other hand, when the target market concerns end-consumers, it is necessary to point out the benefits of a product or service clearly and in a simple and easy way. It should also be kept in mind that end consumers have a shorter decision process than businesses and that this purchasing decision process is most often based on emotion, while it is more based on logic when it has to do with businesses (Lake, 2019).

Finally, presence on the Internet through a website or social media is crucial to communicating with potential customers most effectively. Especially for B2C businesses, it is the message delivered to the customer is the key to the success of a product or service of a business. B2B companies use the web more as a tool to reduce their selling and operating costs, shorten the time between order and delivery, and increase their overall benefits (McCarthy & Patel, 2000).

9.5.4 Challenges and Opportunities of Digital Transformation

As noted in the previous paragraphs, most businesses (65%) are just starting their digital transformation, which is always considered a big challenge. If they are a B2B or a B2C company, the proper strategy must be adopted. If a company is active in both sectors, then it must implement both strategies.

Additionally, it is widely known that people always want to work for the most digitally advanced companies. So, a company to attract the best talents, new technologies always outline a better profile, and therefore, digital transformation is a big opportunity for any business. For example, the most attractive company to work for in the world in 2018 was Google (Barck, 2018), but it is also one of the most developed in digitization (Kane et al., 2015). Moreover, according to a survey conducted by *Cesi, Ipsos* and *Le Figaro*, most companies believe that the expansion of digital technology is an opportunity for their company to rethink their business model, reinvent ways of interacting with their customers and sustainably adapt their production and operating methods using technology. Benoît Perriquet, Vice President of Southern Europe at *OpenText, explained, "Digital transformation projects are carried out in a very heterogeneous way within companies, depending on their organizational structure, size or simply their vision.*" Expectations and motivations are thus

divergent: some companies will favor factors such as cost optimization (22% cite it as their main advantage), while others will justify investment in new technological solutions by the desire to be innovative. However, some challenges remain: 23% of decision-makers consider their company's culture to be the main obstacle to digital transformation (those businesses can be considered as "Conservatives", as seen in the paragraph about the four stages of digital maturity), while 17% point to a lack of internal understanding of the issues (Del Pozo, 2016).

From what has been stated above, there are many opportunities for digitally mature businesses and those that are on the way to reach this level. The example of *Starbucks* demonstrates this verdict. In 2009, the famous coffee shop enterprise's share price fell to half its price. It was clear that something was wrong then, and it was urgent to find solutions to solve the problem. It was then decided to create a new internal service called the *"Department of Digital Ventures."* As a result, four solutions have emerged: free Wi-Fi in all the Starbucks stores, free content such as articles from *The Economist*, faster digital transactions using cell phones or cards and allowing mobile payment (about 3 million payments per week are made through this technology nowadays). The goal of those changes was clearly to reconnect with their customer base. All these modifications have led to an impressive increase in the share price, going from 8 US dollars in 2009 to 78 US dollars in May 2019. This concrete example perfectly shows how digital transformation can transform a challenge into an opportunity (Kkali, 2018).

9.6 Role of Social Media on Consumers' Behavior

As mentioned, the Internet has become a social communication tool, that helps consumers hear and find out each other's opinions and reviews for specific products, brands and shopping experiences. This information consumers share through social media sites is one complex mechanism affecting consumer purchasing decisions. Marketing professionals constantly investigate the magnitude of this impact and how the process operates (see Chapter 15) to understand better how to use social media to develop their business.

The results of scientific research on the impact of social networks on the consumer buying decision-making model and how consumer communications in social networks change certain decisions of the consumer pre/post-purchasing process will be outlined in this paragraph. An analysis of secondary data retrieved from statistical databases of this area is also presented.

9.6.1 A Theoretical Overview

Changes in consumer behavior due to social media are considered one of the most intriguing aspects of modern marketing. The term "*consumer behavior*" assumes that the consumers are actors in the marketplace. According to Engel, Blackwell, and Mansard, *"Consumer behavior is the actions and decision processes of people who purchase goods and services for personal consumption".* Various factors influence consumer behavior:

- Marketing factors, such as product design, price, promotion, packaging, positioning, and distribution.
- Personal factors, such as age, gender, education, and income level.
- Psychological factors, such as buying motives, product perception, and attitudes towards the product.
- Situational factors, such as physical surroundings at the time of purchase, social surroundings, and time factor.
- Social factors, such as social status, reference groups and family, and experience.
- Cultural factors, such as religion, social class—caste, and sub-castes (Chand, 2018).

Social media puts consumers at the center of the business world and provides marketers with a new set of tools to interact with consumers and integrate them into the brands through innovative ways (Chapter **15**). Social media platforms are a potentially powerful medium for finding key consumer influencers, engaging them, and making brand fans. Each user directly influences information about company products and services through online word-of-mouth marketing, the so-called WOM advertising.

Social media platforms provide consumers the arena to share experiences in their social networks and to evaluate businesses through websites featuring reviews and recommendations of products and services. These practices of posting information on frequently visited websites can build or destroy the reputation of a business. Appropriate communication channels and the context of messages are crucial elements in developing trust, as they help to clarify expectations in prospective relationships between companies and customers (Gligorijevic & Leong, 2011).

9.6.2 The Customer's Buying Process

The customer buying process (also called a buying decision process) includes five stages. This 5-stage model can help tailor strategies to increase customer numbers and satisfaction. (Johnston, 2016):

- **Stage 1: Problem Recognition**: The president of the *ITvibes* Company describes this stage as the beginning stage of the customer buying process. Customers identify a problem when they perceive their current situation as different from the what they desire. Whether or not this problem exists, it provides an opportunity for online marketing professionals to show how their products or services can solve the perceived problem (Yenneti, 2016).
- **Stage 2: Information Search:** Now that customers have identified their problem, they are ready to find ways to solve it. They begin to search for more information. This is an opportunity for marketers to intervene and show that their product or service is the solution.
- **Stage 3: Evaluation of Alternatives:** The internet has made it easier for customers to do in-depth research; usually they do not want to purchase unless it is well thought out. They will examine the competition and compare their findings (Yenneti, 2016).
- **Stage 4**: **Final Decision:** At this stage individuals will evaluate different products or brands based on alternative product attributes that can deliver the customer's desired benefits. A factor that heavily influences this stage is the customers' involvement. For example, if the customers' involvement is high, they will evaluate many companies or brands, but if it is low, only one company or brand will be evaluated (Euan Johnston, 2016).
- **Stage 5: Post-Purchase Evaluation:** At this stage, the customers decide whether they like a product. If they are dissatisfied, they may ask for a return. Businesses should use this to learn how to make their brand more effective. Asking for reviews and sending follow-up emails or special promotions are ways to create a positive relationship by establishing brand trust and increasing the likelihood of a returning customer (Yenneti, 2016).

9.6.3 Social Media Influence on Customer Behavior

There are lots of aspects that make an impact and influence customer purchasing decisions at every stage, as they have been presented above. Overall, everything starts with the consumer's attitude. Attitude is usually shaped by a positive or negative experience regarding a certain product (Smith, 1993). In a review of differences between attitudes based on direct or indirect experience, Fazio and Zanna (1981) have stated that attitudes based on indirect experience depend on the expertise and credibility of the source of information.

Kotler and Keller explain that another person's negative attitude towards the preferred alternatives or reluctance to meet the terms of supporting the purchase intention may result in a readjustment of the consumer's initial purchase intention (Kotler & Keller, 2009).

Unanticipated situational factors refer to those that may alter the purchase intention; for instance, there might come an unexpected purchase that is more urgent compared to the purchase the consumer was first stimulated to buy; in other words, preferences and purchase intentions cannot be served as completely reliable predictors of purchase behavior (Kotler & Keller, 2009).

Online reviews by voluntary consumer-generated evaluations of businesses, products, or services by internet users who purchased, used, or had experience with the particular product or service have the potential to make some corrections as well. They typically serve as customer feedback published on a review site or a social media group. In addition to these written opinions and evaluations, a grade or rating may also be assigned to indicate f customer satisfaction. During a survey in 2017 regarding global internet users who post reviews online, it was found that 52 percent of respondents aged 25 to 34 were the most active in posting online product reviews (Statista, 2017).

According to KPMG's recent global survey, 18,430 consumers in 51 countries were asked about their most recent online shopping experiences. This study provided insights and data to help analyze online consumers' behaviors and preferences.

These results show that most (92 percent) of the reviews that consumers across all age groups shared online were positive. The growing tendency for consumers to post positive reviews is driven by many trends, including the rise of social media, where consumers subtly compete with their peers by publicly sharing their latest purchases and experiences; the rise of bloggers whose business models are based on providing product reviews that drive affiliate clicks; and sellers who proactively solicit ratings from happy customers (KPMG International Cooperative, 2017).

Understanding where consumers post feedback can help companies become more proactive in monitoring, managing, and fostering positive online customer reviews. KPMG research described consumers as likelier to post messages directly to seller websites (KPMG International Cooperative 2017). Many popular online sellers have feedback mechanisms built to solicit customers comments shortly after their purchase. By waiting a few days for unhappy customers to register a complaint or return a product, savvy sellers can selectively reach out to those customers who are likely satisfied and willing to post a positive review.

Generational trends indicate an increasing use of social media sites such as Facebook, Instagram, blogs, and X for posting and reviewing feedback (KPMG International Cooperative, 2017). The implication for companies is that user generated reviews are posted on sites that are increasingly beyond their sphere of control or influence. Companies must integrate these social media sites into their marketing and customer strategies. Many digitally innovative retailers and brands have already mastered this approach, but most brands have yet to do so thoroughly. Although Facebook is the most common platform in nearly all regions, it is the preferred choice in North America and Western Europe. Instagram and X are predominantly North American channels, and WhatsApp is particularly popular in Hong Kong, India, Africa, and Latin America (KPMG International Cooperative, 2017).

Finally, the International Congress of Eurasian Social Sciences (ICOESS) research found that social media influences the purchasing behavior of university students. It was also found that Students search social media platforms for products or services before shopping. They also declared *"If they are not satisfied with a product they have bought, they will definitely share this on social media."* Therefore, if businesses cannot manage this case effectively, they may risk losing potential consumers (ICOES, 2017).

9.7 Conclusion

The Internet and the phenomenon of Globalization combined have had a great impact on the world economy and have helped build businesses into empires worldwide. E-Commerce has established itself in the business

world as a great tool to advance into the world's markets. As an innovative byproduct of the Internet, it has the potential to transform economies and market structures, establishing a considerable share of the world's market. A key reason for the rapid growth of e-commerce, especially the B2B segment, is its significant impact on costs associated with inventories, sales execution, procurement, and distribution.

The rate at which technology develops reinforces the possibility of introducing innovative products and services, giving e-commerce the floor to grow rapidly and penetrate the world business by having a prevalent and pervasive influence on a global scale. E-commerce has transformed the marketplace by changing firms' business models, shaping relations among market actors, and contributing to changes in market structure. The competition becomes stronger among markets, while the costs are drastically reduced just because e-commerce has helped eliminate space limitations while lowering entry costs, and not only. Therefore, small businesses can expand on a local and global scale (Davies, 2014). Therefore, economic growth is emerging, helping local economies, positive effecting global markets (Bain, 2017).

E-commerce covers outward-facing processes that touch customers, suppliers, and external partners, including sales, marketing, order taking, delivery, customer service, purchasing raw materials and supplies for production, and procurement of indirect operating-expense items, such as office supplies. It involves new business models and the potential to gain new revenue or lose some existing revenue to new competitors. On the other hand, E-business includes e-commerce but also covers internal processes such as production, inventory management, product development, risk management, and human resources. E-business strategy is more complex, focused on internal processes, and aims at cost savings and efficiency, productivity, and cost savings improvements.

References

Bain M., 2017. “National borders can’t contain the new phase of global connection.” Available at: https://qz.com/1149224/e-commerce-is-driving-a-new-phase-of-globalization/ [Accessed 5 May 2019].

Barck J., 2018. “Europe’s Most Attractive Employers 2018” [online]. Available at: https://universumglobal.com/europes-most-attractive-employers-2018/ [Accessed: 28 April 2019].

Bonnet D., McAfee A., and Westerman G., 2012. “The Advantages of Digital Maturity.” *MIT Sloan Management Review*, Digital Business [online]. Available at: https://sloanreview.mit.edu/article/the-advantages-of-digital-maturity/ [Accessed: 20 April 2019].

Chaffey D., 2011. *E-business and e-commerce management*. Pretince Hall.

Chand S., 2018. "Consumer Behaviour: Meaning/Definition and Nature of Consumer Behaviour." Available at: https://www.yourarticlelibrary.com/marketing/market-segmentation/consumer-behaviour-meaningdefinition-and-nature-of-consumer-behaviour/32301 [Accessed 21 May 2018].

Davies A., 2014. “The globalization of business – E-commerce companies,” Available at: https://www.ivoryresearch.com/writers/amelia-davies/ [Accessed 22 May 2019].

Deelmann T., and Loos P., 2002. "Trust economy: Aspects of reputation and trust building for SMEs in e-business." *Proceedings of the Eighth Americas Conference on Information Systems*.

Del Pozo A., 2016. “Les études sur la digitalisation des entreprises!” [online]. Available at: https://entreprisedigitale.info/etudes-digital-partout/ [Accessed: 29 April 2019].

Dennis C., and Harris L. 2002. *Marketing the e-Business*. 1st edition. London: Routledge.

European Commission, 2018. “Integration of Digital Technology.” Digital Economy and Society Index Report 2018 [online]. Available at: https://ec.europa.eu/digital-single-market/en/integration-digital-technology [Accessed: 28/04/2019].

Fazio R. H., and Zanna M. P., 1981. "Direct experience and attitude-behavior consistency." In L. Berkowitz (Ed.), *Advances in experimental social psychology*. New York: Academic Press.

Gligorijevic B., and Leong B., 2011. "Trust, reputation and the small firm: Building online brand reputation for SMEs." *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*.

European Commission, 2018. *eGovernment Benchmark 2018 - Securing eGovernment for all.* Brussels: European Union Publications.

Hadad S., 2013. “Challenges for Banking Services in the Knowledge Economy,” *Management Dynamics in the Knowledge Economy.* Vol.7 (2019) no.3, pp. 337–352. Available at: https://doi.org/10.25019/MDKE/7.3.04 [Accessed 20 August 2021].

Ibikunle F., 2009. “WiMAX: Appropriate Technology to Provide Last Mile Access to ICTs Infrastructure and Services in Rural Areas.” WIMAX New Developments, Upena D Dalal and Y P Kosta, IntechOpen, https://doi.org/10.5772/8261 Available at: https://www.intechopen.com/books/wimax-new-developments/wimax-appropriate-technology-to-provide-last-mile-access-to-icts-infrastructure-and-services-in-rura [Accessed 23 April 2019].

Influence Central, 2014. "E-Commerce Reviews: The Dramatic Impact on Consumers." Path to Purchase. Available at: https://influence-central.com/e-commerce-reviews-the-dramatic-impact-of-online-reviews-on-consumers-purchasing-journey/ [Accessed 22.05.2018].

International Congress Of Eurasian Social Sciences, 2017. "THE EFFECT OF SOCIAL MEDIA ON MARKETING."

Jewels T. J., and Timbrell G. T., 2001. "Towards a definition of B2C and B2B e-commerce." *ACIS 2001 Proceedings*, Paper 56 [online]. Available at: http://aisel.aisnet.org/acis2001/56 [Accessed 13 March 2019].

Johnston E., 2016. "5 steps to understanding your customer's buying process." Available at: https://www.b2bmarketing.net/en-gb/resources/blog/5-steps-understanding-your-customers-buying-process [Accessed 23 May 2018].

Jow M., 2012. "How globalization of e-commerce is helpful for business." Available at: https://www.selfgrowth.com/articles/how-globalization-of-e-commerce-is-helpful-for-business [Accessed 4 May 2019].

Kane G. C. et al., 2015. "Strategy, not technology, drives digital transformation." *MIT Sloan Management Review*, Becoming a Digitally Mature Enterprise [online]. Available at: https://kityna.ga/146142.pdf [Accessed: 22 April 2019].

Kkali M., 2018. "Digital Transformation: Challenges and Opportunities for Businesses." Cyprus Institute of Marketing, *Business Bulletin* [online]. Available at: https://cima.ac.cy/bulletin-details/business-bulletin/digital-transformaiton [Accessed: 13 March 2019].

Kotler P., and Keller K. L., 2009. *Marketing management*. Upper Saddle River, N.J: Pearson Prentice Hall.

KPMG International, 2017. Global Online Consumer Report.

Kütz M., 2006. "Introduction to E-Commerce: Combining Business and Technology Information." 1st edition.

Lake L., 2019. "Understanding the Differences Between B2B and B2C Marketing" [online]. Available at: https://www.thebalancesmb.com/b2b-vs-b2c-marketing-2295828 [Accessed: 13 March 2019].

Lee G., 2014. *E-commerce, E-business and E-service*. CRC Press, Hong Kong.

Leiner B., Cerf G. V., Clark D. D., Kahn E. R., Kleinrock L., Lynch C. D., Postel J., Roberts G. L., Wolff S., 1997. "Brief History of the Internet." *Internet Society*.

Levine R., Locke Cr., Searls D., and Weinberger D., 1999. The Cluetrain Manifesto.

Manzoor M., 2010. *E-commerce: an introduction*. LAP LAMBERT Academic Publishing.

McCarthy M. P., and Patel K., 2000. "Digital Transformation: The Essentials of E-Business Leadership" [online]. Available at: https://dl.acm.org/citation.cfm?id=578942 [Accessed: 13 March 2019].

Nanehkaran A. Y., 2013. "An Introduction to Electronic Commerce." *International Journal of Scientific and Technology Research*, Vol. 2, Issue 4.

Nuray T., 2011. "The impact of e-commerce on international trade and employment." *Procedia - Social and Behavioral Sciences*, Volume 24, p. 745–753. Available at: https://www.sciencedirect.com/science/article/pii/S1877042811015382 [Accessed 9 May 2017].

OECD, 1999. "Economic and Social Impact of E-commerce: Preliminary Findings and Research Agenda," *OECD Digital Economy Papers*, No. 40, OECD Publishing, Paris. Available at https://doi.org/10.1787/236588526334 [Accessed 11 April 2017].

Ohene-Djan J., 2008. "Electronic Commerce," University of London.

Raynolds M., 2000. *Beginning E-commerce*, Wrox Press Ltd, Canada.

Rayport J.F., and Jaworsky B., 2004. *Introduction to E-commerce*. Mc. Graw-Hill Companies.

Research and Markets, 2019. "Digital Transformation Market - Global Forecast to 2023: Increasing Usage of Disruptive Technologies Such as AI, ML, and Big Data" [online]. Available at: https://www.globenewswire.com/news-release/2019/04/19/1806977/0/en/Digital-Transformation-Market-Global-Forecast-to-2023-Increasing-Usage-of-Disruptive-Technologies-Such-as-AI-ML-and-Big-Data.html [Accessed: 20 April 2019].

Smith P.R., 1993. *Marketing Communications: An Integrated Approach*. London: Kogan Page Ltd.

Statista, 2017. "Online reviews - Statistics and Facts." Available at: https://www.statista.com/topics/4381/online-reviews/ [Accessed 22 May 2018].

Statista, 2017. "Online shopping frequency of internet users in the United States as of March 2017." Available at https://www.statista.com/statistics/448659/online-shopping-frequency-usa/ [Accessed 23 May 2018].

Statista, 2017. "Percentage of global internet users who use online reviews for brand and product research as of 3rd quarter 2017, by age group." Available at: https://www.statista.com/statistics/510532/using-consumer-reviews-for-brand-research-global-age/ [Accessed 23 May 2018].

Statista, 2017. "Global markets with the highest online shopping penetration rate as of 2nd quarter 2017." Available at: https://www.statista.com/statistics/274251/retail-site-penetration-across-markets/ [Accessed 23 May 2018].

Statista, 2018. "Online shopping behavior in the United States - Statistics and Facts." Available at: https://www.statista.com/topics/2477/online-shopping-behavior/ [Accessed 24 May 2018].

Statista, 2018. "Retail e-commerce sales worldwide from 2014 to 2021 (in billion US dollars)." Available at: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ [Accessed 23 May 2018].

Sternthal B., and Craig C. S., 1982. *Consumer Behavior: An Information Processing Perspective*. Englewood Cliffs, NJ: Prentice Hall, Inc.

Sumanjeet, 2017. "Social Implications of Electronic Commerce." *Journal of Social Sciences - Taylor and Francis online*, Volume 21, 2009 - Issue 2. Available at: https://doi.org/10.1080/09718923.2009.11892757 [Accessed 14 May 2017].

Temizel A., 2009. "Introduction to E-Commerce." Topic 3, *E-Business Environment and Architecture*. Available at: http://ocw.metu.edu.tr/course/view.php?id=20 [Accessed 22 March 2018].

The Entreprisers Project, 2019. "What is digital transformation?" [online]. Available at: https://enterprisersproject.com/what-is-digital-transformation#q1 [Accessed: 13 March 2019].

Totonchi J., and Kakamanshadi G., 2011. "Globalization and E-Commerce," *2nd International Conference on Networking and Information Technology*, IACSIT Press, Singapore.

Turbain E., King D., Lee J.K., Liang T.P., Turban D.C., 2015. *Electronic Commerce: A Managerial and Social Networks Perspective*, 8th Edition.

Whyte W.S., 2001. *Enabling E-business*. John Wiley and Sons, Ltd, England.

Yenneti S., 2016. "The Customer Buying Process and How to Use Online Marketing at Each Stage." Available at https://www.huffingtonpost.com/siva-yenneti/the-customer-buying-process_b_9276432.html?guccounter=1 [Accessed 22 May 2018].

Chapter 10 Social Movements and Activism in the Digital Age

Abstract

This chapter discusses how social movements and collective actions that were previously conducted offline have now transitioned to the online age. Various groups of individuals or organizations, which may be informal and large in size, focus on specific political or social issues and express themselves in the national or global digital sphere. Online Activism is also introduced, referring to efforts to promote, impede, or direct social, political, economic, or environmental changes. In the Digital Age, the distance between talk and organized action has grown smaller, highlighted in the various forms of Online Action: the online equivalents of the offline forms of action, forms of Civil disobedience, Hacktivism, Slacktivism, etc. Several case studies are presented within this context, including the Anonymous, the MeToo Movement, Black Lives Matter, the case of Wikileaks, #climatechange etc. Finally, the particular role of social media in forming and coordinating contemporary forms of protesting is highlighted, and the cases of the Arab Spring, the Indignado Movement, and Occupy Wall Street are analyzed.

10.1 Introduction

Starting with the financial crisis in 2008, many social movements all over the world occurred within a short time and which, to some extent, all referred to each other: the so-called *Arabian Spring*, the uprisings of Gezi Park in Istanbul, the *movement of squares* in Spain and latest the *umbrella revolution* in Japan or *Nuit Debout* in France, to name just a few famous. All had one thing in common: All of them were either reported as *The Facebook revolution* (cf. The Guardian, 2010) or social media was reported to coordinating and informing for these social movements. The question raised by all these media reports is how did the latest social movements develop and what the "real" role of social media in their development was from a scientific point of view? One of the most popular social movements was the Occupy Wall Street (OWS) movement, which can be taken as an example of all the "Facebook revolutions." To answer the question, it is first necessary to understand the transformation of social movements in the age of digital media. Indeed, the development of digital technology, i.e. Web 2.0, has changed how the world is connected. More importantly, people increasingly utilize social media Web 2.0 applications for information and interpersonal communications. Protest practices and, more generally, collective actions/social movements have thus shifted from real-life settings to virtual environments. Web 2.0 technologies have clearly changed the way in which social movements and protest activities can now be enacted and coordinated.

10.2 Collective Actions and Social Movements

10.2.1 A Theoretical Framework

Collective action corresponds to actions undertaken by individuals or groups for a collective purpose, such as advancing of a particular ideology or idea or the political struggle with another group. Fundamentally, collective actions are a way people choose to organize and interact together in order to achieve collective outcomes. In this perspective, the definition of social movement is very similar. Tilly defines social movements as "*a series of contentious performances, displays, and campaigns by which ordinary people make collective claims on others*" (Tilly, 2004). Thus, social movements can give us an insight into human actions and why people voluntarily cooperate and mobilize. This is a crucial issue for political and social sciences: to comprehend why and how people choose to interact to achieve collective goals and the common interest instead of only defending their personal benefit.

It must be noted that collective actions/social movements are both the results of:

- An opportunity structure, such as a country's economic, institutional, and social context, which can generate grievances/claims by the citizens.
- A mobilizing structure, which is the social networks and all resources necessary for popular mobilization.

In his introductory work, Sociologist Jonathan Christiansen tried to define the standard characteristics of a social movement for a scientific view of social movements. Therefore, he referred to the scientific development of social movement studies and argued, that *"despite all of the differences in social movements though, there are important analytical similarities that sociologists have distinguished"* (Christiansen, 2015). According to him, a social movement is neither a political party nor an interest group (because these rely on "stable political entities that have regular access to political power") nor is it a mass fad or trend, which is unorganized, fleeting, without goals and on an individual base, but something in between.

Christiansen argues, therefore, that social movements *"can be thought of as organized yet informal social entities that are engaged in extra-institutional conflict that is oriented toward a goal."*

According to the literature, there are four levels of movements: local, state, or regional, national and global.

Local movements are focused on local or regional purposes like protecting natural areas, preserving an important building that is about to be demolished, or calling out politicians for corruption and schools for failing to upgrade education programs. Some movements may also protest for a poor aboriginal population or low-income levels.

State or regional movements affect a larger area but still within national borders. For instance, the right-wing social movements of the 1980s and 1990s campaigned on behalf of the independence of western Canada from the rest of the country.

National movements intend to grab national public attention on native issues. For example, a national issue that has given birth to many activist groups is homosexual marriage.

Global movements are networks of groups and individuals whose collaboration across borders aims to advance thematically similar agendas throughout the world. These networks of actors define their causes as global and organize campaigns and other forms of protest to target international governmental organizations. Global movements take action in general areas of concern, such as efforts to reduce poverty and the use of genetically modified organisms in food. Another example is the Occupy Wall Street movement, which soon went global although it was initially a local movement.

Despite the levels of social movements, we can sort them by what they want to change and how much they want to change it (Aberle, 1966), as follows:

- **Redemptive** movements intend to provoke inner change or spiritual growth through groups. For example, organizations like *AA* (Alcoholics Anonymous) help individuals obtain their meaning in life.
- **Alternative** movements focus on self-improvement and targeted changes to individual beliefs and behavior, like *Planned Parenthood* and the *Slow Food* movement.
- **Revolutionary** movements seek to completely change every aspect of society, like the Cuban movement of the 26th of July.
- **Reform** movements, which aim to change something specific related to the social structure, like the National Action Committee on the status of women and anti-nuclear groups.
- **Resistance** movements, which aspire to undo or prevent a change to the social structure, with the Ku Klux Klan being a characteristic example.

A social movement has a certain life cycle, and as Blumer and Tilly concluded, this cycle consists of four stages. The four stages of social movements are as follows:

- **Stage 1: Emergence.** This is the first stage of a social movement's life cycle, characterized by people becoming aware of a social or political issue. Movements in this stage lack clearly defined strategies for achieving goals and have little organization.
- **Stage 2: Coalescence.** The second stage of a social movement's life cycle is characterized by people coming together and forming groups to spread awareness. Demonstrations and formulation of strategy mark this stage. **Stage 3: Bureaucratization or institutionalization.** The movement is an organization in this stage, with paid staff. Formal organizations and trained staff carry out its strategy. However, the movement may never grow beyond this second stage, and members may never develop into formal organizations. Some social movements consciously choose to reject bureaucratization for ideological reasons. This is particularly prevalent as technology increases, allowing movement members to communicate and engage with the movement through Internet websites without formal groups ever coming together.

- **Stage 4: Decline.** This stage usually marks the end of mass mobilization, where the movement has achieved its goal or people no longer care about the issue.

As social movements can decline for several reasons, Christiansen identified five reasons: success, organizational failure, co-optation, repression, or establishment within mainstream society.

10.2.2 Some Pre-Internet Movements

The *Abolitionist movement* was an organized effort to end the practice of slavery in the United States. Some of the very first abolitionists were white, religious Americans, but the prominent leaders were black men and women who had escaped from bondage. Abolitionists saw slavery as an abomination, making it their goal to eradicate slave ownership. In 1860, Republicans, led by Abraham Lincoln, supported the movement's ideas. Southern leaders believed that Lincoln would stop slavery, as they had already become a minority in the House of Representatives. The long-standing controversy over the enslavement of black people, the divisiveness and animosity fueled by the movement, and the power struggle between both sides reaching its peak led to the Civil War in 1861. The Civil War ultimately meant the end of slavery in America. However, historians argue that the effort did not stop until voting rights were granted to black men (Abolitionist movement, 2009).

Another historical social movement was the *Women's Suffrage* Movement. The demand for women's suffrage started to strengthen in the 1840s. It was becoming a more significant aspect of the Women's Rights movement's activities when women began to give public speeches in opposition to slavery and support of their rights. In 1848, the first Women's Rights Convention approved a resolution favoring women's suffrage despite opposition from some organizers, who considered the idea too extreme. The first national suffrage organizations were established in 1869 when two competing organizations were formed, one led by Susan B. Anthony and Elizabeth Cady Stanton and the other by Lucy Stone (Washington, 2018). The same year, Wyoming became the first state to approve full voting rights for women. In the early 1870s, suffragists tried to vote and then filed lawsuits when turned away, hoping the United States Supreme Court would rule that women had a constitutional right to vote. In 1873, the Women's Christian Temperance Union, the largest women's organization at that time, also fought for women's suffrage, giving a massive uplift to the movement (Burlingame, 2004). Throughout the years, women won the right to vote in some states. Campaigns increased after the turn of the century, and by 1918, as Congress debated the 19th Amendment, women already had the right to vote in 20 states.

Finally, the *Civil Rights* Movement was the movement where African Americans struggled for decades to end institutionalized racial discrimination and segregation in the United States. In 1954, a new movement emerged, which, with nonviolent protests and civil disobedience, produced dialogues between activists and government authorities, leading to radical changes. Two of the most famous civil rights activists were Dr. Martin Luther King Jr. and Malcolm X. King, the former best known for his "I have a dream" speech at the Lincoln Memorial in 1963. Malcolm X. preached equality to all races and his charisma helped him convince the public to join the Civil Rights Movement. The movement's efforts to gain black people's rights led to the desired changes, including voting rights, civil rights laws against workplace discrimination, marriage between persons of different races, equal access to housing regardless of race etc.

10.3 Social Movements in the Internet Age

Considering, the four stages listed above, we can see how the Internet and especially Web 2.0 technologies have facilitated the formation of social movements and thus the enactment of collective actions. It is evident that neither people's grievances nor a particular context of instability (opportunity structure) are enough to bring people to act collectively. Above all, social movements need organization and resources. Thus, resource

mobilization theory argues that resources such as time, money, organizational skills, and certain social or political backgrounds are all critical to the formation and success of social movements.

As social media expands, it has been used to coordinate mass movements, mainly due to its structure: it provides direct and 2-way communication compared to the traditional media (radio, television, and newspapers). This interaction may change or affect the structure of a movement, an organizational or activist network, or a campaign. **Figure 10.1** presents a model describing how social media can affect political movements, which, if implemented, can boost social media activism. However, it must be highlighted that the use of traditional media is always of high importance as well.

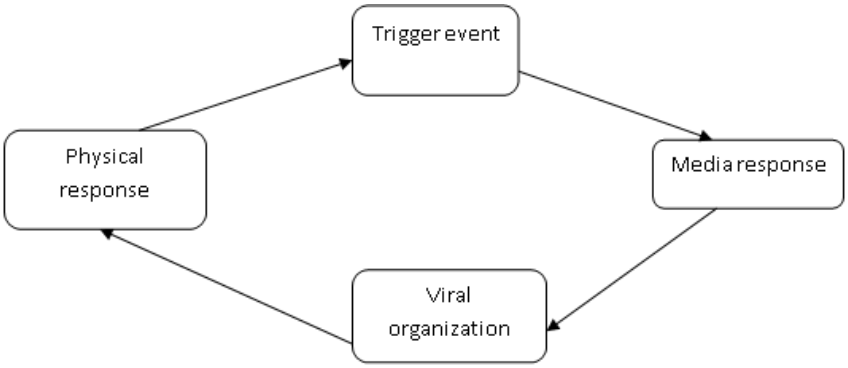


Figure 10.1 *Trigger event: Triggering through the creation of a group. Media response: Dissemination through social media. Viral organization: The organization becomes popular as the movement's outcome. Physical response: In some cases, there is an actual, physical response.*

Tilly was also the first to underline the crucial role of social capital as a resource in social movements. According to him, the primary unit of social movements is not the individuals but the interaction between them. Thus, communication, as a convey of information, is fundamental in achieving collective actions and we conclude that social movements depend on social networks.

All these resources and abilities that have been listed above also represent "costs" for individuals and thus constitute both conditions and obstacles for the achievements of collective actions (in a rational choice approach). It is in this perspective that Web 2.0 technologies have considerably lowered the costs of participation and thus enabled the formation of massive and more diverse social movements.

Shirky (2011) was one of the early scholars to write about social media as a new social networking tool for collective action. He argues that the world communication system has become denser, more complex, and more participatory over the years. People have gained greater access to information, more opportunities to engage in public speech, and, thus, an enhanced ability to undertake collective action.

Indeed, the emergence of the Internet in the 1990s marked a turning point in the sphere of communication; and a bit later, the adoption of social media applications like Facebook, X, and the blogosphere has become a part of online life and has transformed the way people get information and socialize. Traditional organizational tools used to mobilize would use social hubs such as universities, coffee shops, group meetings, etc., to spread information. But the irruption of social media has offered the possibility of more reciprocal communication between ordinary citizens without the necessary intermediation of mainstream media or traditional organizational structures or leaders. It has allowed people to meet without of time, distance, and money constraints. The Internet has dramatically modified the way information is provided and has initiated the principle of co-production of information—every citizen can now be potentially a kind of journalist (known as "citizen journalism").

Through social media, individuals can connect with each other and organize at a meager cost the creation of a group and events, share hashtags, and upload videos. These are indeed "cheap" ways to engage

with political and social issues. More than that, social media is also a resource available to most people; this means that even uncommitted individuals might be able to join the cause. So, one of the core consequences of this change is that a new type of protester may be emerging: the skillful young social media user who is occasionally, and maybe ephemerally, mobilized by calls for action in her/his "news feed," is not affiliated with any formal organizations (but he/she uses the protest event's official hashtag), has not necessarily been politically involved previously, and is more prone to participating in a one-off mobilization or protest event that expresses his/her values and identity preferences.

In any case, the significant contribution of digital media to social movements and political protests would be described by the terms "mobilization," "validation", and "scope enlargement" (Gamson & Wolfsfeld, 1993). All these factors are important concerning the participants, the message they want to pass, and the unfavorable conditions against which they are protesting. In fact, social movements depend on the media to generate public sympathy for their challenge (Butsch, 2007).

10.4 Online Activism, Hacktivism and Slacktivism

10.4.1 From Traditional Activism to Online Activism

Activism includes all efforts to promote, impede, direct, or intervene in social, political, economic, or environmental reform to change society toward a perceived greater good. Therefore, activism has different forms and policies, such as social, political, or hashtag activism. Social and political activism has a social cause or a political goal that should be achieved through a group of people doing a specific action. In general, activism aims to attain a change in society or inspire governmental action. It is the *"use of a direct, proactive and often confrontational action"* (Alto et al., 2011) and can occur in many different forms, like fundraising, donations, demonstrations, strikes, boycotts, campaigns, etc. All those actions require a certain degree of involvement and being "active" to a certain extent.

Online activism (also known as digital activism, cyberactivism, and e-activism) uses electronic ICTs such as social media, e-mail, and podcasts to enable faster communication by citizen movements and the delivery of local information to a large audience. Internet technologies are also used for cause-related fundraising, community building, lobbying, organizing, and coordination. Research has started to address how activist/advocacy groups in the US and Canada use social media to achieve digital activism objectives.

Online activism is construed as the complementary online equivalent of traditional activism but can also be deployed as a standalone form. Digital tools can support traditional activism in many ways. For example, they allow organizers to mobilize large numbers of people quickly, help draw media attention to causes and allow for a centralized portal of information. Today's highly publicized Internet activism is just as effective as traditional activism. In fact, Internet activism can reach a larger audience faster and keep a live two-way communication channel at the disposal of organizers and supporters.

Traditional forms of activism center around one event. With the web, there are many ways to keep in touch with all the supporters, and a movement may quickly dwindle. In an online movement, a constant line of communication is open for organizers to relay information about the campaign's upcoming activities that can engage supporters.

Many critics of Internet activism accuse it of being too easy and appealing to pop culture impulses. Critics say that the ease and appeal of this type of activism could not enact real change, and in the early days, they added that there were few historical precedents for online movements that proved to be effective. From this perspective, even though Internet use has catalyzed the speed at which people learn about major issues, Internet activism cannot be reliable, and traditional forms of activism still serve as the driving force that can promote change. However, in recent years, this approach has proven to be quite simplistic, if not problematic,

and historical events showed that it is often pointless to discriminate between the two complementary components: online and offline activism.

Traditional activism is indeed enhanced by digital tools, sometimes greatly. Digital networks made it possible for large groups to easily link to one another, exchange content, and coordinate acts, underlining the capability to create effective movements quickly and reliably in an amazingly short time. Web 2.0 applications also had a major effect on activism as well. By interlinking, forming virtual communities, and using hashtags (a popular form of topic categorization over several social networking sites), the diffusion of information and coordination can move to new levels. Due to the large number of connected users, awareness for a certain topic can be raised almost instantly and campaigns can spread dramatically fast all over the world within hours due to sharing retweets and likes. Furthermore, through crowdfunding, donations can lead to great supporting funds that would never be attained that effectively using offline methods.

10.4.2 Examples of Early Online Activism

One of the earliest known uses of the Internet as a medium for activism was that around Lotus Market Place. On April 10, 1990, Lotus announced a direct-mail marketing database product to contain name, address, and spending habit information on 120 million US citizens. While much of the same data was already available, privacy advocates worried about the availability of this data within one database. Furthermore, the data would be on CD-ROM and remain fixed until a new CD-ROM was issued. In response, a mass e-mail and E-bulletin-board campaign was started, which included information on contacting Lotus and form letters. Larry Seiler, a New England-based computer professional, posted a message widely reposted on newsgroups and via e-mail: *"It will contain a LOT of personal information about YOU, which anyone in the country can access by just buying the discs."* Over 30,000 people contacted Lotus and asked for their names to be removed from the database. On January 23, 1991, Lotus announced that it had cancelled Marketplace.

Another well-known example of early Internet activism took place in 1998 when the Mexican rebel group EZLN used decentralized communications, such as cell phones, to network with developed world activists and helped create the anti-globalization group Peoples Global Action (PGA) protest to the World Trade Organization (WTO) in Geneva. The PGA continued to call for *"global days of action"* and rally support of other anti-globalization groups in this way.

In the UK, in 1999, the Government introduced a new employment tax called *IR35*. One of the first online trade associations was created to campaign against it. Within weeks, they raised £100,000 off the Internet from individuals they had never met. They became a fully formed trade association called the Professional Contractors Group, which two years later had 14,000 members, all paying £100 each to join. They presented the first ever e-petition to Parliament and organized one of the first flash mobs when using their database; to their surprise and that of others, 1,000 came in their call to lobby Parliament. They later raised £500,000 from the Internet to fund an unsuccessful High Court challenge against the tax, though ultimately, they secured some concessions. Their first external affairs director, Philip Ross, has written a campaign.

10.4.3 Hacktivism

10.4.3.1 Overview

The concept of hacking is as old as the emergence of computer networks. In the beginning, the word hack was used to describe any new and innovative use of technology. As time passed, mass media greatly associated hacking with illegal computer activities such as computer intrusions rather than with technologically innovative uses of computers. This trend led to the emergence of another definition, called cracking, a term used by hackers to describe an unwanted entry into a computer system by either an explorer or a criminal

(Jordan, 2002). Being both a hacker and a cracker is very crucial for hacktivism, which can be defined as the marriage of activism and hacking by using hacking techniques against an online target such as web sit-ins and virtual blockades, automated email bombs, web hacks, computer viruses and worms and computer break-ins as mentioned by Denning. This plethora of tools and techniques makes the boundaries between e-activism, hacktivism, and cyberterrorism fuzzy according to Denning (Denning, 2001). This difficulty in defining the distinctive lines between those different online activities makes it challenging to pinpoint the date that hacktivism emerged.

As for the term hacktivism, Taylor suggests that it came from an article written by a convicted hacker named Kevin Poulsen in 1998 entitled "Grassroots Hacktivism." This article responded to an intrusion on the New York Times' Website by a group calling itself HFG (Taylor et al., 2014).

According to Paul Taylor, hacktivism can be seen as a modern refashioning of the original hacker ethic, which Levy describes with this set of rules (Wall, 2003):

- Access to computers should be unlimited and total.
- All information should be free.
- Mistrust Authority–Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

Taylor tried to identify the hacker generations that came before hacktivism and significantly impacted its evolution. To do that, he first pointed out Levy's three main hacker generations, which are the following:

- **"True" hackers:** These were the pioneering computer aficionados of the earliest days of computing who experimented with the capabilities of large mainframe computers at such US universities as MIT during the 1950s and 1960s.
- **Hardware hackers:** These were the computer innovators who, beginning in the 1970s, played a key role in the personal computing revolution, which served to disseminate and dramatically decentralize computer hardware widely.
- **Game hackers:** In the 1980s, these were the creators of popular gaming software applications for the hardware developed by the previous generation (Levy, 1984).

To these first generations, Taylor suggested that three more could be added (Taylor, 1999):

- **Hacker/crackers**: From the mid-1980s to the present day, these terms have been used to describe someone who illicitly breaks into other people's computer systems.
- **Microserfs:** In Douglas Coupland's novel (1995) of the same name, microserfs is the word used to describe those programmers who, while exhibiting various aspects of the hacker subculture, nevertheless became co-opted into the structure of Microsoft or any similar corporate entity.
- **Hacktivists:** The mid-1990s marked the merging of hacker activity with an overtly political stance. The previously ad hoc political targets of the fourth generation have become increasingly targeted in a much more systematic and focused manner.

Like all other internet hackers, Hacktivists can have unlimited access to cheap or free computational power and almost infinite information. **However, what** differentiates them from other hackers is that they can turn those resources toward political and not standard hacker subculture goals. Some of their tools and techniques were listed above, and they will be further detailed below based on Denning's work. However, one should keep in mind that in many cases, the normal facilities of the Internet may help hacktivists better than hacker tools, and the legality of their ways makes them one of the most accessible hacker types (Taylor et al., 2014).

10.4.3.2 Tools and Techniques

According to Denning, the four main tools and techniques in the hacktivist toolkit are:

- virtual sit-ins and blockades,
- e-email bombs,
- web hacks and computer break-ins,
- computer viruses and worms.

A virtual sit-in is *"little more than a collective, simultaneous requesting of a website. If one requests a website faster and at a more frequent rate than it can be transferred to and built up on the end user's screen, the server receives a message telling it that the first request is no longer valid and, subsequently, the new request. Scripts running on one's computer or go-between servers automate this process, and after a certain number of requests, the server under attack begins to suffer beneath the strain. One must differentiate between knocking out a server for private motives and a political action openly disrupting a web site for clearly formulated reasons and for a limited time. That is when it becomes comparable to a warning strike during wage negotiations, a means of civil disobedience signalling that one side has the willingness and courage to fight"* (Grether, 2000). The term "Distributed denial of service attacks" (DDoSA) also falls within this context and refers to the physical disruption of a network by flooding it with simultaneous requests for data from thousands of computers connected to the Internet. An example of virtual sit-ins is the 1998 coordinated series of web sit-ins by the Electronic Disturbance Theater (EDT) hacktivist group to support the Zapatistas anti-government group in Mexico. The tool mainly used in this incident is the notorious Flood Net software, which, once downloaded onto a person's computer, could automatically connect the computer to a preselected website and request that it be reloaded it every seven seconds. This action done by thousands of computers at the same time could disrupt a website's normal operation.

Email bombing has many similarities to the techniques of virtual sit-ins. The primary target of email bombs is to overload a user's email system with junk mail and thus disable it from receiving legitimate mail. Taylor states that disgruntled groups with very particular political grievances tend to use this technique and points at some examples: email bomb attacks by Tamil hackers directed at the Sri Lankan government and attacks targeting both NATO and the Yugoslav government during the Kosovo conflict by different opposing groups amongst others (Wall, 2003).

When it comes to web hacks and computer break-ins, the defacement of websites is the most common technique traced back to the World Wide Web. Redirects can also be the case here, where interception of web traffic destined for a particular site is performed, and redirection elsewhere is attained. "Humor has frequently played a part in these hacks, such as the changing of a link title in the pre-election online manifesto of the British Labour Party from *"The Road to the Manifesto"* to *"The Road to Nowhere,"* and the changing of the CIA's website so that it appeared the *"Central Stupidity Agency"* title. The hacker group, *Cult of the Dead Cow* (CDC), has sought to combine a humorous attitude with a hardened attitude to corporate power on the Internet. Successive versions of its software package *"Back Orifice"* target computers attached to Microsoft Windows network systems and allow the software's user to access other users' private files (Taylor, 1999). Some other examples of web defacement, redirect, or DDoSA are the following:

- **September 1999**: The racist Ku Klux Klan organization's website is hacked, and all its traffic is redirected to the site of antiracist group Hatewatch.
- **December 1999**: Activists established a protest site (www.seattlewto.org) to attract traffic from the official site for that year's WTO meeting (www.wtoseattle.org). Later, during the meeting itself, Electrohippies Collective launched a 400,000-strong attack on the WTO website to coincide with the street demonstration in Seattle.

- **Year 2000**: At the World Economic Forum (WEF) meeting, its website was duplicated and parodied by a Hacktivist group named *Yes Men*. The group released a software called Reamweaver, which could copy a website, allowing it to be placed on a different server. Thereby, it makes it easy for users to change its duplicate site by inserting critical and satirical content.
- **September 2001**: A French group named *The Federation of Random Action* released the *Protest Online Chat* software that allowed protestors to chat while electronically bombarding the web servers of the International Monetary Fund (IMF) and the World Bank. This coincided with the Prague meeting of the IMF.
- **January 2002**: The meeting of the WEF in New York was disrupted by a virtual sit-in involving 160,000 online protestors. EDT organized a DDoSA using its *Tactical Floodnet* software. The attack took the WEF site down for two days.
- **The Year 2004**: Yes Men *Reamweaver* software created a parody of the World Trade Organization site at the domain wtoo.org (at first sight remarkably similar to the real wto.org). Much of the content had been altered to highlight the perceived role of the WTO in contributing to global inequalities.

Taylor then proceeded to cite some other examples of web hacks of the late 1990s that showed the hackers' clear turn to more politically motivated use of their tools and techniques. "In June 1998, a hacker group from various countries called *Milw0rm* hacked the website of the Indian Atomic Research Centre and inserted their messages, complete with a mushroom cloud, to reinforce their point. In September 1998, Portuguese hackers changed several Indonesian websites to display the words *Free East Timor*. Similar attacks have also been directed on a two-way retaliatory basis between Chinese sites and the West and, in the conflict over Kosovo, between Serbia and the West. Meanwhile, in 1999, hackers from Taiwan and China conducted an online series of web hacks against each other. The Chinese government has been accused of attacking a US website devoted to the Falun Gong meditation sect, which Chinese authorities outlawed in July 1999 (Denning, 2001), while *Doctor Nuker* of the Pakistan Hacker Club defaced Indian websites in support of Kashmiri separatism. In the autumn of 2000, Israeli and Palestinian groups targeted each other's websites in support of their conflict (Taylor, 1999).

Hacktivists also use computer viruses and worms as tools. In 1988, the first widely disruptive computer worm, known as the *Internet Worm*, was propagated by Robert Morris Jnr, who ironically was the son of the chief scientist for the US National Computer Security Center. A year later a worm was used for the first time as a form of protest when anti-nuclear hackers attempted to stop the launch of a NASA probe containing nuclear materials. The "*WANK*" worm (Worms Against Nuclear Killers) was claimed to have cost NASA up to half a million dollars but failed to prevent the probe's launch. More recent examples of virus-based hacktivism include the destruction of an Iraqi government website by an Israeli hacker and attacks by Serbian hackers upon various public and private sector sites during the Kosovo conflict.

10.4.3.3 The 2014 Sony Hack

The fuzzy boundaries between hacktivism and cyberterrorism that Denning talked about in her work are no more apparent than the case of the massive 2014 Sony Entertainment Pictures hack, which took place in the last two months of 2014. The hack, as Haggard and Lindsay mentioned, "raised important questions about the feasibility of deterrence in cyberspace, the protection of First Amendment values, and the responsibility of the US government to safeguard private networks. It also resulted in a US president's unprecedented attribution of responsibility for a cyber-attack to a nation state despite public controversy over the evidence" (Haggard and Lindsay, 2015).

On November 24, 2014, Sony Pictures Entertainment (SPE) employees opened their computer screens and were greeted by a neon red skeleton from the hacker group *Guardians of Peace* (GOP), who was never heard of before and was demanding from the company to cancel the planned release of the movie *The Interview* which was a comedy about a plot to assassinate North Korean leader Kim Jong Un. This attack also deleted all the files from several of the company's hard drives. Some days later, the hackers released private Sony data into the Internet, such as unreleased films, film contracts, personal information of celebrity actors, and e-mails from senior executives, with some of them causing a great deal of embarrassment. On December 16, the GOP started making threats of attacks in theaters that were showing the movie. Attacks that have been claimed to resemble those of the 9th of September, 2001 (Haggard & Lindsay, 2015).

These terrorist threats immediately garnered the attention of US security agencies. From a criminal matter, the hack became a national security concern. Top government officials, including the director of the FBI and the President of the United States, attributed the attack to North Korea. Those allegations were met with skepticism from different sides in the cybersecurity community mainly because of the estimated technological inability of North Korea to launch such an attack and also because theories were being a "false flag" operation and an inside job by one of six disgruntled Sony employees who had the know-how and the motivation to perform such an operation while shifting the focus to North Korea (Berghel, 2015).

What gave even more rise to the theory that North Korea was behind the hack was the fact that after the FBI's and the President's public statements, GOP attacks and threats stopped. Subsequently, Sony decided to release the movie, but the threats or the release of sensitive data from the GOP did not resume. The doubts about North Korea's involvement continued for years until eventually, on September 6, 2018, the US Department of Justice issued formal charges on North Korean citizen Park Jin-Hyok, who was involved in the Sony hack. As the evidence shows, he was working as a hacker for North Korea's Reconnaissance General Bureau, the Korean equivalent to the CIA, and he was responsible, among others, for the development of a tool that was used in both the *WannaCry* ransomware attack in 2017 and the SPE hack of 2014 (Sanger & Benner, 2018).

10.4.4 Slacktivism

10.4.4.1 Overview

"Slacktivism" consists of the two words "slacker" and "activism", with the first describing a person who avoids work. Consequently, the mixture of both words is defined as a costless, token display form of support due to the "lack of real effort to enact meaningful change. (Kirstofferson et al., 2014). It gives users the impression that they "can fight wars from […] their bedroom" (Alzazeera, 2012), by liking, sharing, tweeting and reposting social or political hashtags. This form of "activism" is highly criticized by NGOs like *Unicef Sweden,* which had a campaign entitled "Likes don't save lives." According to them, being active on social media does not process a real-life change and has, as such, less use for the actual cause. "That media attention does not always translate into campaign effectiveness is only of secondary importance" (Albright, 2015). The first importance is the online self-presentation of a person who cares deeply about social and political issues. On the other hand, due to the limited signs of a tweet, Facebook, message and limited time of videos, such hashtags are often very short, and as a result, a simplification of the cause or problem they want to address. Therefore, users often do not know the whole context of what they are sharing. Liking a post and changing the profile picture to get a particular frame that shows a certain campaign can be seen as a digital form of token support.

Critics of slacktivism believe that this type of activism is worthless since it does not have any political impact outside the cyber world, and it leads to a corruption of real activism, as people will rest on digital

activism and forget offline participation processes. Traditional activism is about the people, not visual people hiding behind a screen, who appear to help face to face (Skoric, 2012).

Figure 10.2 shows the path of internet activism. The first step is raising awareness of a certain social cause on the internet. Information about that topic is shared, distributed, and liked on social media. Till now, the steps for meaningful online activism and slacktivism are the same. The last step, which is highly dependent on campaign ‘s quality and the user’s character. decides if this awareness will lead to a real-life action or token support.

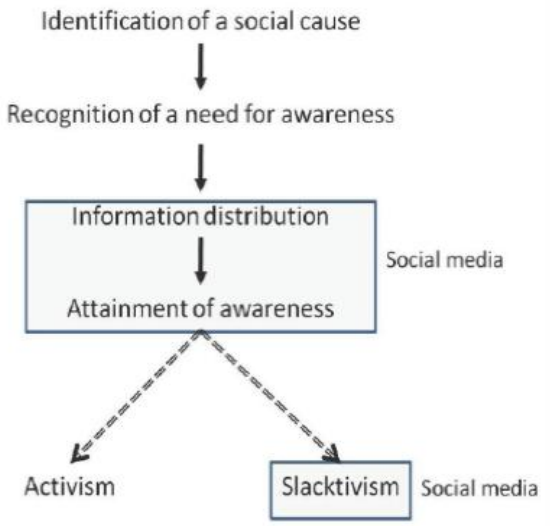


Figure 10.2 *A process diagram of social media-based activism and slacktivism.*

10.4.4.2 Types of Slacktivism

The literature points out the following types of Slacktivism:

- clicktivism,
- charity,
- political,
- sympathy.

The term "clicktivism" corresponds to forms of internet-based slacktivism, such as signing online petitions or sending form letter emails to politicians or other important persons. The procedure concerns the quick ways that social media offers to show support for an organization or cause. Clicktivism is also outlined by interpreting the success of a campaign by counting the number of "likes" it receives. It strives to quantify support, presence, and outreach without emphasizing on actual participation (Hutchins et al., 2016).

Charity slacktivism is cases like posting a Facebook status to support a cause, “liking” a charity organization’s cause on Facebook, tweeting or retweeting a charity organization’s request for support on X, signing Internet petitions, and posting and sharing YouTube videos about a cause. People may post events about a good cause or videos, and individuals donate money for this or take part in this event and give money buying something made for this cause, and the profits will be given for this purpose. The *Kony 2012* campaign that exploded briefly in social media in March 2012 is an example and will be presented in the next paragraph.

Political slacktivism corresponds to forms of slacktivism with political goals in mind, such as gaining support for a presidential campaign or signing an internet petition to influence governmental action. Another expression of this type of slacktivism is the spreading of information and events about a political fact.

Therefore, people, participate in politics, and in online discussions about political things this way (Christensen, 2011).

Finally, sympathy slacktivism can be observed on social media networks such as Facebook, where users can like pages to support a cause or show support to people in need. A popular way to do this is to change their profile pictures to show the user's peers that they care about the topic (Pappas, 2015).

10.4.4.3 The Kony 2012 Case

This campaign was conducted by the organization "Invisible Children, Inc." (referred to as IC in the following text), which was founded in 2004 to raise awareness and to stop the Lord's Resistance Army (referred to as LRA from now on) in Central Africa and to arrest the dictator *Joseph Kony*, who committed war crimes and crimes against Humanitarian Law, especially having children as soldiers. A video was released in March 2012 by IC to raise awareness of the cruelties of Joseph Kony in society all over the world. Moreover, this video aimed to put pressure on the American government and inform people about Kony and the LRA.

The aim was to have Kony arrested at the end of 2012. The video contained next to music faces of popular musicians' interviews with LRA victims, especially with a boy named Jacob. Russel promised this boy to "make Kony famous" all over the world and not to stop until Kony faced justice for his crimes. This was emotional because the viewer felt personally touched to raise awareness through the campaign for children like Jacob. Through online social networks, viewers felt that their share had an important impact on reaching the goal, and every retweet or share had significant power. It became the fastest growing viral video ever, reaching 100 million views in six days (Hebing, 2018). Nevertheless, it was the most popular among American teenagers and young adults. The goal to make Kony known was achieved due to effective slacktivism. Due to the goal of the IC's campaign, $343 million was donated to the cause. Furthermore, the United States Senate sent troops to the African Union to support soldiers as well as 50 million dollars. Nevertheless, the "Cover the Night Action" to which 3.5 million people pledged to support on Facebook (Carroll, 2012), failed due to low participation. The Ugandan government harshly criticized the video for oversimplifying the situation, despite the fact that it is among the most shared videos on social networks. At that time, Kony was not in Uganda and the government, the African Union, the neighboring countries, NGOs, and others were not taking effective action. In addition to this, the Ugandan people criticized that video for showing them as African stereotypes - still at war, helpless and poor, waiting for the "white? saviors" to solve their problems. Furthermore, the IC was criticized for selling token support symbols (like T-Shirts, Stickers, etc.), simplifying the situation in Uganda and not revealing the actual conflict. Additionally, only 35% of the donation was invested in African projects (Dorell, 2012). Some critiques were also aimed to make Kony famous and popular, like a celebrity.

The reaction and participation to this campaign demonstrate charity slacktivism due to how many viewers responded. "The video seemed to embody the slacktivist ethos: viewers oblivious to a complex foreign conflict are made heroic by watching a video, buying a bracelet, and hanging a poster. Advocates of Invisible Children's campaign protested that their desire to catch Kony was sincere, their emotional response to the film genuine—and that the sheer volume of supporters calling for the capture of Joseph Kony constituted a meaningful shift in human rights advocacy" (Kendzior, 2012).

10.5 Some Hashtag Activism Case Studies

Hashtag activism is a term that refers to the use of X's hashtags for Internet activism (Will, 2014). The term can also refer to supporting for a cause through a like, share, etc., on any social media platform, such as Facebook or X. Hashtag activism aims to share certain issues in one's social network, aiming to promote information sharing. This leads to a widespread discussion and allows for a change to occur. Therefore, hashtags can be envisaged as a way to help or start a revolution by increasing the number of supporters from

across the world who have not initially been informed about an issue by making them discuss and comment around a hashtag.

10.5.1 #MeToo

Back in 2006, a sexual harassment survivor and activist, Tanara Burke, used "Me Too" on Myspace to empower young and vulnerable women via empathy. In 2017, following the exposure of sexual abuse allegations against Harvey Weinstein, the movement spread globally through social media in the form of a hashtag. Days later, Alyssa Milano shared her idea, that if all women who have been through something similar posted a "Me too" status, people might sense the magnitude of the problem. Numerous American celebrities responded to the idea, making the movement globally known #MeToo has impacted fashion and media industries, sports, music, and education, among other areas, and now has more than 20 team members and contributors. More importantly, Burke has stated that this movement has grown to include men and women of all colors and ages. Now, #MeToo has programs on its website in which anyone can participate and contribute (Me Too Movement, 2020):

1. **Survivor Leadership Training:** Builds participants' capacities for healing and organizing, creating a space to learn organizing strategies and further develop an array of tools for the individual healing journey.
2. **Community healing circles:** Train the TrainerTrain the Trainer, a guide for moving through the complex and necessary healing process within a community of survivors.
3. **Survivor healing program:** An online series that is for and by survivors. This series introduces tools and practices to help you navigate crisis and trauma, as you rebuild a sense of safety, joy, and overall healing.
4. **HBCU Task Force:** Aims to strengthen services for survivors and to end rape culture on campus.
5. **College Program:** Campus organizing programs offer students, staff, and administrators a space to build skill and community in holding educational institutions accountable for ending sexual violence.

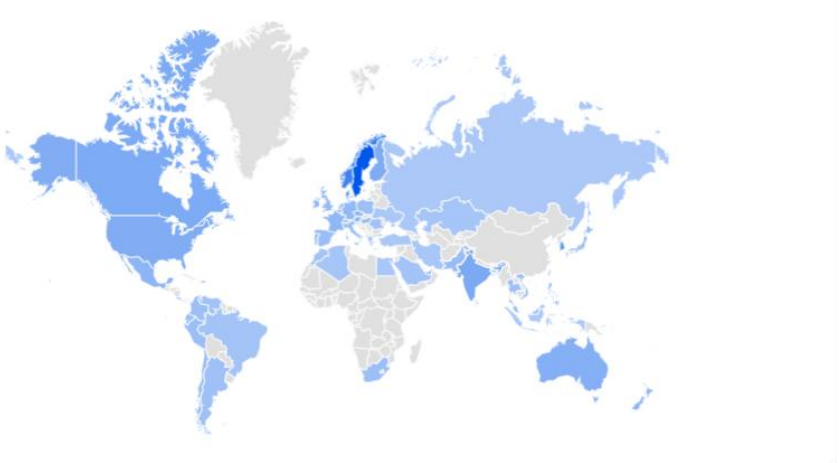


Figure 10.3 *Intensity of #MeToo searches around the world via Google Trend (May, 2020).*

In Burke's words, *"We got to work building a community of advocates determined to interrupt sexual violence wherever it happens."* The #MeToo movement has enabled the involvement of various actors, including NGOs, working with victims and stalkers, polling firms, law firms, public actors, governments, and international organizations. The role of the #MeToo movement has also led to new public initiatives and actions. As with all clicktivism cases, questions remain about the concrete consequences of this movement, i.e., its capacity to

influence and redirect the action of public authorities. However, it is indisputable that women around the world have an option to break the silence by expressing themselves, at least in the social network sphere.

In **Figure 10.3**, we can see the intensity of usage of web users worldwide. It is evident that the #MeToo movement has a massive impact on the world, and almost 85 countries have translated this hashtag into their languages.

10.5.2 #BlackLivesMatter

On July 13, 2013, a Black-centered political and social movement was founded by three black organizers, Alicia Garza, Patrisse Cullors, and Opal Tometi. This is how the #BlackLivesMatter (BLM) movement was born, which was a response to the shooting death of African-American teen Trayvon Martin seventeen months earlier, in February 2012. BLM Foundation is now a global organization in the US, UK, and Canada, aiming to eradicate white supremacy and build local power in black communities. The movement showed its principles by advocating and protesting against incidents of police brutality and all racially motivated violence against black people. The official website states that *"the call for Black lives to matter is a rallying cry for ALL Black lives striving for liberation."*

In 2014, the street demonstrations following the deaths of two African Americans, Michael Brown in Missouri and Eric Garner in New York City, were the reason that the movement became nationally recognized. On May 25, 2020, George Floyd, an African American man, was killed during an arrest by Minneapolis police officer Derek Chauvin, who knelt on Floyd's neck. The next day, protests against police brutality began in Minneapolis, and until the end of May, over 450 major protests were held all over the country. On June 5, it was announced that part of the street outside the White House had been officially renamed Black Lives Matter Plaza. There were more than 10,000 BLM protests in the US, and an estimated 15 to 26 million people participated in the 2020 BLM protests, making it one of the largest movements in US history. Due to online activism, parallel international efforts were made globally. Black Lives Matter also supports movements and causes, including LGBT+ and feminism. BLM's #WhatMatters2020 is a new campaign aiming to maximize the impact of the BLM movement. As it is published on their website, "BLM's #WhatMatters2020 will focus on issues concerning racial injustice, police brutality, criminal justice reform, Black immigration, economic injustice, LGBTQIA+ and human rights, environmental injustice, access to healthcare, access to quality education, and voting rights and suppression." (BlackLivesMatter, 2020).

10.5.3 #Occupywallstreet

Occupy Wall Street (OWS) was a socio-political, grassroots movement that began on September 17, 2011, in New York City. It was initiated by Micah White and Kalle Lasn of the Canadian" Adbusters,", an anti-consumerist, activist media organization. It was a movement against economic injustice and status quo corporatism, which controls the American political system, and a huge reliance on social media and the electronic dissemination of information characterized it. Social media tools became the winning formula of the movement's communication strategy since it would have been impossible for such a large mass of people to gather together in one place so quickly.

According to Schwartz (2011), everything started when, in early June 2011, Adbusters sent an email to their subscribers declaring that "*America needs its own Tahrir*", referring to the Egyptian revolution against President Mubarak a few months earlier, which started in Tahrir Square. On June 9, the OccupyWallStreet.org web address was created and a poster was designed by Adbusters' art department depicting a ballerina pirouetting on Wall Street's Charging Bull while behind her, a crowd of protesters was coming out of a cloud of tear gas (**Figure 10.4**).

Figure 10.4 *The Adbusters' poster for the Occupy Wall Street movement.*

The poster was shared with a tactical briefing email on X, Reddit, and Tumblr. They wanted to motivate people to bring tents and occupy Wall Street, the symbolic heart of the US financial system, on September 17. Soon, many people started registering at OccupyWallStreet.org, and the website became the movement's online headquarters. That was just the beginning. One and a half months later, on August 23, the hacktivist group Anonymous (analyzed later in this chapter) urged its followers to spread the message and participate in the protest. The main causes of the protest were wealth and income inequality, political corruption from venal politicians and labor exploitation being applied by big multinational companies (DeLuca et al., 2012). The movement's main slogan was *"We are the 99%",* expressing that almost the whole American population was financially weaker than the wealthiest 1%, making the allocation of wealth quite disproportionate. The occupiers wanted to end money's political influence, create better living conditions for most American citizens, and eliminate the fast-spreading capitalism. On September 17, an estimated 1000 people gathered in Zuccotti Park, near Wall Street (the N.Y.P.D had blocked Wall Street.) and on the same night 300 people camped and slept there. In the following days, Occupy Wall Street started to gain attention from the traditional mass media and some major newspapers, like the New York Times on September 25 and Washington Post on October 3 (DeLuca et al., 2012). Initially, the movement was buried, and media organizations showed no interest in covering it in contrast with social media, which were protesters' main weapon to be heard and recognized, especially by President Obama. A week later, NYPD began to make arrests, and several streets were overrun with more protesters. At the end of September, many labor organizations and worker unions supported the movement by holding marches, and its popularity grew massively. On October 1, the protesters decided to march across the Brooklyn Bridge and, approximately 700 arrests were made that day. In mid-October, camping sites popped up in almost every major American city, and the movement crossed over the American borders since gatherings started to happen in London, Madrid, Sidney, and Tokyo (Schwartz, 2011). On November 15, Bloomberg's office released an official statement saying that the protesters need to leave the Zuccotti Park to get it cleaned. Due to the protesters' camping there, health conditions were inappropriate for the protesters and the surrounding community. In that way, Occupy Wall Street came to an end.

Social media websites like X and Facebook intensified and incited the offline actions of the movement: they are easy, practical, and spread news quickly worldwide, so they reach broad audiences. According to the social analytics company *PeopleBrowsr*, mentions on X of OWS were already at 4.300 on the first day of protests, 9.466 on September 25, 25.148 on October 2, and 47.856 on October 14t," (DeLuca et al., 2012), i.e. almost one month after the protest had started. X has given various opportunities to participate in a movement: creating a hashtag, sharing or following it are some ways. *"A hashtag is the fundamental element of Twitter's user-generated classification system"* (Gleason, 2013) since all the X posts that contain the same hashtag are collected, and everyone can refer to them very easily. Retweets on X can lead to a huge "avalanche" of information exposed worldwide and raise people's awareness. As mentioned above, X was a crucial assistant, making a big difference in coordinating and promoting the Occupy Wall Street events. According to Penney and Dadas (2014), the protesters and generally the participants used seven methods to make Occupy Wall Street popular and provide the necessary information: e-mobilization, citizen journalism, second-hand circulation, editorial commentary, online deliberation, strengthening ties and e-tactics. E-mobilization was a method that made face-to-face protests easier. It almost replaced posters, brochures, and print-based advertisements, and that was a huge help to the arrangers since the movement was dispersed everywhere very quickly and of course at minimum cost. People who wanted to participate in the protest could find all the essential details, for example, the date and place of a march, with the click of a mouse. Citizen journalism is about the protesters who became journalists themselves with the help of their smartphones. Photographs and videos were uploaded when taken and instantly spread worldwide, allowing protesters to show the real events and the online people to watch and frame a view. The incident of a New York police officer named Anthony Bologna, who caught pepper-sprayed a young protester, was recorded in an amateur video that travelled throughout the world and exasperated many people. The second-hand circulation followed, where people took advantage of the retweeting and linking choices that X provides. That helped spread news and information to even more people and also helped those who could not participate in person take part in the process.

People have used X for one of its most common uses to express their opinions, complaints and comments in order to create an interactive network. Online deliberation is directly connected with editorial commentary. By expressing their point of view, people could also jump into conversations with others in order to exchange arguments. Strengthening ties was a method to help the activists come together. Connection via X made people of similar mindsets more united and feel more powerful. Participants of Occupy Wall Street got in touch with each other and discussed and shared their concerns.

Facebook has also played a role in the OWS movement, being an important source of information (Agarwal et al., 2014). On August 8, almost a month before the attempt to occupy Wall Street, the first Facebook page about the movement was created (Gaby &Caren, 2012). After that, hundreds of pages were established, and posts varied, informing about gatherings and marches, including pictures and videos taken by protesters, with the majority of them containing the movement's main slogan, *"We are the 99%"* or *"I belong to the 99%."* Comments under the posts fueled conversations, creating a huge political network that made Occupy Wall Street a viral object of discussion in the autumn of 2011. During spring 2012, when the movement was not as active as in September-December 2011, data were collected on Facebook using a Python script. They showed that 453 pages relevant to the movement were found. Also, 17 out of the 20 most popular Occupy Wall Street Facebook pages had a direct connection with X and corresponding pages (Agarwal et al., 2014). Facebook helped with organizing events, gatherings, discussions, and also with the approaching of members. Across-group exchanges and storytelling motivated thousands of people around the globe and pushed them to be more active in the socio-political conditions in their state or country.

10.5.4 #JeSuisCharlie

Charlie Hebdo is a French satirical newspaper created in 1970 after the revolution in May 1968 in France. The crew comprises cartoonists and journalists who make cartoons and satirical articles to make fun of everything: politics, religion, people, death, and themselves. On January 7, 2015, two men with weapons, claiming that they belonged to "*Al-Quaida*" and with the will to "*revenge the prophet*", went to the building of Charlie Hebdo during the weekly meeting and killed 12 people, cartoonists, and journalists. Fast, social networks became an important source of mobilization for all French people and soon people around the world. "*Je suis Charlie*" is a slogan and a logo created by French art director Joachim Roncin and was adopted by supporters of freedom of speech and freedom of the press after this incident. It was first used on X and became one of the most popular news hashtags in X history (Goldman & Pagliery, 2015). *Je Suis Charlie* was adopted worldwide, was used in music, displayed in print and animated cartoons (including The Simpsons), and became the new name of a town square in France.

10.5.5 #ClimateChange

On September 25, 2020, thousands of climate strikes took place across the globe to demand urgent action to tackle the climate crisis. This climate strike was held for one week with a great number of participants from all over the world. The environmental issue was projected in the social media sphere, specifically via X under the *#climatechange* hashtag. In this vast global climate protest, 7.5 million people demanded to protect the environment and sent a significant message to the government and politicians of all countries. It is important to note that Italy, Germany, Canada, and USA had the most protesters. In Canada, almost 500,000 strikers, mobilized by the *#climatestrike* via X and based on a X post of the account of *@dotorg*, gave an important message to all people of all ages and politicians of the world, in order to unite and find useful solutions to save our planet. The power of this movement caused the intervention of the United Nations and many politicians who gathered in New York to discuss the emergency of this global topic and confront the climate crisis. Moreover, many famous people, such as reporters, politicians, actors, or eco-activists sent a significant meaning for the environmental protection via their personal accounts on X which caused many views, likes, retweets etc., and of course mobilized millions of people. The impact of this international phenomenon was huge, owing to the coordination based on social media via the *#climatechange*.

10.6 The Case of the Anonymous

10.6.1 Overview

Anonymous is an international network of activists and hackers that emerged in 2003 but became widely known in 2008 with their *"Chanology Project",* which targeted the Church of Scientology. Throughout the years, they gained international fame and admiration. The main reason why people like them so much is reflected in the way they portray themselves: *"People donning Guy Fawkes masks (Figure 10.5) and taking down the government and non-government agencies are sure to attract some attention" (*Raza, 2016). Some picture them as superheroes who reveal the truth behind incidents or politicians, but the truth is that their main goals are to fight for freedom on the internet and combat censorship.

Figure 10.5 *The Guy Fawkes mask, symbol of the Anonymous hacktivists' group.*

Anonymous is an unprecedented political and social phenomenon that amazed the world with vigor and power. Despite its media prevalence, the nature and function of the group remain ambiguous to the public. Playful insurgence, black humor (or lulz as they call it), and devilish offenses for the sole thrill of being naughty were the foundations of what grew to be the famous social movement that took over the media all around the world. Indeed, before the attack against the Church of Scientology in January 2008, Anonymous was little more than that. *"Chantology Project"* was launched in reaction to the attempts of the Church of Scientology to censor a video of Tom Cruise. The means employed ranged from excessive trolling, such as sending unpaid pizzas or faxing pictures of nude body parts or black pages to churches of Scientology, to more serious and illegal offenses, such as Denial of Service attacks (DDoS), towards Scientology websites.

As mentioned earlier, *Project Chanology* was not the first politically charged coordinated trolling of Anonymous. What is unique about it and marks it as the starting point of this hacktivists group is that, unlike previous attempts at coordinated action, the political aim remained relevant for years and established a tradition of political activism (Chen, 2010). The 10th of February in the same year symbolized that transition when over 7,000 Anons (persons involved in the Anonymous movement) in Guy Fawkes masks flooded the streets in 127 cities worldwide (Coleman, 2014). Though the protest was within the scope of Project Chanology, its most significant impact was not on the Church, but on Anonymous itself. In fact, one could go as far as to say that Project Chanology was just the necessary kindle on which the fire took off, the excuse for the revolution to happen. Anonymous had caught the world's attention, and more importantly, Anons became aware of a sense of solidarity, a collective power within the community. Those elements fostered political action ambitions, making activism, or hacktivism a central component of the Anon subculture.

However, it was not until two years later that Anonymous showed its true potential by retaliating to the refusal of Amazon, PayPal, MasterCard, and other companies to provide banking services to WikiLeaks. The successful weapon was DDoS attacks aimed at the companies' websites. Infatuated by their success, Anons began to organize a multitude of Operations over the following years, establishing Anonymous as an actor, a sui generis unprecedented actor, whose nature few could comprehend and whose potential no one could estimate.

However, although everyone knows of the entity coining the moniker "Anonymous" and sporting the Guy Fawkes mask, most do not have a clear idea of what exactly it is, how it operates and for what ends. Anonymous is often vaguely perceived as an organization or group of highly skilled hackers secretly operating to achieve mutually agreed-upon goals (Chen, 2010). They have a very loose and decentralized command structure; they do not have leaders and they act on ideas. Anonymous can speak best for itself: *"Anonymous is not a group, but rather an internet gathering which operates on ideas, rather than directives. We are average internet citizens in ourselves, and our motivation is our sense of being fed up with all the minor and major injustices we witness every day."*

Anonymeasy identify with any specific nation or system of governance. Becoming a member of Anonymousis relatively easy, as it is open and anyone who desires to join is welcome. However, people have been arrested because of their involvement in the group in several countries, including the United States, the United Kingdom, Australia, the Netherlands, Spain, and Turkey. The first person who was sentenced to go to jail was a 19-year-old American named Dimitriy Guzner.

10.6.2 Most Famous Attacks Done by Anonymous

The most famous attacks conducted by the Anonymous are listed below:

Habbo Hotel

The first attack listed in the group's timeline of events is associated with the Habbo (Habbo Hotel), a cartoonish social networking site and online community to which teenagers between the ages of 13 and 18 were attracted. In 2006, it was being discussed on 4chan boards that the hotels' moderators were being racist by banning players with darker-skinned avatars. As a result, Anonymous users signed up to the site with dark-skinned avatars with an afro hairstyle and blocked entry to the pool, saying that it was "closed due to AIDS."

No cussing club

A teenager named McKay Hatch started a website called *"No Cussing Club,"* whose main goal was to prevent foul language and profanity. McKay Hatch was targeted after Anonymous was informed about the site owner, his home address, and his phone number. Then, in order to harass him and his family, pornographic material was sent to his home, weird phone calls were made, and unwanted pizzas were delivered.

UC Davis pepper spray incident

During a demonstration at the University of California, Davis, in 2011, protesters refused to leave and remained seated at the University without making any active resistance. They were then sprayed pepper by the university police officer Lt. John Pike. Journalists attending the demonstration captured a video and pictures that were spread worldwide. Police Officer John Pike was to be punished while remaining on duty. Anonymous got involved and released personal information about him, believing that the officer's action was not compliant with the freedom of speech. He was eventually fired.

2009 Iranian Presidential election

After it was made known that the votes of the election had been alternated, The Pirate Bay, Anonymous Iran, and other hackers from Iran came together and built a website for supporting the protesters in Iran to supply them with resources and allow for the exchange of information between Iran and the rest of the world. Anonymous also published a short video on Iran and released a message to the Iranian government, manifestos in which Anonymous declared its reasons for supporting the protests.

Dark discovery

In October 2011, Anonymous focused on destroying child pornography sites, including the prominent site called *Lolita City*. According to Hqanon, "*After a series of DDoS attacks, 1,589 names of Lolita City users were eventually released to the public, including their username, volume of images uploaded, and age of the account. Interpol and the Federal Bureau of Investigation were invited to investigate further records and conduct follow-ups."* (Hqanon, 2016).

Operation Charlie Hebdo

As a response to the shooting in the satirical newspaper *Charlie Hebdo* conducted on January 7, 2015, Anonymous offered condolences to the families of the victims. They also referred to the shooting as an

inhuman assault to destroy freedom of expression. As for revenge, they targeted and shut down many Jihadist and Islamic websites, and social media accounts, and they addressed a message to al-Qaeda, the Islamic State, and other terrorists: “We are declaring war against you, the terrorists" (Wikipedia, 2017).

Operation Ice ISIS

After the terrorist attack in Paris on November 14, a minor task-hacking force called *Ghost Security* was created to fight ISIS in the digital sphere. Their goal was to take down ISIS supporters’ accounts on social media such as X and to reveal the account holders’ real identities. The group attacked the ISIS internet-based recruitment drives and wiped out a lot of data of new ISIS fighters. After this, Anonymous released a statement on YouTube with a threat towards ISIS, saying: “ISIS, We will hunt you, Take down your sites, accounts, emails, and expose you. From now on, [there is] no safe place for you online… You will be treated like a virus, and we are the cure… We own the internet… We are Anonymous; we are Legion; we do not forgive, or, Expect us.”

Operation Darknet Relaunch

On February 3, 2016, Anonymous gained access to data from the host servers of the website *Freedom Hosting II*, a significant server supplier for the Deep Dark Web, the “underground” network many illegal activities occur (see **Chapter 11**).

10.7 The Case of *Wikileaks*

10.7.1 Overview

The case of WikiLeaks is another well-known example of hacktivism nowadays. It is not based on a massive mobilization but on the actions of some individuals who rebel against their institutions. On simple logic, the model is based on three steps: divulgating, releasing, and expecting the scandal to force political changes. WikiLeaks wants to raise awareness among the public in the hopes that a significant social movement will result in these kinds of disclosures. This logic is not new, this same procedure was used to divulge the "Pentagon-Papers," revealed in 1971 under the initiative of S. Elseng’s, a former employee of the US Defense Department.

The website *WikiLeaks* was founded in 2006 by a computer programmer, journalist, and publisher named Julian Paul Hawkins, also known as Julian Assange, who was born on July 3, 1971, in Townsville, Queensland, Australia. He lived in many places during childhood and was often on the move with his mother, Christine Ann Hawkins. His mother had separated from Julian’s biological father (John Shipton, who was an anti-war activist) before he was born. When he was one year old, she married his stepfather, Richard Brett Assange, who used to work as an actor and whom she also had a theatre company with. As a result of Assange’s roaming upbringing, he was forced to attend 37 different schools, and he later studied programming, math, and physics at Central Queensland University and the University of Melbourne, never receiving a degree from his studies.

At the age of 16, Assange started hacking with two friends and formed a small hacking group named *“International Subversives.”* Throughout this period, he gained access to the Pentagon, a few other US Department of Defense divisions, the US Navy and NASA, and many other targets that could have held valuable information. Eventually, Assange got caught, and his home was raided in December 1996 by the Australian Federal Police, who tracked his internet activity. The police eventually noticed when he hacked into the company *“Nortel,”* a big Canadian telecom corporation. After his arrest, he was released on a good behavior bond but had to pay 2,100 Australian Dollars for the damages he caused to the website. He pleaded guilty to 25 of the 31 charges pressed against him, while the remaining five were discarded (Lagan, 2010).

10.7.2 The Site Wikileaks.org

Julian Assange's site, WikiLeaks.org, became a highly mentioned website in the year 2010 when it released footage from the Department of Defense of an Apache helicopter that shot down a group of journalists who were carrying cameras but were mistaken for armed men during the Afghanistan war of 2007. To be able to confirm what happened, *WikiLeaks* sent a team of journalists to get a hold of hospital records and obtain death certificates, amongst other things.

The footage of the different leaks comes from anonymous sources, also known as whistleblowers, who upload their findings to the *WikiLeaks* servers located in Sweden. WikiLeaks claims that it wants to reveal unethical behavior within governments and corporations, and also wants everyone to have free access to information that could be of public interest. WikiLeaks argues that it wants the readers to be able to make up their own minds about what the actual truth is. *WikiLeaks* has been awarded the *Economist New Media Award 2008 and the 2009 New Media Amnesty International human rights reporting award* for its action.

10.7.3 Famous Leaks

Some of the most famous leaks are listed below:

The Guantanamo Bay Files Leak

The Guantanamo Bay files were published on April 25th, 2011. A total of 779 confidential records pertaining to detainees held at the United States-operated Guantanamo Bay detention facility were made accessible to the public. These documents contained many assessments, interviews, and personal information about detainees. Upon closer examination of these documents, it was discovered that over 150 people were detained for years at Guantanamo Bay without clear justification. According to *Wikipedia*, 2017, *"Documents also reveal that some of the prison's youngest and oldest detainees, who include Mohammed Sadiq, an 89-year-old man, and Naqib Ullah, a 14-year-old boy, suffered from fragile mental and physical conditions."*

Secret Bibles of Scientology

On March 24, 2008, *WikiLeaks* published a collection of the *"Secret Bibles of Scientology"* which explained the whole hierarchy within Scientology. The Church of Scientology started threatening *WikiLeaks* to take the information down few days after publication, which they refused (Chivers, 2017).

The Iraq War Logs

In 2010, Julian Assange shared more than 391,830 classified documents of the US military with famous newspapers, including *The New York Times*, *The Guardian,* and *Der Spiegel*. They were all related to the war of the United States with Iraq. This has been referred to as the biggest leak in military history (Marchal, 2016).

Kaupthing Banks Businesses/Deals

The Icelandic bank's secret documents were published by WikiLeaks in September 2009, which revealed that the owners had done some shady deals before the bank was closed due to bankruptcy; they had purposely lent to other companies, which they owned before the bankruptcy occurred, and, therefore, large debts had vanished.

CIA Hacking Tools

The CIA was deprived of most of its hacking tools which contained viruses, malware, Trojans, weaponized malware, and other remote-control systems. *Wikipedia* claims that *"there were several hundred million lines of code",* which is now in the hands of third parties, giving them the entire hacking capacity of the CIA. One of the hackers who now possess the codes is the whistleblower who notified WikiLeaks about these documents.

The malware programs were used to gain access to many company products like Apple's iPhones, Google's Android, Microsoft's Windows, and Samsung TVs, which were used as covert microphones.

Afghanistan War Logs

Close to 92,000 documents from the Afghanistan war have been published covering US activities from January 2004 to December 2009.

Tunisian Governmental Documents

Documents revealing extensive corruption in Tunisia are considered to be one of several causes behind the Jasmine revolution and the Arab Spring, which is analyzed in the next paragraph, as it involved many peaceful and violent protest, and it spread to other dictatorships rapidly.

All of the footage has been spread worldwide and the website retrieves confidential information from governments and corporations to publish it. *WikiLeaks* claims it has released more classified information than the entire world press combined.

10.8 The Arab Spring

10.8.1 Historical Overview

Born in Tunisia at the end of 2010, the Arab Spring was a protest movement that quickly spread to other MENA (Middle East and North Africa) countries by the spring of 2011. Social media played an unprecedented role in these mobilizations—one of the most significant in human history. Therefore, it is imperative for it to be presented and analyzed thoroughly.

In the MENA countries, the populations were protesting against poverty, unemployment, tyranny, and the corruption of authoritarian governments that have been in power for decades. In Tunisia, the movement was called *"The Jasmine Revolution"* and forced the President Zine el-Abidine Ben Ali to leave the country. In Egypt, the President Hosni Mubarak was set out of power. The revolution has led to free elections in both countries. In Libya, the rebellion against Colonel Muammar al-Kaddafi ended up in a civil war in which the NATO forces were involved. At the beginning of 2011, the Tunisian and Egyptian revolutions encouraged other populations, like Yemen, Bahrain, and Syria, to protest against their governments. Ali Abdallah Saleh, president of Yemen agreed to quit in November. In Syria, the procedures have led to a civil war in which many countries have been involved: France, Russia, Turkey, the USA, the UK, and Jordan. In Algeria, Jordan, Saudi Arabia, Oman, and Morocco the governments responded to the population's demands and made many reforms.

This revolution has gradually spread to many other countries in the Arab world, with a different outcome (Κουσκουβέλης et al., 2012). For example, in Libya and Syria, the response was violent repression with the risk of civil war. Therefore, 2011 was marked by this wave of popular protest, which had a "domino effect," as it was supported and encouraged by activists in other countries. Massively using digital media, cell phones, and satellite television characterized the Arab Spring protests. Moreover, the decisive use of social media for the dissemination of ideas, organization of events and coordination during the Arab Spring revolts has led to its being named *"revolution 2.0."* This was the first time in history that a tweet, a video on YouTube, or a comment on Facebook proved their potential in easily creating the "buzz," a social movement, and finally, a whole revolution with results like the downfall of the regimes of Ben Ali or Mubarak. Social networks have allowed the whole world to access information uncensored by political regimes and revolutionaries to feel united in their cause. Furthermore, during these revolutions, the number of users and connected people in the MENA countries increased significantly. Indeed, five million Egyptians had a Facebook account during this period, five times more than two years ago. Also, in the week before the fall of the government of Hosni

Mubarak (President of the Arab Republic of Egypt from 1981 to 2011), the number of tweeters on this subject rose from 230 to 230,000 per day.

In a broader sense, this revolution *"differs from historical ones, because this time the demonstrators had farther and more efficient ways to express their displeasure, such as social networks"* (Σταματόπουλος, 2016).

10.8.1.1 The Case of Tunisia (the Jasmine Revolution)

In Tunisia, it all started on December 17, 2010, when Mohamed Bouazizi, a young graduate and unemployed, set himself on fire in Sidi Bouzid. This event would not have attracted as much attention if it had not been filmed by passers-by and posted on social media, more precisely on Facebook. In most MENA countries, the press is under surveillance and censorship; therefore, it is difficult for people to express their political opinions and ideas. The Internet, back then, proved to be a new, powerful means of expression and communication that had been little known. Indeed, the revolutionaries demonstrated in the streets while having on their screens broadcast videos of other ongoing demonstrations and the capability of organizing new ones and spreading slogans and ideas. The government tried to stop this diffusion as quickly as possible by imprisoning Internet users, but the spread via social networks was far too fast and impossible to stop.

Initially, the protestors' requests were of a social: stopping police violence, reducing unemployment among young people, reducing the prices of food, increasing the minimum wage, fighting widespread corruption, as well as improving life conditions. However, they soon became political, eliminating the late autocratic president's regime, democracy, and freedom of speech.

The protests represented Tunisia's strongest wave of social and political unrest for three decades. They led to the escape of President Zine Al-Abidine Ben Ali, who was retiring after twenty-three years in power and left Tunisia on January 14, 2011. After the escape of Ben Ali, an interim government was formed, including members of his party (Democratic Constitutional Rally, RCD) in some ministries, and members of the opposition. The government was valid until the new elections, 60 days after the reformation. However, five opposition government ministers left almost immediately. Since January 21, 2011, daily street protests in Tunis and other cities have continued the request towards the new government not to include ministers from Ben Ali's party and the party itself to be disbanded. The uprising took over 220 casualties and 94 injured. On February 6, RCD was dissolved.

The protests and the government shift are known in Tunisia as the Tunisian Revolution of Dignity, while in the Western media, these events are usually referred to as the Jasmine Revolution or the *Web Revolution 2.0*.

The Tunisian people had received significant support from the hackers of the *Anonymous* group, which launched computer attacks against official Tunisian government websites. The government tried to react by mobilizing staff from the Tunisian Internet Agency, which censored and blocked access to sites opposed to the government, such as *WikiLeaks* published documents revealing corruption, and a real virtual war broke out.

10.8.1.2 The Case of Egypt

The revolt in Egypt started in June 2010 after the murder of a young businessman, Khaled Mohamed Saeed, by the police, which exasperated the Egyptians. The official cause of death was that he swallowed a bag of drugs, but photos of his beaten-up body uncovered the truth that police beatings killed him. As a result, online mobilization took place via a Facebook group against police violence, which soon turned into an offline one. Cairo's Tahrir Square brought together ten thousand Egyptians demanding that their president, Hosni Mubarak, step down. The slogan *"We are all Khaled Said"* became a trend and can be considered a prelude to the revolution that followed. Facebook was the dominant social media platform in Egypt with 7 million users,

mainly used to tackle police brutality. The protesters used Facebook groups to organize and get informed on the places and times that they would gather, as well as to share photos of violent incidents that were caused by the authorities. However, the *"Dubai School of Government, 201"* says that X had a better role in organizing people on site, through its interface capabilities, even though its users were only around 130,000.

The government took swift action to survive, attacking the Information and Communication Technologies at its heart, shutting down the entire internet for five days. This action alone proves the significance of the Internet during periods of crisis and civil unrest. With the internet being off the game, the government managed to stop the pre-protest organizing via Facebook and the offline coordination that X would provide. It was not for long, but five days seemed a lot for the people of Egypt at that time, and it could indeed be a decisive factor in saving Hosni Mubarak's position. However, protesters operated blindly for a while, forcing President Mubarak to resign after 30 years of authority, 18 days after the beginning of the continuous protests, not without casualties, that were sparked from a Facebook page.

Usually, telecommunication companies have little power in environments of authoritarian regimes, but in the case of Egypt, Vodafone and Orange (among the providers involved) took action to prevent shutdowns from happening again. They helped create an organization called *"Telecommunications Industry Dialogue"* which promotes freedom of expression and privacy.

10.8.1.3 The Case of Bahrain

In Bahrain, people were getting information and news from sites like *Al Jazeera,* which were organized via Facebook and journalists' blogs, with the highlight of their protest taking place in a historic gathering on the Pearl roundabout. However, the country's leadership had declared martial law and was trying to control the situation in total, even though it was clear that most of the people were united in trying to topple the regime. King Khaliah (Hamad bin Isa Al Khaliah) communicated a message on national television that distorted the facts heavily. He talked about Sunni and Shia forces fighting each other in the streets while the demonstration was clearly being conducted by united Sunni and Shia populations against his tyrannical rule.

A considerable percentage of the Bahraini people who were not taking part in the demonstrations (mainly because they were afraid to do so), were informed via social media about the true causes of the uprisings, as well as about the actual number of the people that suffered or lost their lives under Khalilah's rule. The Salmaniya hospital was the main treatment hub for the injured at the Pearl roundabout rallies and it was labelled as the *"base of the insurgents"* by the government. In reality, sites like *Al Jazeera* showed that the Salmaniya hospital workers would work tirelessly, even for 48 hours straight at the time, to treat victims of the protests regardless of which side they served. That included even Syrian and Pakistani mercenaries, who were rushed to Bahrain to help control the revolt and were never mentioned in the government broadcasts. As the situation in Bahrain was reaching its peak, and the king was forced to employ thousands of foreign soldiers to maintain his position, the regime cut the signal of the phones of the protesters. It evacuated Pearl's roundabout and ended the people's dream of democracy. With the signal being off, people could not broadcast to the rest of the world or to Bahrain itself, the mass arrests that happened violently in Shia villages and the taking of Salmaniya hospital where even patients were being attacked.

Ending the uprising was not enough for Khalilah's regime. They took upon a manhunt of prominent figures and activists via Facebook, creating pages like *"Together to unmask the Shia traitors,"* using photos of the uprising that were once used to celebrate and motivate to track down the frontrunners. They called people to write the pictured person's address and workplace and let the government handle the rest. This was basically a virtual lynch mob, providing vital information to state agencies, based on photos of people who were simply attending the Pearl roundabout events. It was efficient, as it led to many arrests and

imprisonments, as well as online shaming by the public, with countless degrading comments under these posts.

10.8.2 An Analysis of the Role of Social Media in the Arab Spring

From what has been stated above, it is clear that the Internet and social media played an essential role in Arab uprisings. To begin with, these technologies have entered the lives of MENA countries in recent years, and in 2010 specifically, Internet use steeply increased, with 40-45 million users identified in 16 Arab countries. Contrary to countries in Western Europe, social media use increased rapidly and the fact that ruling elites feared social media gave the Arabs the chance to explore a new digital world. Verily, many people quickly started to express their point of view and blamed the state for their poverty. Consequently, a complex relationship between media and governments was developed, with the second wanting to penetrate and control the information. States banned some websites, but the disenfranchised youth found another path to participate in the public and political spheres. In that way, Facebook, X, and YouTube activists took the situation into their own hands (Storck, 2011). Locals started utilizing social media to organize protests while using them to directly inform more and more people about what was happening there and raise awareness.

In Tunisia, Bouzouazi's self-immolation was the excuse for Arab people to revolt against the long-time oppression. When spontaneous uprisings flared, state media did not project them much. At the same time, the Tunisian internet censorship filter blocked large amounts of internet content, like YouTube. For that reason, Facebook (which until then was not blocked) got engaged to inform people about demonstrations. By mid-January, 18% of the country's blog posts referenced the uprising and the political developments there, while 10% talked about liberty. The third week of that month was the peak of the mass demonstrations, with estimates of even 100.000 people protesting in the streets. It is also remarkable that 90% of Egyptians and Tunisians participating in a survey declared that they used Facebook in order to organize protests or spread relevant pieces of information. Even X, which was not popular among Tunisians, played a significant role in information dissemination during that time (Comninos, 2011). *#sidibouzid* was a famous hashtag connected to the revolution in Tunisia, featured in 13,262 tweets. X was mainly used as a means of international information dissemination about the uprisings in Tunisia—according to a survey from January 14 to March 16, 2011—18% of the Tweets about the revolution originated in Tunisia, 8% in bordering countries, and 32% elsewhere (there was no information about the rest of the tweets). The consecutive civil disorder ended with the fall of President Zine El Abidine Ben Ali on January 15, 2011. Furthermore, the situation in Tunisia became widely known through social media, and many countries were affected by the power of that mass of people. As a result, a mass Arab movement began (Howard et al., 2015).

The situation in Tunisia directly influenced Egyptians, who had protested many times during the previous decade and were also experiencing a big expansion in Internet use. Many pages and tweets were created to motivate people, along with e-mails and conventional means like word of mouth and photocopied flyers. One of these pages, created by Wael Ghonim in Facebook and called "We are all Khaled Said" referred to a young man who was hit repeatedly until death by police in Alexandria, as described in the previous paragraph. The page was quickly followed by 500.000 members and soon became a platform to discuss online and share grievances against the Mubarak regime. Wael was working for MENA's Google as marketing director in 2008. He created this page to engage Egyptians in political activism, and it played a crucial role in proposing antigovernment protests, calling for people to join them. He returned to Egypt to fight together with the rest of the people, but his track was lost during the protests. Finally, the government released him after 11 days in prison with no information about his situation. (Μελιτά, 2011). Meanwhile, Egypt's government initially decided to block Facebook and X and cut off Internet use on January 28, an action that proved the threat it felt from internet activism. That move not only failed to calm down the activists, but it actually triggered an even better collaboration among them. Mass protests in the country's biggest cities caused the dissolution of

the government and forced Mubarak to appoint his first vice-president after nearly three decades. Moreover, when the government blocked cell-phones, people seemingly switched to a more traditional form of communication—word of mouth. For example, activists planning the demonstrations in Cairo spread the word via taxi drivers. Also, many activists achieved to find proxies and get online again, while others carried their updates to friends outside of the country to publish them (Μελιτά, 2013).

The uprising in Bahrain was also strongly affected by internet use. Bahrain is a country in which internet users reach 88% of the population (the biggest percentage in Arab countries, bigger than even countries like the USA). So, when revolutions started in the Arab world, Bahrain's activists immediately tried to organize big protests through social media, e-mails, forums, and text messages, demanding better living conditions, employment, and freedom of expression. What is remarkable in Bahrain's case is that the government tried and managed to use the internet for itself. First, they banned websites (as happened in other countries) and arrested bloggers. However, they also went one step ahead and used social media to identify faces of people who had participated in the protests. Indeed, an X account called *Haraqhum* which published the faces, names, and many personal details of anti-government protesters. For that reason, many people were victimized, lost their job, and were even afraid for their lives. As a result of all these actions, more and more people stopped using social media, and combined with internet filtering, internet traffic dropped by 20%.

On the other side, internet access and social media presence in Yemen and Libya were limited, so their impact on the uprisings and the following wars was relatively low. In Libya, people tried to post their opinions against the regime and call for action, but soon Gaddafi blocked internet traffic. That explains why the country was the exception to the rule that saw social media use in the Arab world rising more than 100% during the uprisings. However, cell phones, emails, and videos were used to raise awareness outside of the country, as there was very little coverage of what was happening by the traditional media, and Libyans, who had participated in interviews declaring their views against the government, were arrested.

In Syria, again at the beginning of 2011, social media became the field where protests were being announced and citizens demanded respect for human rights and liberties and an end to the state of emergency imposed on the country. A Facebook page called *"The Syrian Revolution 2011"* played a prominent role in the uprisings. Almost 50,000 people would use the page to discuss the situation in Syria daily, while its members reached 343,637. They were young Syrian activists from all the provinces trying to achieve the revolution's objectives f and gain freedom. Fighting for the overthrow of Assad, they wanted to establish a democratic policy that would host all Syrians with nondiscrimination. Videos and photos were uploaded every day and described the demonstrations that were happening at the time. It is also interesting that the religious part was also intense in the comments of X users during uprisings in Syria since they called on God Allah regularly. Just like Bahrain's case, Assad's regime also used the internet to confront his political opposition, as the *Syrian Electronic Army*, a still active group of hacktivists, was established in the same year. (Shehabi & Jones, 2015)

In contrast to other countries, Internet activists in Jordan did not mobilize many people in the protests, but they managed to create a safe place for discussion. The X hashtag *#reformjo* was created by a Jordan blogger and accumulated many activists, professionals, politicians, and active citizens. The hashtags allowed people to express their ideas, discuss freedom, and talk about other "taboo topics." The civil resistance, however, was limited to online debates, making many people wonder whether online activism reduces offline political actions and the number of offline activists.

10.8.2.1 The Role of Facebook

Before the uprisings, there were 3,294,000 Facebook users in Tunisia out of a total population of 10,732,900, which means that from 85 out of 100 people who have access to the Internet, 31 were registered on Facebook. On the other hand, in Egypt, there were 12,134,660 Facebook members out of a total population of

83,688,164, ranking 20th in the world. These statistics show that this social network was used by 15% of the country's population, while only 55% had access to the Internet at that time. During the uprising, Egypt and Tunisia experienced a significant increase (Egypt +1,951,690, Tunisia +535,640) from January to March 2011 in the number of Facebook users, according to the Arab social media report. In Tunisia's Facebook, 31% of the population was registered, compared to only 15% in Egypt and Morocco.

Moreover, the 18–24-year-old group is the age group to which most users in all Arabic countries belonged, followed by the 25-34 age group, so the population mobilized by these revolutions was relatively young. It should be noted that in this region of the world, young people aged 25 and under are almost half of the population. These Arab countries have a very high unemployment rate for young graduates, which contributes to the feeling of indignation in the middle class and poor population. According to many international organizations, such a very strong element could trigger social revolts. It should also be noted that most social media users who have risen were young and were mobilized due to excessive unemployment, their need for entertainment, their quest for freedom and free expression, and their desire to be involved in the political, social, economic, and technological fields. Young people, therefore, constituted a significant part of the population that were digitally literate, which was a tool that allowed them to impose their ambitions despite their governments' attempts to silence and ignore them. These young people have come together and founded Facebook pages. A community of young, committed Arabs was created to try to change their future. According to Farah Hached, a lawyer in charge of the Tunisian association, "*Facebook has played a fundamental role in linking the different social groups (...) people who were not aware of the information, and who did not exchange it, began to know what was going on and the extent of it.*"

10.8.2.2 The Role of X

X derives its way of functioning from the blog principle, which allows you to publish short messages, sometimes accompanied by images or videos. This way of operation allows you to tell what you are doing the moment you are doing it. It allows information and links to be exchanged and differs from other media by its simplicity of use, which is one of the main factors of its success. The hashtag "#" principle makes it possible to assign a subject to the tweet and thus r target everyone's interests better. For example, the X hashtag *#jan25,* about the January 25, 2011 demonstration, which marked the beginning of the Egyptian revolution, circulated widely on social networks. Several weeks after Ben Ali left for Saudi Arabia, the hashtag *#sidibouzid* (the city where protests began after Mohamed Bouazizi's immolation) continues to be supplied by users, as well as *#Tunisia,* which was the hashtag for monitoring events. In the case of Egypt, the corresponding hashtags were *#Egypt* and *#Mubarak*. The profile with the most followers was Mohamed ElBaradei *(@ElBaradei*) with more than 1,162,765 followers worldwide. His commitment during the Egyptian protests was much appreciated while he actively supported the demonstrators and was even designated as spokesman to negotiate with Hosni Mubarak. There were 300,000 X accounts in Egypt in 2011, according to the Arab Social Report. In Tunisia, the most monitored account of ShemsFm *(@RadioShemsFm*), with 24,676 subscribers, which followed the country's demonstrations in real time and regularly posted videos of the protesters online. In Tunisia, there were also just over 10,000 X accounts in 2011 according to the Arab Social Report.

Although the Egyptian population is much larger than that of Tunisia or Libya, Internet use was more intense in Tunisia, where 51% of the population had access to it, while only 35% in Egypt. This can be partially explained by Internet surveillance and excessive repressive censorship by the government. However, in Morocco, the state had adopted a relatively liberal policy regarding access to foreign sites, and there were relatively few cases of censorship. Paradoxically, the country had lower Internet access rates than in Libya. This was because there was no ongoing revolution there, so coordination and information sharing were not as imperative as in Egypt, Tunisia and Libya, for example.

Although X was a social media platform with a few user accounts in these countries, its role is evaluated as highly crucial in making one's voice heard worldwide.

10.8.2.3 The Blogosphere

The political blogosphere has provided fertile terrain for the reproduction of political discourse (Adamic & Glance, 2005). More specifically, blogs tend to form clusters where, among others, similar topics of interest are discussed (Vagianos & Zafeiropoulos, 2020).

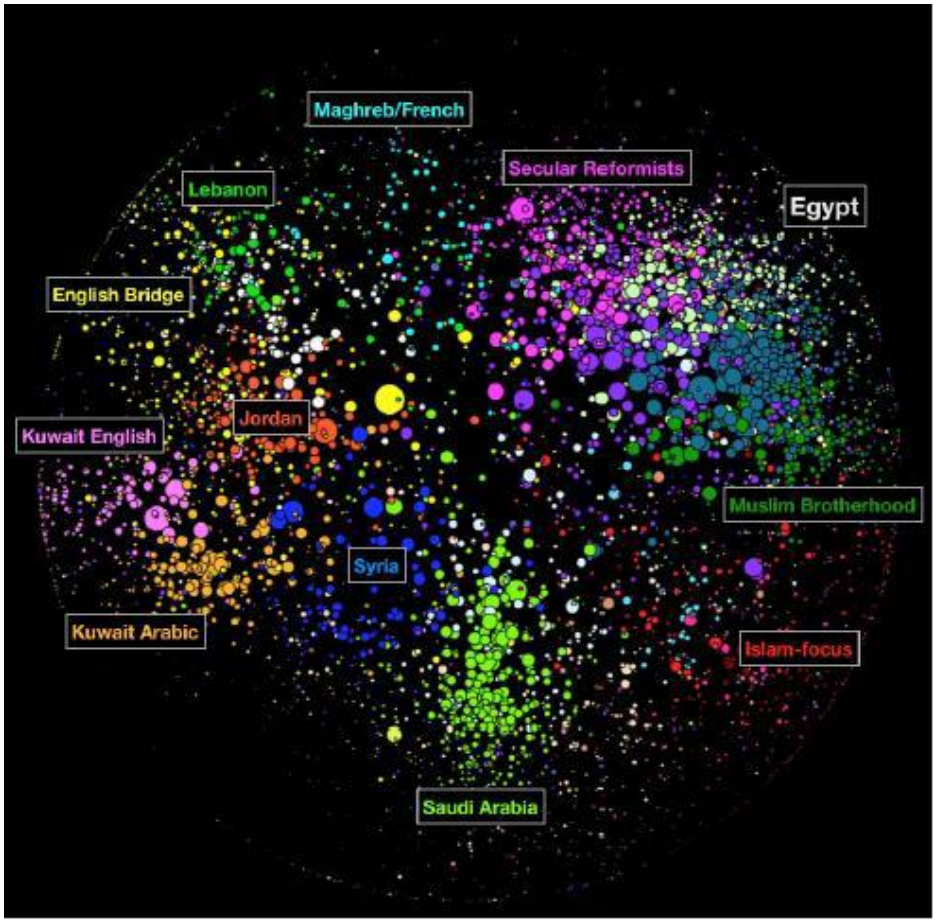


Figure 10.6 *Map of the Arabic Blogosphere (Etling, 2009).*

At Harvard University, Bruce Etling, John Kelly, Robert Faris, and John Palfrey did an extensive case study about the impact of Arabic bloggers before the revolution. The title of their study was *"Mapping the Arabic Blogosphere: Politics, Culture, and Dissent."* According to this investigation, Egypt was by far the largest cluster of blogs. It included several distinct subclusters, one characterized by secular reformist bloggers, and another by Muslim Brotherhood members, a group that is technically illegal in Egypt but whose online presence appears to be tolerated (Etling, 2009).

Interestingly, the Muslim Brotherhood, a political movement in the Arabic sphere since 1920, is a big part of the Egyptian blogosphere. Their leader became, in 2012, the first president after Mubarak. During Mubarak's presidency, they were strictly forbidden, leading them to use the Internet to exert their influence. During the Arab Spring mobilizations, the government declared them as a terrorist organization, with most of their leaders being arrested.

The map in **Figure 10.6** depicts the Arabic language blogosphere. Each dot is a blog, and the dot's size represents how many other blogs link to this blog, while the size represents the popularity of the content. The

position of the dots is also not random. It is positioned by linkages to the neighboring dots (Etling, 2009). The map shows that the Egyptian bloggers are the largest group in the Arabic blogosphere. They are the biggest population of any Arab country. Lynch argues that Egypt has the most active political bloggers and that people on the web are interested in political movements and slogans (Lynch, 2007).

During the Arab Spring, the blogosphere projected the actions of the street on the internet so that everyone could be informed and, in a way, take part without being physically there. This was a great support for the social movement (Hamm, 2006), and these two facts, the overcoming of distances and time shifted communications, are the prime characteristics of the new digital media. According to Bieber (2007), blogs can be venues for protests that regimes cannot control (Bieber, 2007). In Egypt, blogs played the role of information distribution because media corporations were mostly censored (Armbruster, 2011). Therefore, the blogs acted more than information distributors, and bloggers used their channels to promote political ideas, spread appeals to Egyptian people, and inform about new approaches. From this point of view, they also had a considerable impact on the development of the Arab Spring in Egypt and the retirement of the autocratic president Muhammed Husni Mubarak in February 2011.

10.8.3 The Role of Women

The impressive percentage of women in the Tunisian demonstrations and the recent actions contrast with *"stereotypes about the Arab streets that propagate the image of a male-dominant public space"* (Marzouki, 2011). Similarly, Khamis and Vaughn (2011) argue that social media's horizontal and non-hierarchical structure empowered women who engaged in online activism and effectively and courageously participated in demonstrations and protests. The action of these women utilizing tools and space brought them into global recognition and, in many ways, equated them to Western feminist heroines.

In this context, Sahar Khamis (2011) argued that *"the prolific online and offline political activities of Arab women over the last several months have contributed a new chapter to the history of both Arab feminism and the region."* Since then, international focus and recognition of women's involvement through traditional activism and social media have allowed for a gendered revolution or gender oriented social change. However, the complexity of civil society—online or offline—under authoritarian regimes introduces another level of difficulty, conceptual (i.e., the challenge of understanding and navigating authoritarian procedures) and technical (i.e., the barriers to social network access). For example, the case of Arab women who are often perceived as powerless (Lengel & Newsome, 1997; Newsome & Lengel, 2003). The impact of the Arab Spring revolution on enhancing gender equality in the Middle East and North Africa is under investigation as multiple feminist scholars and activists have challenged it.

10.8.4 An Evaluation of the Result

As mentioned earlier, the revolts of the MENA countries did not lead all to the same results in terms of democratization: in Tunisia, there has been progress regarding freedom of speech and press. The elections became free and corruption has declined. In Algeria, the government of Abdelaziz Bouteflika raised people's salaries and reduced the prices for basic necessities in 2011. However, with the downtrend of the oil revenues at the end of 2015, the country had to follow an austerity policy that forced the government to increase the prices again and lower the subsidies. In Morocco, on March 9, 2011, King Mohammed VI announced an important constitutional reform to strengthen the power of the Prime Minister and other political parties. In July, a referendum established legislative elections in the country. In Egypt, on February 11, 2011, protests led to Hosni Moubarak's resignation after 30 years as president and giving his powers to the Supreme Council of the Armed Forces. Mohamed Morsi has been elected, but he has been removed and arrested by the army. In

2014, Marshal Sissi was elected with 96% of the votes after he stamped out all his competitors. The government of Al-Sissi muzzles every kind of opposition.

Whatever the results of this revolution are, one of the consequences is the strong development of the digital media, especially the social media. They did not make the Arab Spring themselves, but it was certainly a tool that helped spread of information and coordination., Without social media, there would have been no revolution, for many scholars. Indeed, the people would not be able to get informed without them.

The cases of Egypt and Tunisia are two different examples of how social media could be used. In Egypt, long-term activism has been developed through the Internet. In Tunisia, this kind of activism could not take place because of censorship and state repression, but social media played an important role in giving the final blow to the regime.

Social media can, at the same time, promote political and social reforms and have the most power in times of crisis as a mobilization tool and information repository. In the troubled countries, the result of the revolt was not predictable. A network revolution can lead to regime change but also to bloody repression (as it is in Libya and Syria). A satisfying theory about the link between digital activism and regime changes could never be elaborated. Those changes depend on several factors, particularly the economic and social situation and the conflicts inside the regime or the level of repression. In some countries, the Arab Spring did not change many things: less corruption and a little more democracy. Nevertheless, macroscopically, the social and economic situation remains more or less the same, with very high unemployment and persistent inequalities. Moreover, the collapse of the governments has permitted the emergence of many political and radical groups, which keep expanding, taking advantage of the fragile situation in those countries. This is particularly the case with radical Islamist groups such as ISIS, which leads actions in almost all countries, mainly in Syria or Libya, which are in a harmful civil war. However, these groups use new media extensively for their propaganda, which confirms that social media has become a permanent component of contemporary politics. This is the first time in history that social media has been used to such an extent as a tool for supporting a revolution, and it is no longer a temporary incident.

10.9 The *Indignados* Movement

10.9.1 The Birth of the *Indignados* Movement in Spain

The *Indignandos* movement, the *Anti-Austerity* movement, or the 15-M movement, is a well-known series of demonstrations in Europe and worldwide organized using social media. It mobilized people to protest against the political and economic measures enforced after the Great Recession of 2008. It started in Spain in May 2011, calling fifty-eight Spanish cities to protest. Their main demand was a change in the political system, beginning with the change of their current Spanish politicians. That was mainly because the demonstrators were not satisfied with the existing political parties and politicians supposed to represent their interests and beliefs. They were also against the measures that were approved, signed, and taken by the government. They were also opposed to the expanding corruption, the banks' operation, and the deteriorating economy and public sector, which worsened the economic conditions, rapidly raising the unemployment and cutting welfare funds. There was a major call to protest for citizens to preserve their homes, work, culture, health, and educational rights which were underestimated.

According to statistics published by RTVE (the Spanish public broadcasting company), between 6.5 and 8 million Spanish have participated in these events. The main reason that the movement started in Spain was because of its economic circumstances. Since the crisis of 2008, Spain had one of the highest unemployment rates in Europe, reaching a Eurozone record of 21.3%. The number of unemployed people in Spain stood at

4,910,200 at the end of March 2011, about 214,000 more than the previous quarter, while the youth unemployment rate stood at 43.5%, the highest in the European Union.

In September 2010, the government approved several reforms to the labor market aiming to reduce unemployment and revive the economy. Many trade unions rejected the plan because it made it easier and cheaper for employers to hire and fire workers and called for a general strike on September 2010. Meanwhile, the government for the rest of the year kept proceeding with economic reforms suggesting increasing the retirement age from 65 to 67. The Spanish and other unions still rejected the program, and a strike was called on January 27 in Galicia, Catalonia, and the Basque Country about that. Some of the demonstrations in Madrid ended up in clashes.

In February, the Sinde law passed, which added another reason to protest. That law permitted an administrative commission to shut down any web page that showed links, allowed downloading of copyrighted content without judicial supervision, even though the courts had repeatedly declared the legality of linking to these contents. That meant that people would not have access to downloading music, movies, and other content through websites because of the copyright policy. Of course, that led many users on Spanish forums and on social networks to criticize the law that had been approved. An anonymous campaign was created, *#nolesvotes,* calling citizens to vote against the parties that supported the law.

In January 2011, the digital platform ¡Democracia Real YA*!* (a true democracy, now) was created by users in Spanish social networks and forums using X and Facebook, calling the unemployed, the poorly paid, the subcontractors, the precarious and young people generally to protest on May 15 in 58 cities. That same day, small demonstrations in support of the Spanish ones were organized in Dublin, Lisbon, Amsterdam, Istanbul, Bologna, London, and Paris. Before the demonstrations, *¡Democracia Real YA!* organized several symbolic events, such as the occupation of a bank in Murcia on May 13. While demonstrations were still going on, the website of *¡Democracia Real YA!* had the support of over 500 diverse associations. Nevertheless, they kept rejecting any kind of collaboration with any political party or labor union to defend the protests' independence from all institutionalized political ideology.

The Portuguese *Geração à Rasca* movement was also an inspiration. Students were protesting against Education Minister Couto dos Santo. According to organizers' estimates, 200,000 to 300,000 people participated in the Lisbon rally. Other demonstrations took place in Porto with about 80,000 people in Funchal, in Ponta Delgada, and Viseu. The spontaneity of the demonstrations reminded media observers of the beginnings of unrest in Tunisia and Egypt. A group of friends, Alexandre Carvalho, António Frazão, John Labrincha, and Paula Gil, were the ones that started it by creating a Facebook page and a blog. Its main call was to improve working conditions, especially for qualified young people. A manifesto, which was published in Facebook, called for participation in a demonstration in Lisbon on March 12, 2011.

On May 15, 2011, the exasperation of the crisis led the Spaniards on the path of indignation, and a significant event was organized, including the *Puerta del Sol*. The event was convened on social networks and was supported by the platform "*Democraria Real Ya,*" which coordinated various groups and marches that brought together thousands of people. Dispersed by the police on May 16, they returned the next day and settled on the spot. What started with Madrid spread very quickly to several cities in the country such as Barcelona, Cartagena, and Valencia. The movement brought together individuals of all classes, statuses, and origins. All protests were against social inequalities and denounced the excesses of capitalism. Thus, *The Indignados* occupied *Puerta del Sol* from May 17 to June 12, 2011, and the movement would continue in the form of citizen assemblies and popular committees in other cities. From May 17, 2011, an alternative village was created in Puerta del Sol, with many blue tarpaulins. Connected to the internet, thanks to antennas installed by neighbors or businesses to relay their Wi-Fi networks and electricity through solar panels, a dozen laptops were aligned in the stand "communication" of the camp. A team of ten people was responsible for

managing the movement's information published on social networks, such as updating the Facebook page of the "Spanish revolution," which emerged in the wake of the recent Arab revolutions. On May 25, 2011, the Spanish Revolution Facebook page had 146,000 fans: on X, the *@acampadasol* account had nearly 50,000 subscribers. On X, the keywords *#acampadasol* (encampment ground), *#notenemosmedio* (we are not afraid), *#nosquedamos* (we remain), or *#spanishrevolution* made the race at the top of the most popular keywords in Spain during the first days of mobilization. After leaving the Puerta del Sol square, the June 19, 2011, demonstration, organized by the Indignados of Spain brought together 200,000 people. Subsequently, the movement was institutionalized by the Podemos party.

10.9.2 The Proliferation of *Indignados* (*Indignants*) in Greece

What happened in Spain was repeated with almost the same characteristics in Greece. The use of social networks was quite similar. The demonstrations there started through Facebook as a response to the Spanish *Indignandos* (Indignants = Aganaktismenoi) movement. Because they started through social media, the phenomenon was named "*May of Facebook.*" Another name given was "*The Movement of the Squares*", as people gathered in squares with demonstrations expanding radically across squares around the country. The mobilizations were caused by the fact that in April 2010, a memorandum was signed with the IMF, the EU, and the ECB to cover the borrowing needs. A memorandum, followed by other agreements, provided austerity measures and extensive cuts in public spending. As a result, social needs were taken into little consideration by increasing taxes, freezing recruitment, reducing salaries, and cutting social benefits. In the private sector, increased unemployment and reduced economic development. Since the announcement of the measures and throughout the period of these agreements, major social reactions were created, leading to organized public demonstrations and strikes in Greece. In June 2011, the Medium-Term Fiscal Strategy was put on the table, which was also met with great disapproval by the Greek population and with rejection of the opposition and objections even within the ruling party.

It all started with two citizens from the city of Thessaloniki, who were inspired by the movement of the Spanish "Indignandos" or "M-15" and possibly the ironic slogan "Make silence not to wake them Greeks." It built a Facebook page named "*Indignants at the White Tower*" to protest peacefully against the crisis and all the factors that led to it. The page "*Indignandos in Syntagma"* was an initiative by two or three adolescents who were the instigators of the initiative. They claimed that they saw the page *"Indignants at the White Tower"* on Facebook that coordinated the concentrations in Thessaloniki, where around 1,000 people were gathered, and decided to do such an event in Athens as well.

Several thousands of Greeks invaded Syntagma Square on May 25, 2011: the gathering, inspired by the Puerta del Sol in Madrid, was organized via the internet, including the Facebook platform, under a single word, *"the indignados."* On May 25, 2011, the Facebook page *"Indignation you in Syntagma"* had 32,500 fans. On the evening of May 24, when the call for demonstrations arrived in the editorial offices, it numbered only about 22,000 people. About 8,000 people, including many young people, were present, according to the police, while other spontaneous demonstrations on the same model took place in other Greek cities. People from all class origins were mobilized there, with the majority being young people demanding a "real democracy, now!". Concentrations continued for several days in Syntagma Square, the White Tower in Thessaloniki, and dozens of other cities in Greece. Some people who attended were on lasting protest, staying overnight in tents. The movement soon spread to many countries in Europe and the United States.

The main and common feature of the demonstrations and concentrations of the *"Indignants"* were the absence of separate party identities and the peaceful character. The difference was that in Greece more conventional protests from unions and political groups occurred, accompanied sometimes by general strikes

and demonstrators' clashes with the police. A new feature added was informal folk assemblies and demands of direct democracy and resolutions publicly accessible online.

10.9.3 Analysis

The *Indignant* movement is one of the most important collective actions in the recent history of Greece (and not only), which has drawn the interest of social and political scientists about the "democratic possibilities" offered by the "social web." *Aganaktismenoi* was the most powerful reaction of citizens towards the Greek crisis and its consequences: the several austerity plans (memoranda) adopted by the Greek government under the aegis of the so-called Troika (the European Commission, the European Central Bank, and the International Monetary Fund), which considerably impacted the Greek society (increase of inequalities, enhancement of distrust toward traditional political institutions, increase of unemployment, poverty etc.).

In many ways, this social movement distinguished itself from the previous Greek ones and led many to consider it a new way to engage in political life. The movement claimed to represent a new political voice, nonpartisan and nonviolent. The anarchic and anti-establishment roots of the Internet subculture pervaded the *Aganaktismenoi.* Indeed, the protest was organized through social networking sites and microblogs, without any domination of the usual political activists, such as trade unions and political party members, who are deeply rooted in Greek political and social life.

Fundamentally, the Greek *Aganaktismenoi* resembled the Spanish *15-M* movement: it was a movement of citizens, by citizens and for citizens, defying the party system and, more generally, the well-established Greek political sphere (joining and connecting elites, labor unions, media leaders, etc.). Facebook and X were the main tools used as organizing platforms to encourage people to meet in Athens' Syntagma Square and other Greek cities to demonstrate peacefully against corruption, mainstream media, and austerity plans without party labels. Thus, social media, especially X, Facebook, and some influential blogs like *@radiobubblenews*, and *@theproject* played a major role in reproducing content, so they were the main conveyors of alternative information. Nevertheless, beyond the unusual massive use of social media to mobilize people, one of the most significant aspects of *Aganaktismenoi* that distinguishes it from protests that are organized—or at least supported—by traditional political organizations is the composition of the protesting public. The socio-political composition of the demonstrators appeared to be different from the typical political activists' profile: people who gathered were generally younger, more educated, unemployed, and with lower levels of previous political activity and organizational involvement.

These features bring to the foreground the question of whether the social web could be a means to revive the old-fashioned representative democracy and thus give a voice to people who were left aside up to now. Thus, the "glue" (the term is used by Putnam who speaks about "social glue") that holds these loose networks of actors together is not a shared ideology but rather the loose, non-hierarchical modes of organizing that allow different perspectives to coexist.

Considering all the arguments above, it is clear that the number of protesters would not be that big and the demonstrations so massively organized if not for the use of digital media. As in the other case studies presented in this chapter, they not only contributed to changes in political regimes and enforced policies but also demonstrated the power of these technological innovations as they can transform an entire society passing messages globally and thus enabling actions that can succeed in protecting personal interests and rights.

10.10 Conclusion

This chapter has dealt with the role of digital media in cases of collective action and civil disobedience. More specifically, it has been shown that the internet has the potential to act in the following two ways: as an organizational tool for the protesters and as an alternative to mainstream media, informing people about the course of protests or whole revolutions. It has also been demonstrated how Internet tools have the potential to be used to gain support, both on a national and an international level.

Some studies have shown that the technologies offered by Web 2.0 have enabled social movements and collective actions to organize and thus erupt in the offline world in a new way: less hierarchical, more spontaneous, more creative, broader, and more diverse as well as at incredibly lower cost than "traditional" social movements. Recent incidents like the Arab Spring indicate that it seems unavoidable for future protestations not to use social media: they are free, instant, and unlimited. With a group on Facebook, X, or any blog, people can instantly find like-minded people and share ideas and information to make plans to change policies and not only.

Web 2.0 can facilitate the emergence of collective actions in the offline world, but in the digital age, online social movements can also exist without offline concretization. Modern techniques of expressing opposition online, such as Hacktivism, have also emerged and have been thoroughly presented along with their "impressive" results when applied.

Main doubts concern the ephemeralness of social movements born on the Internet, and many point out the need for face-to-face communication to sustain the vitality of collective action and the social ties created on their occasion. Furthermore, it is also argued that what people expect from a social movement (and more generally from political engagement through collective action) is not only the possible outcome but also the emotional retribution provided through real-life collective action: to feel the rush, the thrill of real, physical action. However, the case studies presented in this chapter show that online initiatives can potentially revitalize social ties that may have been damaged or lost.

References

Black Lives Matter, 2020. "Black Lives Matter." Available at: https://blacklivesmatter.com/ [Accessed 1 September 2020].

Adamic L., and Glance N., 2005. "The political blogosphere and the 2004 US election: divided they blog." *Proceedings of the 3rd international workshop on link discovery*, pp. 36–43. Available at http://www.blogpulse.com/papers/2005/AdamicGlanceBlogWWW.pdf [Accessed 6 March 2012].

Aelst J. V. L., 2010. "Internet and Social Movement Action Repertoires: Opportunities and Limitations." *Information, Communication and Society*, pp. 1146–1171.

Agarwal S.D., Barthel M.L., Rost C., Borning A., Bennett W.L., and Johnson C.N., 2014. "Grassroots organizing in the digital age: considering values and technology in Tea Party and Occupy Wall Street." *Information, Communication and Society*, [e-journal] 17(3), pp. 326–341. Available at: https://doi.org/10.1080/1369118X.2013.873068

Aladro-Vico E., Jivkova-Semova D., and Bailey O., 2018. "Activism: A New Educative Language for Transformative Social Action." *Media Education Research Journal*, v. 26 n57, pp. 9–18. Available at: https://eric.ed.gov/?id=EJ1192386

Albright D., 2015. "Hashtag Activism: #powerful or #pointless?" Web culture. Available at: http://www.makeuseof.com/tag/hashtagactivism-powerful-pointless/ [Accessed 9 December 2016].

Alto P. C. Glaisyer T., Pirolli P., Preece J., Rotman D., Shneiderman B., Vieweg S., and Yardi S., 2011. "From Slacktivism to Activism: Participatory Culture in the Age of Social Media." Available at: http://yardi.people.si.umich.edu/pubs/Yardi_CHI11_SIG.pdf [Accessed 27 December 2016].

Anderson L. G., Herr G. K., 2007. *Encyclopedia of Activism and Social Justice*. California: SAGE Publications.

Anonymous Official @ YouTube, 2014. "Anonymous Documentary - How Anonymous Hackers changed the World; We are Legion." Available at: https://www.youtube.com/watch?v=FAECyLvSCHgandindex=39andt=402sandlist=WL [Accessed 15 November 2018]

Anonymous, 2011. "Anonymous - The Uber-Secret Handbook." Retrieved in December 2018 from Anonops@Facebook.com. Available at: https://anonhq.com/wp-content/uploads/2014/05/Anonymous_Security_Handbook.pdf [Accessed 15 December 2018].

Arendt H., 1963. *On Revolution*. London: Penguin Books.

Arendt H. 1958. *The Human Condition*. Chicago and London: The University of Chicago Press.

Bayat A., 2010. *Life as politics: How ordinary people change the Middle East*. Amsterdam, The Netherlands: Amsterdam University Press.

Benjamin F., Jun N., and Williams L., 2018. *Anarchism; a conceptual approach*. New York: Routledge.

Bennett W.L., and Segerberg A., 2012. "The logic of connective action." *Information, Communication and Society*, 15, pp. 739–768.

Berghel H., 2015. "Cyber chutzpah: The Sony hack and the celebration of hyperbole." *Computer*, 48(2), pp.77-80.

Blumer H., 1969. "Collective Behavior. Indianapolis." Ind.: Bobbs-Merrill, College Division.

Brian Lehrer Live, 2010. "Gabriella Coleman on Anonymous." *Vimeo*. Retrieved in December 2018.

Brown H., E. Guskin E., and Mitchell A., 2012. "The Role of Social Media in the Arab Uprisings." Available at: http://www.journalism.org/2012/11/28/role-social-media-arabuprisings/ [Accessed 14 May 2018].

Bruggeman J., 2008. *Social Media: An Introduction*. Edition 1, Routledge.

Buechler S. M., 2000. *Social movements in advanced capitalism: the political economy and cultural construction of social activism*. Oxford University Press.

Burlingame D., 2004. *Philanthropy In America: A Comprehensive Historical Encyclopedia*. ABC-CLIO.

Butler M., 2011. "Clicktivism, Slacktivism, or real Activism? Cultural codes of American activism in the internet era." University of Colorado. Available at: https://scholar.colorado.edu/cgi/viewcontent.cgi?article=1011andcontext=comm_gradetdsandfbclid=IwAR3rXAtWPW6MsoN3Z5RHO19cSlRo_1-AGWNKD4ULBRBsPvq1lHMVk5mCx70 [Accessed 19 December 2018].

Butsch R., 2007. *Media and public spheres*. Basingstoke, UK.

Cabrera N., Matias C., and Montoya R., 2017. "Activism or slacktivism? The potential and pitfalls of social media in contemporary student activism." *Journal of Diversity in Higher Education*, 10(4), pp. 400–415.

Castells M., 2009. *Communication Power.* Oxford, New York: Oxford University Press.

Castells M., 2012. "*Networks of Outrage and Hope: Social Movements in the Internet Age*." Wiley.

Cernison M., 2019. *Social Media Activism Water as a Common Good*. Amsterdam University Press B.V.

Chen Adrian, 2010. "The Top Three Myths About Anonymous." Retrieved from Gawker: https://gawker.com/5710948/the-top-three-myths-about-anonymous

Chivers T., 2017. "Wikileaks' 11 greatest stories." Available at: *The Telegraph*: http://www.telegraph.co.uk/news/0/wikileaks-greatest-ever-stories-scandals/ [Accessed 22 May 2017].

Christensen H. S., 2011, "Political activities on the internet: slacktivism or political participation by other means?" *First Monday*, 7 February 2011. Available at: https://uncommonculture.org/ojs/index.php/fm/article/view/3336/2767 [Accessed 19 December 2018].

Christiansen J., 2009. "Four stages of Social Movements." EBSCO Publishing Inc.

Christiansen J., 2015. "Four Stages of Social Movements." *Research Starters: Sociology*, EBSCO Publishing Inc.

Chu D., 2018. "Media Use and Protest Mobilization: A Case Study of Umbrella Movement Within Hong Kong Schools." Available at: https://www.researchgate.net/publication/323648241_Media_Use_and_Protest_Mobilization_A_Case_Study_of_Umbrella_Movement_Within_Hong_Kong_Schools [Accessed 20 December 2018].

Ciambriello R., 2014. "How a No Makeup Selfie Trend Suddenly Became a Cancer Awareness Effort Viral posts evolve organically," *Adweek*. Available at: https://www.adweek.com/creativity/how-no-makeup-selfie-trend-suddenly-became-cancer-awareness-effort-156480/

Coleman G., 2014. *Hacker, hoaxer whistleblower, spy; The many faces of Anonymous*. London: Verso.

Coleman G., 2017. "Gopher, Translator, and Trickster; The Ethnographer and the Media." In D. Fassin, *If Truth Be Told; The Politics of Public Ethnography.* Durham and London: Duke University Press, pp. 20–45.

Comninos A., 2011. "Twitter revolutions and cyber crackdowns: User-generated content and social networking in the Arab Spring and beyond." Association for Progressive Communications (APC).

Comunello F., and Anzera G., 2012. "Will the revolution be tweeted?" A conceptual framework for understanding the social media and the Arab spring. Taylor and Francis Online. Available at: https://www.tandfonline.com/doi/abs/10.1080/09596410.2012.712435

DeLuca K. M., Lawson S., and Sun, Y., 2012. "Occupy Wall Street on the Public Screens of Social Media: The Many Framings of the Birth of a Protest Movement," *Communication, Culture and Critique*, [e-journal] 5(4), pp. 483–509. Available at: https://doi.org/10.1111/j.1753-9137.2012.01141.x

Denning D. E., 2001. "Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy." Networks and netwars: The future of terror, crime, and militancy, Internet and International Systems: Information Technology and American Foreign Policy Decision-making WorkshoNautilus Institute, San Francisco.

Dennis J., 2018. *#stopslacktivism: Why Clicks, Likes, and Shares Matter. Beyond Slacktivism.*, Palgrave Macmillan, Cham, pp. 25–69.

Dennis J. 2018. "People. Power. Change. 38 Degrees and Digital Micro-Activism on Social Media." *Beyond Slacktivism*. Palgrave Macmillan, Cham, pp. 95–121.

Dennis J.W., 2014. "Click here to save the world? rethinking slacktivism and digital participation." *Political Studies Association*: Insight Plus.

Docsteach.org, 2020. "Civil Rights Act Of 1964." Available at: https://www.docsteach.org/documents/document/civil-rights-act-of-1964 [Accessed 15 July 2020].

Douay N., 2014. "Digital Social Movements and Spatial Planning." *Social Information*, 2014/5 (No. 185), pp. 123–130. Available at: https://www.cairn.info/revue-informations-sociales-2014-5-page-123.htm [Accessed 16 April 2018].

Dustin K., 2016. "Social Media and Social Movements." *Sociology Compass*.

Earl, J., Kimport, K., Prieto, G., Rush, C., Reynoso, K. 2010. "Changing the World One Webpage at a Time: Conceptualizing and Explaining Internet Activism, *Mobilization: An International Quarterly*." [e-journal] 15(4), pp. 425–446. Available at: Mobilization: An International Quarterly, website: https://mobilizationjournal.org/doi/abs/10.17813/maiq.15.4.w03123213lh37042 [Accessed 12 May 2019].

El-Bendary M., 2013. *The Egyptian Revolution And Its Aftermath*. New York: Algora Pub.

Encyclopedia Britannica, 2020. "Arab Spring | History, Timeline, Causes, Effects, and Facts." [online] Available at: https://www.britannica.com/event/Arab-Spring [Accessed 20 July 2020].

Faris D., 2008. "Revolutions without revolutionaries? Network theory, Facebook, and the Egyptian blogosphere." *Arab Media and Society*, 6, pp. 1–11.

Faris D., 2010. "Revolutions Without Revolutionaries? Social Media Networks and Regime Response in Egypt." Publicly Accessible Penn Dissertations. 116, Available at: http://repository.upenn.edu/edissertations/116 [Accessed 15 June 2019].

Fischer M., 2016. "#Free_CeCe: the material convergence of social media activism." *Feminist Media Studies* (5), pp. 755–771.

Franks Benjamin, 2014. "Anti-fascism and prefigurative ethics." *A Journal of Radical Theory*, 8(1), pp. 44–72. Available at: http://eprints.gla.ac.uk/94199/1/94199.pdf [Accessed 17 November 2018].

Fuentes M.A., 2014. "Digital activism." Available at: https://www.britannica.com/topic/digital-activism [Accessed 12 May 2019].

Gaby S., and Caren N., 2012. "Occupy Online: How Cute Old Men and Malcolm X Recruited 400,000 US Users to OWS on Facebook." *Social Movement Studies*, [e-journal] 11(3-4), pp. 367–374. Available at: https://doi.org/10.1080/14742837.2012.708858 [Accessed 9 May 2019].

Gamson W. A., and Wolfsfeld G., 1993. "Movements and Media as Interacting Systems." *Annals of the American Academy of Political and Social Science: Citizens, Protest, and Democracy* 528: pp.114-125.

Georgalou M., 2015. “Small Stories of the Greek Crisis on Facebook.” Social Media + Society, *Sage Journals*, pp. 1–15.

George J., and Leidner D., 2019. "From clicktivism to hacktivism: Understanding digital activism." *Information and Organization*, 29(3), pp. 100-249.

Gerbaudo P., and Treré E., 2015. "In search of the ‘we’ of social media activism: Introduction to the special issue on social media and protest identities." *Information, Communication and Society*, 18(8), pp. 865-871. Glenn, C., 2015.

Gitlin T., 2013. "Occupy’s predicament: the moment and the prospects for the movement." *The British Journal of Sociology*, [e-journal] 64(1), pp. 3-25. Available at: https://doi.org/10.1111/1468-4446.12001 [Accessed 5 May 2019].

Gladwell M., 2010. "Small Change - Why the Revolution Will Not Be Tweeted." *The New Yorker*.

Gleason, B., 2013." #Occupy Wall Street: Exploring Informal Learning About a Social Movement on Twitter". American Behavioral Scientist, [e-journal] 57(7), pp. 966–982. Available at: https://doi.org/10.1177/0002764213479372 [Accessed 3 May 2019].

Glenn L. Cerise, 2015. “‘Activism or “Slactivism?’: ‘Digital Media and Organizing for Social Change.’” Published online, pp. 81-85. Available at: https://www.tandfonline.com/doi/abs/10.1080/17404622.2014.1003310 [Accessed 17 December 2018].

Goldman D., and Pagliery J., 2015. "#JeSuisCharlie becomes one of most popular hashtags in Twitter's history." *CNNMoney*.

Goodwin J., and Jasper J., 2003. *The Social Movements Reader: cases and concepts*. Malden: Blackwell Publishing.

Grether R., 2000. "How the etoy campaign was won: An agent's report". *Leonardo*, 33(4), pp. 321–324.

Gunkel D. J. 2005. "Introduction to hacking and hacktivism." *New Media and Society*, 2005/10 Vol 7; Iss.5.

Haggard S., and Lindsay J. R., 2015. "North Korea and the Sony hack: Exporting instability through cyberspace." Honolulu: East-West Center, *AsiaPacific Issues*, No. 117.

Halupka M., 2017. "The legitimization of clicktivism in Doing democracy and governance in the fast lane? Towards a ‘politics of time’ in an accelerated polity." *Australian Journal of Political Science* 53:4, pp. 548–564. Available at: https://www.tandfonline.com/doi/abs/10.1080/10361146.2017.1416586 [Accessed 20December 2018].

Hebing L., 2018. "Persuasion in the Millennial Era: A Case Study of KONY 2012." Honors Senior Theses/Projects.

Herman J., 2016. "Hashtags and Human Rights: Activism in the Age of Twitter." Carnegie Council for Ethnic international affairs. Available at: https://www.carnegiecouncil.org/media/series/ethics-online/hashtags-and-human-rights-activism-in-the-age-of-twitter [Accessed 25 November 2016]

Howard P., Duffy A., Freelon D., Hussain M., Mari W., and Mazaid M., 2015. “Opening closed regimes: What was the Role of social media during the Arab Spring?” Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096 [Accessed 17 April 2020].

Hutchins A., and Tindall N., 2016. *Public Relations and Participatory Culture: Fandom, Social Media and Community Engagement.* Routledge.

IDCA, 2020. "Civil Rights Act Of 1957." Available at: https://iowaculture.gov/history/education/educator-resources/primary-source-sets/right-to-vote-suffrage-women-african/civil-rights-act-1957 [Accessed 25 July 2020].

Jasko K., and Besta T., 2018. "Activism – Radicalization – Protest: An introduction to a special section." *Social Psychological Bulletin*, 13(4), Article e32244. Available at: https://doi.org/10.32872/spb.v13i4.32244 [Accessed 13 December 2018].

Jones C., 2013. "Activism or Slacktivism? The Role of Social Media in Effecting Social Change." Research Paper in STS 4600. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.467.6295andrep=rep1andtype=pdf [Accessed 9 December 2016].

Jordan T., 2002. *Activism! direct action, hacktivism and the future of society*. Reaktion books.

Juris S. J., 2005. "The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements." *The Annals of the American Academy of Political and Social Science*, Vol. 597, pp. 189–208. Available at: https://journals.sagepub.com/doi/10.1177/0002716204270338 [Accessed 10 December 2018].

Kaplan A., and Haenlein M., 2012. "Social media: back to the roots and back to the future." *Journal of Systems and Information Technology*, Vol. 14 No. 2, pp. 101–104. Available at: https://www.emerald.com/insight/content/doi/10.1108/13287261211232126/full/html [Accessed 23 April 2020].

Karatzogianni A., 2015. *Introduction: Four Phases of Digital Activism and Cyberconflict. Firebrand Waves of Digital Activism 1994–2014*. pp. 1–4, Palgrave Macmillan, London.

Kaun A., 2018. "Digital Activism: After the Hype." *The New Media and Society*, Vol. 20, no 6, pp. 2099-2106. Available at: https://journals.sagepub.com/doi/abs/10.1177/1461444817731924[Accessed 15 December 2018].

Kavada A., 2015. "Creating the collective: social media, the Occupy Movement and its constitution as a collective actor." *Information, Communication and Society*. Vol 18, No. 8.

Kavada A., 2016. "Social Movements and Political Agency in the Digital Age: A Communication Approach." *Media and Communication,* 4(4), pp. 8–12. Available at: https://doi.org/10.17645/mac.v4i4.691 [Accessed 13 December 2018].

Kendzior S., 2012. "The Subjectivity of Slacktivism." Al Jazeera.

Kidd D., and McIntosh K., 2016. "Social Media and Social Movements." *Sociology Compass*. 10. pp. 785-794. https://doi.com/10.1111/soc4.12399

Kligler Vilenchik N., and Thorson K. Good, 2014. "Citizenship as a frame contest: Kony2012, memes, and critiques of the networked citizen." *Journalism of consumer research*.

Lagan B., 2010. "International man of mystery." *The Sydney Morning Herald*.

Lane D. S., and Dal Cin S., 2018. "Sharing beyond Slacktivism: the effect of socially observable prosocial media sharing on subsequent offline helping behavior." *Information, Communication and Society*, 21(11), pp. 1523–1540.

Lee Y., and Hsieh G., 2013. "Does slacktivism hurt activism?" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* - CHI '13, pp. 811–820.

Lengel L., and Newsome V.A., 2012. "Framing Messages of Democracy through Social Media: Public Diplomacy 2.0, Gender, and the Middle East and North Africa." School of Media and Communication Faculty Publications. 1., Available at: https://scholarworks.bgsu.edu/smc_pub/1 [Accessed 11 June 2019].

Levy S., 1984. "Hackers: Heroes of the computer revolution." (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

Marchal N., 2016. "Wikileaks' 10 Biggest Leaks From the Past Decade." Available at: https://heatst.com/politics/wikileaks-turns-10-julian-assanges-most-devastating-leaks-from-the-past-decade/ [Accessed 1 June 2017].

Marcia M., 2018. "Scaling social movements through social media: The case of Black Lives Matter." *Social Media + Society*, pp. 1-14.

May Phing A., and Yazdanifard R., 2014. "How does ALS ice bucket challenge achieve its viral outcome through marketing via social media?" *Global Journal of Management and Business*. Available at: https://journalofbusiness.org/index.php/GJMBR/article/view/1572/1475 [Accessed 17 December 2018].

Mccaughey M., and Ayers M., 2013. *Cyberactivism: Online Activism in Theory and Practice*. Routledge.

Me Too Movement, 2020. "Me Too Movement." Available at: https://metoomvmt.org/ [Accessed 2 September 2020].

Miller J., 2018. "Digital citizenship tools for cause-based campaigns: a broadened spectrum of social media engagement and participation-scale methodology." University of Central Florida. Available at: https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=7022andcontext=etd [Accessed 13 December 2018].

Milner R. M., 2013. "Pop Polyvocality: Internet Memes, Public Participation, and the Occupy Wall Street Movement." Available at: https://ijoc.org/index.php/ijoc/article/view/1949 [Accessed 12 May 2019].

Morozov E., 2009. "The future of 'public diplomacy 2.0': Net effect." *Foreign Policy*. Available at: http://neteffect.foreignpolicy.com/posts/2009/06/09/the_future_of_public_diplomacy_20 [Accessed 15 June 2019].

Mutsvairo B., 2016. *Digital Activism in the Social Media Era*. New York, NY: Springer International Publishing.

Newsom V., and Lengel L., 2014. "Mutable selves and digital reflexivities: Social media for social change in the Middle East and North Africa." *Studies in Symbolic Interaction*, Volume 43, pp. 85-119.

Newsom V., and Lengel L., 2003. "The power of the weblogged word: Contained empowerment in the Middle East North Africa region." *Feminist Media Studies*, 3(3), pp. 360-363.

Newsom V., Cassara C., and Lengel L., 2011. "Discourses on technology policy in the Middle East and North Africa: Gender mainstreaming vs. local knowledge." *Communication Studies*, 62(1), pp. 1-16.

Newsom V., Lengel L., and Cassara C., 2011. "Local knowledge and the revolutions: A framework for social media information flow." *International Journal of Communication*, 5, pp. 1-20.

Newsom V.A., and Lengel L., 2012. "Arab Women, Social Media, and the Arab Spring: Applying the framework of digital reflexivity to analyze gender and online activism." *Journal of International Women's Studies* (JWS), Vol 13, iss.5, Available at: https://vc.bridgew.edu/jiws/vol13/iss5/5/ [Accessed 24 May 2019].

Olamilekan A., "Cyber-Activism and Social Network Media: Appropriating the Emerging Platform To The Promotion of Nation-Building and Peace." Available at: https://www.academia.edu/2464782/cyber-Activism_and_Social_Network_Media_Appropriating_the_Emerging_Platform_To_The_Promotion_of_Nation-Building_and_Peace [Accessed 12 April 2020].

Ouedraogo A., 2015. "Arab Spring and Social Media: the Social, Economic and Governance Issues Driving Revolutions: The Case of Tunisia." University of Ottawa. Available at: https://ruor.uottawa.ca/bitstream/10393/32754/1/Ouedraogo_Adolphe_2015_researchpaper.pdf [Accessed 24 May 2018].

Pappas S., 2015. "French Flags on Facebook: Does Social Media Support Really Matter?", LiveScience. Purch. [Accessed 4 January 4 2017].

Penney J., Dadas C., 2014. "Tweeting in the service of protest: Digital composition and circulation in the Occupy Wall Street movement." *New Media and Society*, [e-journal] 16(1), pp. 74–90. Available at: https://doi.org/10.1177/1461444813479593

Prasad V., 2018. "If Anyone Is Listening, #MeToo: Breaking the Culture of Silence Around Sexual Abuse Through Regulating Non-Disclosure Agreements and Secret Settlements." *Boston College Law Review*.

Rahman S., 2018. "How social media breeds social movements." *The Daily Star*. Available at: https://www.thedailystar.net/news/opinion/perspective/how-social-media-breeds-social-movements-1618270 [Accessed 15 November 2018].

Reed N., 2016. "The Influence of Social Media in Egypt during The Arab Spring." *SIT Graduate Institute/SIT Study Abroad SIT Digital Collections*, Available at: http://digitalcollections.sit.edu/cgi/viewcontent.cgi?article=3986andcontext=capstones [Accessed 20 June 2018].

Rohr Lopes A., 2014. "The Impact of Social Media on Social Movements: The New Opportunity and Mobilizing Structure." Creighton University, pp. 1-23 Available at: https://www.creighton.edu/fileadmin/user/CCAS/departments/PoliticalScience/Journal_of_Political_Research_JPR_/2014_JSP_papers/Lopes_JPR.pdf [Accessed 20 January 2016].

Rotman D., Vieweg S., Yardi S., Chi E., Preece J., Shneiderman B., Pirolli P., and Glaisyer T., 2011. "From slacktivism to activism." *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems* - CHI EA '11, pp. 819-822.

Sandoval-Almazan R., and Ramon Gil-Garcia J., 2014. "Towards cyberactivism 2.0? Understanding the use of social media and other information technologies for political activism and social movements." *Government Information Quarterly*, 31(3), pp.365-378.

Sanger D.E., and Benner K. 2018. "US Accuses North Korea of Plot to Hurt Economy as Spy Is Charged in Sony Hack." *The New York Times*, 6.

Schwartz M., 2011. "Pre-Occupied: The origins and future of Occupy Wall Street." Available at: https://www.newyorker.com/magazine/2011/11/28/pre-occupied?currentPage=al [Accessed 12 May 2019].

Shehabi A., and Jones M., 2015. *Bahrain's uprising: resistance and repression in the Gulf*. Kindle edition.

Skoric M.M., 2012. "What is slack about slacktivism." In Marolt P. (ed.), *Inter-Asia roundtable 2012: methodological and conceptual issues in cyber activism research*. Singapore: Asia research institute. Available at: https://ari.nus.edu.sg/wp-content/uploads/2018/10/InterAsiaRoundtable-2012.pdf [Accessed 2 December 2018].

Smith B., Krishna A., and Al-Sinan R., 2019. "Beyond Slacktivism: Examining the Entanglement between Social Media Engagement, Empowerment, and Participation in Activism." *International Journal of Strategic Communication*, 13(3), pp.182-196.

Statista, 2016. The Statistics portal, Most famous social network sites worldwide as of September 2016, ranked by number of active users (in millions), *Adweek*, Available at: https://www.statista.com/statistics/272014/global-social-networks [Accessed 20 January 2017].

Storck M., 2011. "The role of social media in Political Mobilization: a case study of the January 2011 Egyptian uprising." Available at: http://www.culturaldiplomacy.org/academy/content/pdf/participant-papers/2012-02-bifef/The_Role_of_Social_Media_in_Political_Mobilisation_-_Madeline_Storck.pdf [Accessed 17 April 2020].

Sutkutė R. 2016. "Social media as a tool of resistance or a new form of slacktivism?" Tiltas į ateitį [elektroninis išteklius]= The bridge to the future. Kaunas: Technologija, Nr. 1 (10). Vie S., 2014. "In defense of "slacktivism: The Human Rights Campaign Facebook logo as digital activism." *First Monday*, 19(4).

Taki M., and Coretti L., 2013. "The role of social media in the Arab uprisings-past and present." Communication and Media Research Institute of the University of Westminster.

Tantawy N., 2011. "Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory." *International Journal Communication*. Available at: https://ijoc.org/index.php/ijoc/article/view/1242/597 [Accessed 17 May 2020].

Tarrow S., 2005. *The New Transnational Activism*. Cambridge: Cambridge University Press.

Taylor R.W., Fritsch E. J., and Liederbach J., 2014. *Digital crime and digital terrorism*. Prentice Hall Press.

Taylor P., 1999. *Hackers: Crime and the digital sublime*. Routledge.

The Economist, 2013. "The Streets Erupt: A Demonstration About Bus Fares Has Become Something Much Bigger." Available at: https://www.economist.com/americas-view/2013/06/18/the-streets-erupt?spc=scodeandspv=xmandah=9d7f7ab945510a56fa6d37c30b6f1709

The Guardian, 2010. "Egyptian government fears a Facebook revolution." Available at: https://www.theguardian.com/commentisfree/2010/oct/21/egypt-facebook-revolution [Accessed 19 December 2016].

Theocharis Y., 2009. "Young People, Postmaterialism and Online Political Activism: The Greek Case." Paper presented at the *PSA Annual Conference*, 7th to 9th April 2009, Manchester, UK.

Theocharis Y., Lowe W., van Deth J. W., and García A. G. M., 2014. "Using Twitter to Mobilise Protest Action: Transnational Online Mobilisation Patterns and Action Repertoires in the Occupy Wall Street, Indignados and Aganaktismenoi movements." *Information, Communication and Society*, Taylor and Francis Online.

Theocharis Y., 2015. "Every Crisis is a Digital Opportunity: The Aganaktismenoi Movement's Use of Social Media and the Emergence of Networked Solidarity in Greece." *The Routledge Companion to Social Media and Politics*, pp. 1-15.

Thorson K., Driscoll K., Ekdale B., Edgerly S., Thompson L.G., Schrock A., Swartz L., Vraga E.K., Chris Wells C., 2013. "YOUTUBE, TWITTER AND THE OCCUPY MOVEMENT,", Information, Communication and Society, [e-journal] 16(3), pp. 421-451. Available at: https://doi.org/10.1080/1369118X.2012.756051

Tilly C., 1978. *From Mobilization To Revolution*. New York: McGraw-Hill.

Ufuophu-Biri E., and Ojoboh L., 2017. "Social Media as a Tool for Political Resistance: Lessons from the Arab Spring and the Nigerian Protests," *Academic Journal of Interdisciplinary Studies*, Vol. 6 No.1, pp. 61-66. Available at: https://www.researchgate.net/publication/315956553_Social_Media_as_a_Tool_for_Political_Resistance_Lessons_from_the_Arab_Spring_and_the_Nigerian_Protests [Accessed 14 May 2020].

Vie S., 2014. "In defense of slacktivism: The Human Rights Campaign Facebook logo as digital activism," *First Monday*, 7 April. Available at: https://uncommonculture.org/ojs/index.php/fm/article/view/4961/3868 [Accessed 16 December 2018].

Voultsios L., 2018. "The role of social networks and media in the shaping of public opinion: A case study of the Libyan Conflict." Aristotle University of Thessaloniki.

Wall D., 2003. *Crime and the Internet*, Routledge.

Wikileaks, 2011. "About us." Available at: https://wikileaks.org/About.html, [Accessed 25 May 2017].

Wikipedia, 2017. "Denial of service attack." Available at: https://en.wikipedia.org/wiki/Denial-of-service_attack [Accessed 31 May 2017].

Wikipedia, 2017. "Project Chanology." Available at: https://en.wikipedia.org/wiki/Project_Chanology [Accessed 4 June 2017].

Wikipedia, 2017. "Timeline of events associated with Anonymous." Available at: https://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous#Project_Chanology [Accessed 31 May 2017].

Wikipedia, 2017. "Guantanamo Bay files leak." Available at: https://en.wikipedia.org/wiki/Guantanamo_Bay_files_leak [Accessed 20 May 2017].

Wikipedia, 2018. "Wikipedia." Available at: https://en.wikipedia.org/wiki/Occupy_Wall_Street [Accessed 13 December 2018].

Will G., 2014. "Hashtag Activism: Not Intended To Have Any Effect On The Real World." *Real Clear Politics*.

Κουσκουβέλης Η., Λίτσας Σ., Ραπτόπουλος Ν., Κυριακίδης Κ., 2012. *Η Αραβική Άνοιξη*. Εκδόσεις Πανεπιστημίου Μακεδονίας.

Μελιτά Α., 2011. "Ο ρόλος της κοινωνικής δικτύωσης σε σχέση με τη πρόσφατη Αραβική Άνοιξη." Μη εκδοθείσα πτυχιακή Διατριβή. Τεχνολογικό Πανεπιστήμιο Κύπρου.

Σταματόπουλος Ο., 2016. *ΙΣΤΟΡΙΑ ΤΗΣ ΜΕΣΗΣ ΑΝΑΤΟΛΗΣ*. Θεσσαλονίκη, Επίκεντρο.

Chapter 11 Cybercrimes and the Deep/Dark Web

Abstract

Chapter 11 outlines the illegal and illicit actions committed in cyberspace: intellectual property theft, hacking, cyber stalking, identity theft, malicious software, online harassment, etc. The measures that both organizations and nation-states should take to prevent cybercrimes are presented, as well as the response of the EU to confront issues like large scale cyberattacks and sensitive issues like the exploitation of children's vulnerabilities. The Deep and the Dark Web are also outlined here, and the illegal activities that are conducted in the latter are listed, including human trafficking, Illicit trade, drugs or guns trade.

11.1 Introduction

The internet's increased interconnectedness has introduced an increased risk of theft, fraud, and abuse between people of all kinds and ages and all walks of life. The same technological achievements that helped make life more convenient and empowered us to create even more empowered those willing to disrupt and damage. As people and companies or organizations worldwide become more and more dependent on networks and technology, they are unavoidably becoming more exposed to cyber-attacks and frauds.

Malicious actors take advantage of cutting-edge technology; they have committed highly sophisticated criminal activities deployed on the Internet. Moreover, these kinds of crimes constitute today the largest portion of criminal offenses, with their numbers dramatically increasing in recent years and surpassing, traditional crime rates. Some of the characteristics that play a significant role in that direction, are the low cost of committing a cybercrime, the high speed of its realization and effects, and, the fact that it can be highly profitable. According to the National Crime Agency "…*the cost of cybercrime to the UK economy is billions of pounds per annum – and growing*" (NCA, 2016). Following the same report, high-profile crimes have proven that common approaches to information and computer security are insufficient no matter what countermeasures we take to tackle them.

Law enforcement has a very important role in guaranteeing the necessary security by trying to detect a wide range of cybercrimes worldwide, such as theft or fraud towards the exploitation of children, and to locate and arrest cyber criminals. There are huge challenges concerning the legislation, which needs to keep adapting to the continuously evolving cyberspace, and jurisdictions that need appropriate international laws to harmonize national ones to facilitate the investigation process and promote international cooperation among law enforcement and other stakeholders.

Today, criminal investigators and experts on network security, with a deep understanding of today's technologies, are constantly developing standardized methods, practices, and tools to minimize or even stop cyber-attacks and protect humanity in the new technological paths life follows.

11.2 Cybercrimes

11.2.1 Cybercrime: definition

The word cybercrime refers to a crime that may be related to a computer and an Internet connection (network). In some specific cases, only the computer, used by someone who is called a hacker, may have been used to commit the crime, while in other cases, the computer may have been the target of the crime. Indeed, currently, more and more criminals are exploiting the internet's speed, convenience, and anonymity to commit a wide range of criminal activities. The term cybercrime also includes traditional crimes conducted over the Internet. Such examples could be hate crimes, telemarketing and Internet fraud, identity theft, and account or credit card theft. Therefore, cybercrime is all about all these features of a conventional crime involving cyberspace.

David Wall stresses the importance of first understanding the internet's impact on society and how ICTs have shaped the world over the years and then trying to define cybercrime (Wall, 2007). Cyberspace provides tools and creates new opportunities for bad actors to commit illegal activities by taking advantage of its unique characteristics. Walls named these characteristics as the "*key transformative impacts of the Internet,*" and are the following (Wall, 2005):

- **Globalization**, which enables bad actors to surpass local or national boundaries.
- **Distributed networks and grid technologies** that create new opportunities for victimization.
- **Synopticism and panopticism**, which enables remote surveillance capabilities on victims.

- **Asymmetric rather than symmetric relationships**, which do not justify spending resources in the investigation or prosecution of small-impact victimizations distributed across jurisdictions.
- **Data trails** that generate new opportunities for bad actors to commit identity theft.
- **Changes in the organization of criminal activities** that enable lone or groups of criminals to perpetrate extremely complicated and far-reaching tasks that can be repeatedly performed countless times across the globe.

Therefore, the Internet creates new opportunities for offenders by providing them with speed, global range, and the appropriate means to engage in illegal activities.

Cybercrimes are the fastest growing crimes in the industry today. Yet less than half of them go unnoticed or unreported. A definition for cybercrime is that it is "a term for any illegal activity that uses a computer as its primary means of commission". Another definition given by Hadler and Jaishankair is that cybercrimes are "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as the Internet (chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS)." This definition includes all aspects of digital crime, namely identity theft, cyber fraud, child pornography, creating spyware, and even bullying. The combination of these two definitions and the addition of a financial dimension makes cybercrime a term for any illegal activity using a computer, telephone, digital notebook, or any other technological device that stores data or uses modern telecommunications networks to commit offenses against individuals or groups of persons with criminal motivation to harm the reputation of the victim deliberately or to cause physical, economic or mental harm or loss to the victim for personal gain.

Donn Parker very early introduced the term "*computer abuse"* as "*any incident involving an intentional act where a victim suffered or could have suffered a loss, and a perpetrator made or could have made a gain and is associated with computers*" (Parker, 1976). The four ways in which computers engage in computer abuse are when:

- The computer is the *object*, or the information in the computer is the object of the act (e.g., when someone steals or damages a computer).
- The computer is the *subject*, creating a unique environment or unique form of assets (e.g., when a virus infects or impairs a computer).
- The computer is the *medium* or the *tool* of the act (e.g., when a computer is used to gain access to other computers).
- The computer represents a *symbol* used to fear or to deceive (e.g., a stockbroker pretending to have secret computer software in a powerful computer in a Wall Street brokerage firm to earn a lot of money on rapid stock option trading).

However, over the years, these categories have proved to be general enough to address the definitional issues on how to include both the "computer abuses" as defined by Parker in 1976, and the modern computer crimes the way we perceive them today. Following Parker's definitions from 1976 to 1998, on the one hand, and having in mind the evolution of technology that affected the nature of crimes, on the other, Robert Taylor presented four updated perspectives (Taylor, 2007):

- The computer as a *target*. In this category falls any attack on the system of legitimate user to render it inoperable or even destroy it (e.g., Denial-of-Service, virus infection, etc.).
- The computer as a *tool of crime*. For example, a computer might be used to access another computer and steal personal data.
- The computer as *an ancillary component to a crime*. In that sense, the computer is simply facilitating the crime. (e.g., money laundering, trade with child abuse material-CAM).

- Crimes related to the *dominance of computers*. This involves crimes against the computer infrastructure, such as the theft of intellectual property and software piracy.

Majid Yar (2006) suggests that cybercrime should not be seen as a sole concept but rather as "*a range of illicit activities"* whose common denominator is the key role that ICTs play in their commission. Yar also shares Douglas and Loader's definition (Douglas & Loader, 2000), who describe cybercrime as those computer mediated activities that are either illegal or considered illicit by certain parties and can be conducted through global electronic networks. It is important to note that Douglas and Loader, in their definition, differentiate crime (which is any explicitly prohibited illegal act) from deviance (which is any act against social norms and rules and, thus, undesirable or objectionable). However, from the criminology point of view, this is not always the case, and one might not be separated from the other. Yar goes further by citing Furnell (2002), who distinguished between *computer assisted crimes* (essentially traditional crimes that take advantage of the cyber domain e.g., fraud, theft, money laundering, etc.) and *computer-focused crimes* (offenses that have appeared at the same time with the advent of the Internet, and could not exist apart from it e.g., hacking, cracking, website defacement) (Yar, 2006).

The Council of Europe's Cybercrime Treaty uses the term cybercrime to refer "*to offences ranging from criminal activity against data to content and copyright infringement.*" However, Zeviar-Geese suggested that the definition should be more general, "including activities such as fraud, unauthorized access, child pornography, and cyberstalking," which all occur online. The United Nations Manual on the Prevention and Control of Computer Related Crime includes the definition of Cybercrime fraud, forgery, and unauthorized access. Other definitions of cybercrime include "unlawful acts where the computer is either a tool or a target or both."

Therefore, Interpol acknowledges that there is no global definition for cybercrime; however, Law Enforcement agencies, by and large, categorize cybercrimes into two types: Firs, those highly sophisticated and complex crimes (high-tech crimes) against computer hardware and software, and secondly, those cyber-enabled crimes, such as crimes against children, financial crimes. Interpol argues that a shift from simple forms of cybercrime to more complex and highly organized ones (criminal organizations rather than individuals) has been made in recent years, significantly impacting the global economy. By taking advantage of the new technologies, criminal rings are becoming "widespread and damaging."

According to Wall (2005), there are four legal categories for cybercrime:

- **Digital-trespass**: Crossing boundaries into other people's property and causing damage. For example, hacking, defacement, and viruses.
- **Digital-deceptions and thefts**: Stealing (money, property). For instance, credit card fraud and intellectual property violations (known as piracy).
- **Digital-pornography**: Activities that breach laws regarding obscenity and decency.
- **Digital-violence**: Doing psychological harm to, or inciting physical harm against others, thereby breaching laws about the protection of the person. For example, hate speech and stalking. We do not perceive digital crime until we are affected by the consequences.

In 2001, the Council of Europe (CoE) adopted its Convention on Cybercrime Treaty, also known as the "*Budapest Convention,"* which recognizes certain activities to be cybercrimes (CoE, 2001):

- The illegal access to a computer system with the intent of obtaining computer data.
- The illegal interception of private (non-public) computer data traffic to, from, or within a computer system, "including electromagnetic emissions from a computer system carrying such computer data."
- The illegal interference on computer systems for damaging, deleting, deteriorating, alternating, or suppressing computer data without being eligible.

- The serious preventing, without right, of the function of a computer system by “inputting, transmitting, destroying, erasing, deteriorating, modifying or suppressing computer data.”
- The international input, modification, erasure, or suppression of computer data, resulting in “inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic (forgery).”
- Any fraudulent or dishonest action such as interference, input, modification, erasure, or suppression of computer data for profit purposes. The production and distribution of child pornography material, distribution, or transmission, offer or making it available, the procurement, possession in a computer system or on a computer-data storage medium.

In the effort to eradicate cybercrime, the European Union has adopted a series of laws while encouraging operational cooperation as an integral part of its strategy for cyber security.

11.2.2 Types of Cybercrime

We can consider three main categories of cybercrimes. Cybercrimes in which the computer is the target, cybercrimes in which the computer is the tool to commit illegal activities, and cybercrimes in which computers are just facilitating other crimes.

11.2.2.1 Computers as a Target

In these cases, a computer or information system becomes the target of a cyber-attack. In other words, all these illegal activities in which the perpetrators engage in and attack a computer or an information system to obtain access, steal or destroy data, etc. Some of the main types of such cybercrimes are:

Hacking or Cracking

This usually refers to a crime on a person’s computer that violates sensitive and personal information. The criminal uses various different tools to enter the computer without the owner's consent. The hacker has access and attacks from a remote location. Hacking will be analyzed further in paragraph 2.3.

Malicious Software (Malware)

Malware is referred to by numerous names: malicious software, malicious code, and malcode. McGraw and Morrisett (2000) define malicious code as “any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system.” Malware cases mainly include attacks made by viruses, worms, and Trojan horses. A computer virus is a code duplicated by inserting itself into other programs. A worm replicates itself by its code independently of any other software or program. The main distinction between a virus and a worm is that a worm does not need a host to cause harm, it is independent. Worms can also spread via network or internet connections aiming to infect and cause harm to as many computer systems connected to the network as possible. Trojan horses are associated with accessing and sending illegal information from their host. Such Trojan horses can be treated as spyware as well. A Trojan horse is a special kind of malware embedded by a specialist in an application or system. The application or system may perform a function, such as giving some information about the weather; however, it performs other unauthorized malicious actions like stealing and sending a password to a remote thief or attempting to damage the system resources physically. Known types of destructive malware have been Cryptowall (2014), Cryptolocker (2013), CryptoDefense (2014), TorrentLocker (2014), Wannacry, Petya, etc.). Such software is used on the Internet, and its main objective is to harm or to prohibit computer operation in a network.

Ransomware

Ransomware is software that infects a computer and restricts users' access until a ransom is paid to unlock it. Some entities impacted by ransomware are hospitals, school districts, state and local governments, law enforcement agencies, and small and large businesses. The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and losing access to personal and often unique items, such as family photos, videos, and other information.

When seeing an email addressed to them, victims will open it and click on an attachment that appears lawful, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. The email may also contain a legitimate looking URL, but when the victim clicks on it, they are directed to a website that infects their computer with malicious software.

Since the inflection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network the victim's computer is attached to. Users and organizations are unaware they have been infected until they can no longer access their data or until they begin to see the computer advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom. Ransomware attacks are not only proliferated. Some years ago, ransomware was normally delivered through spam emails, but because email systems got better at filtering out spam, cyber criminals turned to spear phishing emails targeting specific individuals. In newer instances of ransomware, some cyber criminals are not using emails at all.

Denial of Service (DoS or DDoS)

A Denial-of-Service attack is meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected. DoS will be analyzed further in paragraph 3.3.4 of the next chapter 12.

Other types may be email bombing, data diddling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, etc.

11.2.2.2 Computers as An Instrument

Although computers can be the target of a perpetrator, they are often used as an instrument in order to commit illegal activities. In this category fall types of cybercrimes such as:

Online Fraud

It is a type of deception that involves hiding information or providing incorrect information to trick victims out of money, property, and inheritance. Online fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions committed in cyberspace. They can be business fraud, credit card fraud, internet auction fraud, investment schemes or non-delivery of merchandise.

Phishing and Spear Phishing

Phishing is a social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to

installing malware, freezing the system as part of a ransomware attack, or revealing sensitive information (Imperva, n.d).

Spear phishing targets a specific person or enterprise, instead of random application users. In this case, the scammers use specific information related to their target, such as name, workplace, or telephone number to make the victim think they have some connection to the sender. It is a more in-depth version of phishing that requires special knowledge about an organization, such as its power structure (Chawski, 2015).

Pharming

Pharming is a phishing attack type that differs from all the mentioned above: Pharming does not occur by sending emails but by attacking the domain name system (DNS) cache. The DNS servers usually convert alphabetical website names into a specific numerical IP address. Every website name is associated with an IP address that locates the computer services and devices. During a pharming attack, the victims are directed to a harmful site even though they enter the correct website name; the attackers change the IP address of the website to redirect the victims to the website they want.

Identity Theft (Clough, 2010)

This occurs when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

Spamming

It is sending multiple unsolicited messages to many recipients for commercial advertising or non-commercial proselytizing, for any prohibited purpose (especially the fraudulent purpose of phishing), or simply sending the same message multiple times to the same user.

Spoofing

Spoofing happens when someone or something forges the sender's information and pretends to be a legitimate source, business, colleague, or other trusted contact to gain access to personal information, acquire money, spread malware, or steal data (Cisco, n.d.).

11.2.2.3 Computers as Facilitators

In this category belong all types of cybercrimes where a computer's involvement is less significant. In these cases, computers were neither the target nor the instrument to perpetrate them. This category includes cases in which a computer is used in the perpetration of a crime; however, its involvement is so trivial that it does not rise to the level of being integral to the commission of the crime (Brenner, 2010).

Examples here could be trading sex material, exchanging child abuse material, drug talk, and trade, etc. In all these cases, the crime itself exists from the beginning; however, cyberspace plays the role of the facilitator, enabling the communication and the sharing of illegal information and the trading of illegal materials. Cyber Stalking (which will be analyzed in Chapter 14) is a kind of online harassment using Internet communication channels. In these cases, criminals know their victims and would implement this fraudulent process one way or another; however, they use the Internet to stalk.

11.2.2.4 Two Cybercrime Cases

Two representative cases of incidents of the categories described above, a botnet and a phishing case, are presented below:

The Coreflood Virus Botnet Case

Botnets are computers infected by a virus and remotely controlled by an attacker. They can be used to retrieve illegal funds, hijack identities, and commit other cybercrimes and illegal actions. The "*Coreflood*" virus investigation began in April 2009 when a Connecticut-based company clarified that the *Coreflood* virus had infected many computers on its premises. This program allowed cybercriminals to steal personal, financial, and encrypted information by recording every unsuspecting user's keystroke. This virus infected mostly devices running Microsoft Windows operating systems. The infection starts when users open an infected email; thereby, the criminals gain control of the malware remotely. On April 13, 2011, the US Department of Justice received warrants to turn off the "Coreflood" botnet by seizing the five US servers used by the hackers. By interrupting the botnet servers' operation, the FBI Bureau's IT specialists could prevent "Coreflood" from sending stolen information to the cyber thief. However, the computers which were infected remained in the same condition. This is the reason why the FBI worked with private-sector partners that worked on updates of the antivirus programs and Windows Live Updates. It also worked towards releasing a command that stops the virus from running and authorized the Internet Service Providers (ISPs) to inform users that their computer was infected.

The HSBC Bank phishing in India

In this incident, cybercriminals designed a "replica" of the official website of the HSBC bank to deploy phishing practices. The website's main target was to ambuscade the users (employers of the bank) and convince them to text and submit their credentials (username and password) using phishing mail. One hundred twenty employees of the HSBC bank were targeted by receiving phishing emails containing a fake link embedded in the body of the e-mail and informing them about a risk involving their account. This link was associated with their original Customer ID and Password. The email informed them that the bank's IT department had brushed up on the employees' accounts and had indications of some third party trying to access and obtain information from them.

The concern for securing the network clients' privacy was highlighted in the email informing that services associated with the employees' accounts have been recently deactivated for fear of breaching. Finally, recipients were requested to log in with the last available credentials to prove the account's authenticity and reactivated it. After logging in, a message was sent informing that the reactivation process had been successful. A total of 44% of the employees responded to the email, providing their credentials, confidential data, and granting access to their accounts. These activities are consistently ranked as the top choices for cybercriminals, in which victims are deceived, and a significant proportion of individuals who receive such emails or messages (e.g., Viber) willingly divulge their sensitive information.

11.2.3 EU Response to Cybercrime

Attacks in cyberspace have caused humanity to move to a state of anticipated risk (van Loon, 2002). According to Joost Van Loon, risk is always potential, waiting to happen or become real. Nowadays, attacks demonstrate vulnerabilities in the online world and the potential damage that can be caused in various fields.

Personal identifiable information (PII) of internet users is like one's fingerprint. They depict profiles that can be accessed by third parties, essentially violating privacy. Therefore, a realistic approach considers that privacy does not really exist in cyberspace today. Despite the indisputable fact that progress has been made in making privacy protection laws in cyberspace, cybercrime is not easy to come out from the root, at least not yet.

In an effort to eradicate cybercrime, the European Union has adopted a series of laws while encouraging operational cooperation as an integral part of its strategy for cyber security. Very early, in 1995, the European

Union (EU) adopted the Data Protection Directive (officially Directive 95/46/EC), which considers the processing of personal data within the European Union, to be an important component of EU privacy and human rights law. In Europe, the right to privacy is a highly developed area of law. The United States Department of Commerce created the International Safe Harbour Privacy Principles certification program in response to Directive 95/46/EC. The European Commission has also set up the "*Working Party on the Protection of Individuals with regard to the Processing of Personal Data*," commonly known as the "*Article 29 Working Party,*" whose aim is to advise about the level of protection in the European Union and third countries.

In 2013, the EU adopted a direction for the attacks against information systems, to deal with large-scale cyberattacks. EU has also been extremely sensitive to issues of exploitation of children and sexual abuse, so, in 2011, a direction to combat child pornography on the Internet was issued, trying to face problems such as grooming (analyzed in Chapter 14).

At the same time, the EU requests the member states individually to strengthen their national legislation on cybercrime and introduce criminal penalties that are even tougher for cybercriminals. Moreover, when malicious actors commit cybercrime or deploy cyberattacks, many electronic traces and data transfer processes affect and pass through more than one country. Even in domestic transfer processes within a country, data may go outside the borders of the originated country, be transmitted over routers, and return their destination. That creates jurisdiction problems and challenges, such as difficulties in interpreting and defining cybercrimes because, apart from the relevant legislation at a national level, international laws and regulations are necessary to cover and facilitate such cases. Besides, acts on the internet that are legal in the source country may be illegal in the destination and other involved countries (Gercke, 2012).

Unlike traditional crime, which is usually perpetrated in one geographic location, cybercrime has global dimensions because it emerges online without linkage to any geographic location. Therefore, a coordinated global response is required. Cybercrime investigations need international cooperation from law enforcement agencies in all involved countries. Most countries do not allow investigations conducted by different countries within their territory; therefore, cooperation based on the principles of mutual legal assistance is necessary. However, the requirements and time needed to collaborate with foreign law-enforcement agencies, especially when digital evidence and other electronic traces vital to the investigation are likely to be lost or deleted, hinder the whole investigation procedure. Thus, in that direction, harmonizing cybercrime related laws and the speed of international cooperation will improve the investigation procedure (Gercke, 2012).

In January 2013, the European Commission established the European Cybercrime Centre. This service acts as a focal point for the fight against cybercrime in the EU Member States by coordinating the collaboration of European experts towards this end. However, it also investigates cyber-related crimes in the Member States (MS). Moreover, it is a collective voice for establishing European law by conducting campaigns to eradicate the phenomenon of cybercrime. The challenge here that lawmakers face is that Internet technologies are changing fast, and there is a need to continuously adapt laws to new technological capabilities that criminals may use for their new advanced schemes. However, it takes time to update national criminal law to prosecute the new forms of online cybercrime, not to mention how much it will take for international law to harmonize domestic legislation in different countries. Every delay in law adjustments, even from one country, may have disastrous consequences for the investigation process, with law enforcement agencies being unable to examine the case further. In general, the whole adjustment process has three basic steps:

- The recognition that a new form of offense has appeared, using the latest technological developments that create the need for specific legislation.
- The identification of gaps in the law (e.g., penal code) that do not cover the details of the new variety of offense.

- The drafting-writing of the new legislation (Gercke, 2012).

Undoubtedly, many countries are working on adjusting their legislation to new forms of offenses; however, the main challenge is how fast they can do it before it is too late. Conclusively, a multidimensional and comprehensive strategic approach should be put in place (Zerzri, 2017):

1. **Legislative Framework:** It is important to enact an Internet regulation concerning the various threats, including the monitoring of social media platforms or other communication channels to detect, respond, and deter any suspicious activities. Monitoring mechanisms showing respect to the freedom of expression and privacy can be weapons for effective tracking of possible threats.
2. **National Partnerships:** As stated above, it is very important to strengthen cooperation between all stakeholders of the public and private sector, that is, the government, including security forces, cyber security experts, telecommunication network operators, internet service providers, and civil society. Moreover, it aims to strengthen stakeholders' capacities (digital security specialists, law enforcement agencies, and the judiciary), as well as civil society, by raising awareness regarding digital security to prevent threats.
3. **National Strategies:** It has become indispensable to analyze digital threats accurately, that is, studying their objectives, motivation and the resources used, monitoring strategies, and activities, and analyzing and evaluating risks for any possible damage they could cause. In parallel, it is necessary to formulate, for instance, a National Cyber Security Strategy that aims to develop and enhance digital security to be secure and resilient to digital threats. The strategy must outline the objectives and the implementation plan to help create the conditions for all stakeholders to work effectively on digital security and raise awareness and knowledge throughout society. A National Response and Risk Management Strategy should be implemented to identify and characterize digital threats, assess the vulnerability of critical assets to those threats, determine the risk, identify ways to reduce those risks, and prioritize risk reduction measures.
4. **International Cooperation:** Actions should be coordinated, and agreements should be signed with other states regarding crimes to regulate the prevention and treatment of these crimes and the exchange of information and evidence.

The ongoing EU Cybersecurity Strategy has included several legislative actions against cybercrime, such as:

- 1995 – the Data Protection Directive 95/46/EC, which regulates the processing of personal data within the European Union and is an important component of EU privacy and human rights law.
- 2002 – the ePrivacy Directive, whereby providers of electronic communications services must ensure their services' security and maintain client information's confidentiality.
- 2011 – Directive 2011/93/EU on combating the sexual exploitation of children online and child pornography, which better addresses new developments in the online environment, such as grooming (offenders posing as children to lure minors for sexual abuse).
- 2013 – Directive 2013/40 on attacks against information systems, which aims to tackle large-scale cyber-attacks by requiring Member States to strengthen national cyber-crime laws and introduce tougher criminal sanctions.
- 2019 – Directive 2019/713 on combating fraud and counterfeiting non-cash means of payment, which defines the fraudulent behaviors that the EU States need to consider as punishable criminal offenses.

The European Commission has also set up the "*Working Party on the Protection of Individuals with regard to the Processing of Personal Data,"* commonly known as the "*Article 29 Working Party.*" This Working Party advises about the level of protection in the European Union and third countries.

11.2.4 US Response to Cybercrime

In response to the European Union Directive 95/46/EC, the United States Department of Commerce created the International Safe Harbor Privacy Principles certification program. The United States has also adopted a series of acts to protect against certain types of cybercrime very early. Some of them are listed below.

Communications Decency Act (CDA)

The Communications Decency Act of 1996 is an Act of Congress. The Act regulates pornographic material on the internet. The Act affects the internet by regulating indecency and obscenity. The provision of the Act is:

- to promote the continued development of the internet and other interactive computer services and other interactive media,
- to preserve the vibrant and competitive free market that presently exists for the internet and other interactive computer services, unfettered by Federal or State regulation,
- to encourage the development of technologies that maximize user control over what information is received by individuals, families, and schools who use the internet and other interactive computer services,
- to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material,
- to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment using computers.

Child Online Protection Act (COPA)

COPA is a US federal statute designed to control child pornography on the Internet by prohibiting Internet speech that is harmful to minors. According to the Act, "Material harmful to minors" includes any material that by "contemporary community standards" was judged to appeal to the "prurient interest" and that showed sexual acts or nudity (including female breasts). It does not apply to e-mail or chat-room communications. It applies to sexually explicit material that appears to depict minors, even if the people are actually over 18 or the images are computer-generated and do not depict living people. The Act has been challenged because it violates the constitutional protection of free speech. After several court challenges, COPA was held unconstitutional and never became effective.

Digital Millennium Copyright Act (DMCA)

DMCA (1996) is a US federal law relating to copyright. The Act implements the World Intellectual Property Organization (WIPO) treaties of 1996. The Act criminalizes:

- The production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.
- The act of circumventing an access control, whether or not there is actual infringement of copyright.

The Act penalizes the infringement of copyright on the internet and mainly encompasses five titles:

- Copyright and Performances and Phonograms Treaties Implementation Act of 1998.
- Online Copyright Infringement Liability Limitation Act.
- Computer Maintenance Competition Assurance Act.
- Miscellaneous provisions relating to the functioning of the Copyright Office.
- Vessel Hull Design Protection Act.

Children's Online Privacy Protection Act (COPPA)

A right to privacy has been based on the US Supreme Court's examination of the Constitution. Case law has interpreted the US Constitution to protect personal freedoms, such as the right to privacy under the 14th Amendment. The 1st, 4th, and 5th Amendments also provide some privacy protection, although in all cases the right is narrowly defined. There is also the statutory right to privacy, which limits access to personal information. The Federal Trade Commission (FTC) is responsible for enforcing this statutory right of privacy. However, the right to privacy must be balanced against the state's compelling interests. Such compelling interests include promoting public morality, protecting the individual's psychological health, and improving the quality of life.

In the information mining age, many entities collect personal data, such as name, address, email, demographic info, social security number, IP address, and financial information. In many cases, this information is then provided to third parties for marketing purposes. Fraud and identity theft frauds have increasingly generated the right to privacy legislation requiring disclosure of information collection practices, opt-out opportunities, and internal protections of collected information.

Children's Internet Protection Act (CIPA)

CIPA is a US federal law designed to limit the collection and use of personal information about children by the operators of Internet services and Websites. Passed by the US Congress in 1998, the law took effect in April 2000. It is administered and enforced by the Federal Trade Commission. CIPA is the first US privacy law written for the Internet. It was written specifically for Internet marketers who operate Websites visited by children under 13 and collect personal information from those kids. Its purpose is to regulate that collection.

Trading with the Enemy Act (TWEA)

TWEA is a United States law restricting trade with countries hostile to the nation. The TWEA authorized economic sanctions against foreign nations, citizens and nationals of foreign countries, or other persons aiding a foreign country. The law allows the President to oversee or restrict any trade between the US and its enemies during war. The TWEA delegates to the President the powers of economic warfare during a time of war or any other period of national emergency.

11.3 The Deep and the Dark Web

It is widely known that the Internet is a global platform supporting the World Wide Web, an application that allows people to disseminate, share, and communicate ideas. It is less widely known that the Web is divided into three categories. These are the Surface web, the Deep web and the Dark web (**Figure 11.1**).

The Surface Web is the standard web that is visible to ordinary internet users. It is formed by websites indexed by common search engines, such as Google. These indexed pages are estimated to form a tiny percentage of the internet content users use daily. The vast available content is not accessible by ordinary search engines. This is called the Deep web, a portion of the web that is not visible to common users. Its content is not accessible at all unless the user has some sort of authorization or login credentials. The Deep Web usually stores personal information like organizations' and military data. It is a fact that all internet users use Deep Web all the time. Examples of Deep Web are internet banking, Netflix, webmail, databases and generally everything that is password or paywall protected.

Figure 11.1 *Surface Web, Deep Web and Dark Web (Source: Hackers League).*

The small portion of the Deep Web, which can only be accessed by special software or browser with a suitable decryption key, is called the Dark Web or Dark net. The BBC once defined the Dark web as "anonymous, virtually untraceable global networks used by political activists and criminals alike."

This structure of the web will be analyzed in the following paragraphs.

11.3.1 The Web and the Surface Web

The World Wide Web, as a subset of the internet, consists of the pages that can be accessed using a web browser. Many wrongly assume that the web is a synonym for the internet and use these terms interchangeably.

The internet generally refers to the collection of networks that link computers together. However, a technical definition would describe the internet as the global information system that:

- is logically linked by a globally unique address space based on the Internet Protocol (IP) or subsequent extensions or follow-ons,
- can support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols,
- provides, uses, or makes accessible, publicly or privately, high level services layered on the communications and related infrastructure described herein" (Lister et al., 2009).

Therefore, the term internet refers to the global network that offers the vehicle supporting the web information. Web pages are produced using a language named Hypertext Markup Language that allows for the creation of hyperlinks in them, allowing users to click around and surf the net by jumping from webpage to webpage. Browsers such as Internet Explorer, Google Chrome, or Mozilla Firefox are used to download the HTML code of the web pages from web servers and construct the graphical interface of each page, presenting it to the end user's screen. The protocol that supports the whole operation is the hypertext transfer protocol (HTTP). Therefore, the World Wide Web is a web of interlinked HTML pages accessible online. However, as mentioned earlier, it contains three layers, the Surface, Deep Weband Dark web.

The Surface web is the visible part (the tip) of the iceberg of **Figure 11. 2** containing all the content indexable by search engines: Websites, email pages, Social Networking sites, etc. It is accessible via web crawlers and search engines like Google, Bing, or Yahoo. Search engines crawl and index the web pages available on the web to make them available for users. They then rank these websites to display the most relevant results to a user, according to their previous history and profile, basing them on a complicated algorithm that may take more than 200 factors into account. This segment of the internet comprises

approximately 4% of the overall content and offers relatively limited anonymity, as users are typically identified by their IP addresses. Additionally, the Surface Web is alternatively referred to as the Common Web, Clearnet, Visible Web, or Lightnet. The remaining 96% corresponds to the residual section of the iceberg, commonly known as the Deep Web.

11.3.2 The Deep Web

The Deep web is a part of the invisible, underground web iceberg that an average user cannot access. This is so because it contains data not crawled and indexed by search engines. As mentioned, one can access the Deep web only if one has the authorization or login credentials. The data stored in the Deep Web ranges from private information such as military or any organization's data to financial records, academic databases, legal dossiers, medical records, social media profile information, and scientific and e-government records (**Figure 11.2**). For example, personal emails do not appear in search engines; otherwise, everyone would have access to them with a simple Google search. The same happens with personal e-banking, social media account settings, or the management interface of a site. It is, therefore, realistic that users often visit pages that objectively belong to the Deep web.

Furthermore, the Deep web also includes pages we can only access to through a link. For example, YouTube videos that are labelled "*unlisted.*" Anyone with a video link can view it normally, even if they do not have a YouTube account. However, unlisted videos are never displayed on YouTube searches, or suggested next to other videos. They are entirely invisible to users who do not have the link.

Accessing the Deep web is not something illegal. It owes its existence to the fact that certain confidential data stored need protection and require special authorization or credentials to access them. For instance, People Search Engines such as Pipl or MyLife extract data from databases that normal search engines cannot index when looking up an individual. Also, some engines give access to the academic section of the web about scholarly articles. These search engines, such as Google Scholar, the Library of Congress, and JSTOR, enable searching through otherwise-isolated records of articles and books. Webpages that are not indexed by traditional search engines may be categorized as one or more of the following (Hamilton, 2003):

- **Dynamic Content**: dynamic webpages that someone can access to only by submitting forms with their data.
- **Contextual web**: pages with dissimilar content for different access contexts (e.g., variables of IP addresses).
- **Private web**: pages that require a username and password to be accessed.
- **Limited Access Content**: sites that have limited access to their pages.
- **Scripted content:** pages accessible via JavaScript links and dynamically downloaded content from web servers via Flash or Ajax solutions.
- **Non - HTML/Text Content**: textual content encoded in multimedia (image or video) files or special file formats not handled by search engines.
- **Unlinked content**: pages that are not linked to other pages can prevent web crawling programs from accessing the content. This content is referred to as pages without backlinks. Also, not all backlinks from searched web pages are always detected by search engines.
- **Web archives**: Web archival services such as the *Wayback Machine* allow users to view archived versions of webpages over time, including websites that have become difficult to access and are not indexed by search engines such as Google.

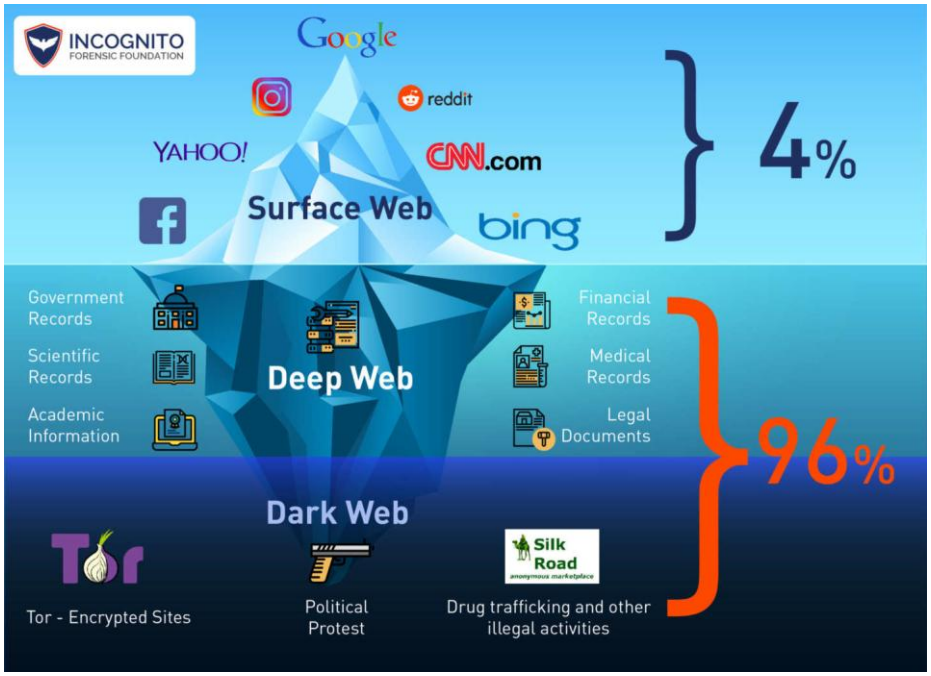


Figure 11.2 *The Layers of the Web–Surface Web, Deep Web and Dark Web (Source: Incognito Forensic Foundation).*

Commercial search engines have begun exploring alternative methods to crawl the Deep Web. The *Sitemap Protocol*, first developed and introduced by Google in 2005, is a mechanism that allows search engines to discover Deep Web resources, allowing web servers to advertize the URLs that are accessible on them, and therefore automatic discovery of resources that are not directly linked to the Surface Web.

11.3.3 The Dark Web

11.3.3.1 Definition

The Dark Web refers to information and resources found within the deeper layers of the Internet, requiring specialized software or other mechanisms for access. The Dark Web is a small part of the Deep web. These two terms are usually interchangeable, but in fact, they have different meanings. Further, it is underlined that the Dark web is constituted by the darknets, namely by small-scale friend-to-friend or peer-to-peer networks or large-scale networks, such as Tor. Contrary to the unencrypted nature of the Surface Web, the Dark Web allows encryption and, hence, anonymization. The whereabouts and personal information of Dark Web users remain undisclosed due to the inability to trace them, which can be attributed to the complex encryption system that resembles an "onion." Through this system, users' data is passed through multiple intermediary servers to safeguard their anonymity, making it impossible to decipher the transmitted information. This complicated scheme does not allow websites to track their visitors IPs while the visitors cannot get information about the host. So, communications on the Dark web are effectively encrypted and users can communicate confidentially. Because of these features, the Dark web is used for several illegal activities (Fahad, 2018), such as cyberterrorism (analyzed in Chapter 12).

One can access the Dark web using special software and an anonymizing browser, with "*Tor*" being the most popular. Tor is commonly known as an "Onion" browser and contains multiple layers that enable a user to remain completely anonymous i.e. it neither traces the user's IP address/location nor records any detail.

The Tor browser serves the user's webpage requests through a chain of proxy servers that renders the IP address untraceable and unidentifiable. The Tor network works encrypts all messages and content at every point. This makes tracking their point of origin or occurrence difficult and almost impossible.

Overall, the Dark web can be defined as "*the part of the Deep Web that has been intentionally hidden and is inaccessible through standard Web browsers. Dark Websites serve as a platform for Internet users for whom anonymity is essential, since they not only provide protection from unauthorized users but also usually include encryption to prevent monitoring*" (Chertoff & Simon, 2015).

11.3.3.2 Malicious Activities

The dark side of the internet was anticipated. Abuses such as the illegal sharing of music files, IT interruptions, etc., are important consequences of the spread and advance of information technology. Their implications, though, represent a lighter shade of the dark side of the internet. The truly harmful aspects of the Internet are represented by activities that take place on the Dark web (George et al., 2016). The Dark Web facilitates virtual criminal activities, which closely resemble traditional criminal activities but are carried out through digital means. The utilization of the Dark Web provides criminals with numerous novel avenues to engage in diverse forms of criminal behavior. In this context, illegal trade of drugs, weapons, and exotic animals, stolen goods and information, murders, hacktivism, illegal financial transactions, the hidden wiki, human experimentation, heist, gambling, pedophilia, arms trafficking, Illegal trading of human organs, Hitmen and terrorism are among the leading criminal activities that can be facilitated by the Dark Web (Chertoff & Simon, 2015). Some of these illegal activities are outlined below:

Human Trafficking

According to Homeland Security Investigations, a Department of Homeland Security Agency in the US responsible for human trafficking enforcement, there are millions of men, women, and children all around the world who are victims of human trafficking every single day. The United Nations has estimated that human trafficking profit is $150 billion a year. Dark web has made human trafficking easier to propagate and conceal because of its anonymity. Internet advertisements are usually used to entice potential trafficking victims and solicit those victims of sex trafficking. Also, illicit forums discussing sex trafficking and services are hidden in the Dark web. Because sites are not indexed, it is very challenging for law enforcement to identify the illegal behavior hidden within the Dark Web.

Illicit trade

Darknet markets or black markets—also known as cryptomarkets—provide a largely anonymous platform for trading illicit goods and services. It is estimated that approximately two-thirds of the offers are drug related. Drug sales on these darknet markets, although modest when compared to the overall retail drug market, are significant and appear to be expanding. The profit of these markets in the European Union is estimated to be 18 million euros, while the profit of both online and retail drug markets is 80 or 90 million euros. The system is designed to be relatively safe for the buyers, and in most cases, it is more likely to be arrested for buying drugs in real life than online. The motive for buying drugs on the Dark Web is peoples' assumption that the Dark net offers a safe environment and that the quality of the product is better. According to Alexis Goosdeel, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) Director, this perception is not necessarily wrong, but is not always guaranteed. If what it is said is true, then there may be a negative side effect regarding health. When the product is pure, it means that it contains a high dose of the drug, and that makes it more dangerous. Another motive for buying drugs online is the wide range the Dark net offers and the convenience of buying a product easily and quickly. As a result, the online trade in illicit goods and services was recognized as one of the engines of organized crime and a critical threat to the safety of EU citizens.

Guns

Every year, illegal trafficking in small arms and light weapons is estimated to be worth approximately between $1.7 and $3.5 billion, equivalent to around 10 to 20 percent of the legal arms trade. Increasingly, all sorts of

guns, from pistols to Kalashnikovs, are finding their way onto the Dark net. Last year, a Global Financial Integrity study estimated that the average price for the latter on the Dark net is in the $2,800 to $3,600 range. According to a study from RAND Corporation, the Dark net is increasing the availability of firearms for similar prices as those available on the regular black market out on the streets. It also found that the United States is the most common source country for arms sales on the Dark net. Despite that, according to the data from 2017, Europe represents the largest Dark net market for firearms, with revenues about five times higher than the United States, while on a country-by-country basis, Denmark had the second highest share of Dark net firearm vendors last year at 12.98 percent while Germany comes third with 5.31 percent.

Silk Road

A well-known example of an anonymous marketplace that used to sell all kinds of illegal products, such as drugs or weapons, and thrived on the Dark web is Silk Road. Founded in 2011, Silk Road adopted an Amazon-like platform for vendors to buy and sell goods using Bitcoin. This crypto-currency enables two parties to conduct a trusted transaction without knowing each other's identity. The Silk Road's consumer-friendly approach and guaranteed anonymity were the keys to quickly becoming the go-to contraband website. By the time it was shut down in 2013, the marketplace had accumulated 1,400 vendors and 957,079 registered users, and it had brokered more than 1.2 million transactions worth $214 million. After the Silk Road's takedown, many illegal marketplaces, such as Agora and AlphaBay, have successfully taken over the Silk Road's space as their business is expanding.

Noteworthy is the use of the Dark web for "*Black Hat Hacking."* Hackers not only use the Dark Web for hacking but also for selling the spoils of hacking, such as user credentials, financial information, or corporate data. It serves as the preferred platform for the illegal trading of government or scientific databases, malware, drugs, exotic animals, banned movies or literature, fake documents, and much more.

To sum up, services that someone can meet on Dark Web are:

- **Ransomware**: The Dark Web is involved in certain extortion related processes. It is common to find data from ransomware attacks on various Dark Websites.
- **Botnets**: A botnet is collection of Internet-connected devices, each with one or more bots installed. Botnets can be employed to execute distributed denial-of- service attack, steal data, send spam, and grant the attacker to access to the device and its connection.
- **Dark net markets**: Dark net markets facilitate transactions for illegal goods and typically use Bitcoin as payment. Some notable markets include: Silk Road, Sheep Marketplace, Empire Market etc.
- **Illegal pornography**: Popular markets include those featuring child pornography or revenge porn.
- **Hacking groups and services**: Hackers sell their services individually or as a part of groups (Holden, 2015), such as *xDedic*, *hackforum*, *Trojanforge*, *Mazafaka*, *dark0de* and the *TheRealDeal* Dark net market.
- **Bitcoin services**: Illegal operations on Dark Web are often completed using bitcoins, a currency chosen for its flexibility and relative anonymity.
- **Terrorism**: The Dark net is an ideal space for terroristic activity due to its anonymity, lack of regulation, social interaction, and easy accessibility.
- **Financing and Fraud**: Numerous carding forums, PayPal and Bitcoin trading websites, as well as fraud and counterfeiting services, are prevalent.
- **Hoaxes and not verified content**: Reports of crowdfunded assassinations and hitmen for hire exist, but these are believed to be exclusively scams.

- **Social media**: In the Dark Web, several social media Platforms emerge, resembling those on the Surface Web. An example is the Dark Web Social Network (DWSN) offering customizable pages, friends, like posts, and blog in forums.

In recent years, journalists, alternative news feeds, educators, and researchers have influences public opinion when speaking of the Dark net, highlighting the power and freedom of speech the Dark Web allows people to express.

11.3.3.3 Policing the Dark Web

While it is widely believed that the Dark Web promotes civil liberties, freedom of speech, privacy, and anonymity, prosecutors and government agencies express concern about the criminal activity that can deployed there. Policing involves targeting specific activities on the private web deemed illegal or subject to internet censorship. When investigating online suspects, police typically use tracing techniques to identify the origins of specific traffic. However, due to Tor browsers that create anonymity, this becomes almost impossible (Davies, 2020). Therefore, law enforcement has adopted other tactics to identify and apprehend those engaging in illegal activity on the Dark Web. Open-Source Intelligence (OSINT) refers to data collection tools that legally gather information from public sources.

In general, security services worldwide have started to develop specialized teams that focus on this aspect of cybercrimes. Some related reports on this issue include:

- In October 2013, the UK's National Crime Agency and GCHQ announced the formation of a "Joint Operations Cell" to focus on cybercrime. In November 2015, this team was tasked with tackling child exploitation on the Dark Web as well as other cybercrimes.
- Interpol started offering a specialized Dark Web training program in 2015, featuring technical information on Tor, cybersecurity and simulated Dark net market takedowns.
- The Congressional Research Service released an extensive report on the Dark Web in March 2017, noting the changing dynamic of how information is accessed and presented on it.
- In August 2017, cybersecurity firms, which specialize in monitoring and researching the Dark Web on behalf of banks and retailers routinely, started sharing their findings with the FBI and with other law enforcement agencies regarding illegal content.

11.3.3.4 Opportunities of the Dark Web

Despite the malicious activities in the deep or Dark Web there are instances in which this part of the Web can actually be useful and beneficial. After all, Dark Web also has a legitimate side, offering activities that comply with the law. Thanks to the anonymity that the Dark Web provides, many journalists and dissidents can communicate with each other and share their opinions without censorship.

Furthermore, the Deep Web enables the user to remain nameless and faceless. It can host open discussion forums that victims of violence and abuse leverage to share their stories on public forums. The Dark Net houses forums for victims of rape, racial and religious discrimination, rainbow communities, domestic violence, and much more. It allows them to share their grief and personal stories without the fear of identification or harassment.

The Dark Web can also serve as a means to circumvent persecution. In some countries s citizens face arbitrary subjugation based on factors such as sexuality or religion. The Dark Web offers opportunities for people to form communities in a less extensively policed forum, where they can share tips, tell their stories, express their opinions or plan to meet up in person. For example, individuals living in countries with oppressive regimes, like North Korea, may seek more freedom on the Dark Web. Therefore, individuals possess the ability to share their experiences in similar countries through blogs, reducing the risk of their identities being exposed

due to their capacity to take effective precautionary measures. Another role of the Dark Web is to provide a platform for whistleblowers who would otherwise face retaliation in the real world. It allows them to leave messages or documents without revealing their identities. A Dark Web service called "*Dead Man Zero"* even enables the automatic publishing of the user's secrets in case they are injured, jailed, or killed, automatically releasing secret information to a prescribed set of email addresses.

In the realm of literature, the Dark Web has a presence as well. Access to books can be restricted for various reasons, but the Dark Web offers ample opportunities to read books that may either be altered or entirely prohibited in the offline world. A well-known example is the original Grimm's Fairy Tales, which nowadays does not exist in any bookstore or library, but only on the Dark Web.

Through the Dark Web, people also have the opportunity to purchase certain gadgets and other electronic devices at lower prices than on the Surface Web. They can also find rare movies or book that were never officially released.

Eventually, the Dark Web offers the government a safe habitat to store sensitive data such as intelligence reports and political records. Above all, the Dark Web is often used by law enforcement agencies to intercept wrongdoers by posing as anonymous users on illegal sites.

11.3.3.5 Dark Web and Cryptocurrency

On the Dark Web one can find a plethora of goods to purchase, ranging from stolen art to drugs and even prostitutes. It is evident that such transactions cannot be implemented with ordinary currency online; the traders of such goods had to find a new way of transacting money. This is where Blockchain technology is introduced. A Blockchain is a growing list of data, called blocks, linked together using cryptography. Each block contains the cryptographic data of the previous block, a timestamp, and the transaction data. As each block is strongly linked with its precedent, all blocks together create a chain, and therefore, they are resistant to modification after being recorded because if the data on one block is altered, then the whole chain after that block would have to be altered accordingly. Blockchains are typically managed by peer-to-peer networks. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT) (Tewari, 2020).

The two biggest characteristics of Blockchain were anonymity and security, making it perfect for transactions on the Dark net. The problem before was that one could not really trust some created digital currency because there was no reinsurance that the creator of that digital currency would not just run away and steal all the wallets containing it. The digital currency designed to solve this problem was Bitcoin, which used Blockchain to its full potential. This meant that no one is in charge, and Bitcoin would be run by the people who use it (Tewari, 2020). This absence of central authority makes owners of Bitcoin remain anonymous.

An encryption program called Pretty Good Privacy (PGP) is used for communication between the transactors. This program provides cryptographic privacy as well as authentication for data communication. PGP can be used for encrypting, decrypting texts, such as e-mails, as well as signing them, while also being able to encrypt files, directories, and even whole disk partitions. It was developed by Phil Zimmermann in 1991.

Five steps that need to be taken when operating an illegal transaction involving the Dark Web and Cryptocurrency (Tewari, 2020). The first step is advertisement. When advertising illegal products or services on the Dark Web, a different approach has to be taken since known search engines cannot index content from the Dark Web. If the advertiser decides to build a Dark Web website to promote sales, then this information must be registered with a directory service provided on the Dark Web so potential buyers can find information, like domains, on the indexed part of the web. Another way of advertisement is for the Dark Web website to

be advertized on market platforms and/or general Dark Web search engines. The second step is discovery. Buyers tend to share access information with other buyers directly. However, some have to follow the leads of the seller's advertisement approach through search engines on the Dark Web or communities. The third step is negotiation. Here, the buyer and the seller discuss shipping, pricing, and payment methods. These can change depending on the type of product or service. The fourth step is payment. There are two payment options on the Dark Web. One is when a third-party person takes care of the payment, and the other is when the payment is made directly to the seller's cryptocurrency address. The fifth and final step is fulfillment. The seller completes the order like an e-commerce site on the indexed part of the web would do. The products have to be sold via the agreed delivery method.

On average, the daily transactions on the Dark Web are estimated between $300,000 and $500,000 (Chen, 2011). With the constant rise of strictness on GDPR and with the Dark Web and Cryptocurrency being the best techniques for concealing someone's identity, it would not come as a surprise that numbers will get ever higher in the future. Recent studies have shown that Bitcoin transactions alone have risen from $250 million in 2012 to $872 million in 2018, with a projected over a billion in the following years (Tewari, 2020).

11.4 Conclusion

Cybercrime has emerged as a burgeoning form of criminal activity in recent years, displaying various manifestations and effects on society. Today's criminals use high technological improvements to engage in highly sophisticated attacks. A collaborative strategy is required to effectively address the ever-changing nature of cybercrime. This entails engaging not only government entities, but also industry stakeholders and individual users. Additionally, it is crucial to take into account both international and national laws and regulations of all countries involved throughout the entire investigation, arrest, and prosecution process of the offenders. Beyond the Surface Web, which is easily accessed by everyone online, there is a deeper and much larger layer that cannot be accessed through a standard online search. This deep and intentionally hidden area of the internet, the Dark Web, can be used not only for legitimate purposes but also for criminal or other malicious activities (Finklea, 2015). Overall, the Dark Web is a massive black box that facilitates criminal activities (Weimann, 2016a).

Although the Dark Web primarily facilitates illicit activities, it does possess certain redeeming qualities. While the Dark Web can be a tool for pedophiles and extremists, it is also a tool for scientists, government officials, professors, and anyone who is just looking for privacy. The Tor, for example, began as an anonymous communications channel, and it still serves a valuable purpose in helping people communicate in environments that are hostile to free speech.

Nevertheless, security agencies need to coordinate internationally and develop and adopt modernized methods for tracking and eliminating criminal activities in today's multidimensional digital domain.

References

Ampatzis C., 2017. "Καλύτερα να μην μάθεις ποτέ τι συμβαίνει στο Dark Web." *ONEMAN*. Available at: https://www.oneman.gr/keimena/diabasma/megala_keimena/kalutera-na-mhn-matheis-pote-ti-symvainei-sto-dark-web.4851953.html [Accessed 17 January, 2018].

Anagnostopoulos C., 2017. "Τι Είναι το Deep Web και το Dark Web, Μύθοι και Αλήθειες." Pc Steps. Available at: https://www.pcsteps.gr/200164-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CF%84%CE%BF-deep-web-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF-dark-web-%CE%BC%CF%8D%CE%B8%CE%BF%CE%B9-%CE%B1%CE%BB%CE%AE%CE%B8%CE%B5%CE%B9%CE%B5%CF%82/ [Accessed 13 November, 2018].

Baggili I., 2010. *Digital Forensics and Cyber Crime*. Springer.

Barquet M., 2015. "5 Benefits Of The Deep Web." Dj Designer Lab. Available at: https://www.djdesignerlab.com/2015/07/5-benefits-of-the-deepweb/ [Accessed 18 December, 2018].

Bergman M.K., 2001. "White paper: the Deep Web: surfacing hidden value." *Journal of electronic publishing*, 7(1).

Bernik I., 2014. "*Cybercrime and Cyberwarfare*." Wiley.

Bregant J., and Bregant R., 2014. *Cybercrime and Computer Crime, The Encyclopedia of Criminology and Criminal Justice*, First Edition, Edited by Jay S. Albanese, John Wiley and Sons, Inc.

Brenner S. W., 2010. *Cybercrime, Criminal Threats from Cyberspace*. Praeger

Brinson A., Robinson A., and Rogers M., 2006. "A cyber forensics ontology: Creating a new approach to studying cyber forensics." *digital investigation*, 3, pp. 37–43.

Carr J., 2009. *Inside Cyber Warfare*. United States of America: Jeffrey Carr.

Carrier B., 2003. "Defining digital forensic examination and analysis tools using abstraction layers." *International Journal of digital evidence*, 1(4), pp. 1–12.

Casey E., *Digital Evidence and Computer Crime*, Elsevier, 2004.

Chen H., Chung W., Qin J., Reid E., Sageman M., and Weimann G., 2008. "Uncovering the Dark Web: A case study of Jihad on the Web." *Journal of the American Society for Information Science and Technology*, 59(8), pp. 1347–1359.

Chen H., 2011. "Dark Web: Exploring and Data Mining the Dark Side of the Web." *Integrated Series in Information Systems*, 30, 2012th edition, Springer.

Chertoff M., and Simon T., 2015. "The impact of the Dark Web on Internet governance and cyber security." Centre for International Governance Innovation and Chatham House.

Ciancaglini V., Balduzzi M., McArdle R., and Rösler M., 2015. "Below the Surface: Exploring the Deep Web." Forward-Looking Threat Research Team. Available at: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf [Accessed 5 January 2019].

Cisco, (n.d). "What Is Spoofing?" Cisco. Available at: https://www.cisco.com/c/en/us/products/security/email-security/what-is-spoofing.html [Accessed 21 January 2022].

Clough J., 2010. *Principles Of Cybercrime*. Cambridge University, 2010.

Combs C.C., 2017. *Terrorism in the twenty-first century*. Routledge.

Council of Europe, 2001. "Convention on Cybercrime," *European Treaty Series*-No.185, Budapest, 23.XI.2001.

Curtis G., *The Law of Cybercrimes and Their Investigations.* CRC Press.

Dashora K., 2011. "Cyber crime in the society: Problems and preventions." *Journal of Alternative Perspectives in the Social Sciences,* 3(1), pp. 240–259.

Davies G., (2020). "Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers." *The Journal of Criminal Law*. 84 (5): pp. 407–426. https://doi.com/10.1177/0022018320952557

Douglas T., and Loader B.D., 2000. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.

European Commission, 2013. "High Representative of the European Union for Foreign Affairs and Security Policy." Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.

Fahad S., 2018. *Dark Web: Dark Side of Internet*." Shah Fahad.

Finklea K. M., 2015. "Dark Web." Congressional Research Service.

Furnell S., 2002. *Cybercrime*. United Kingdom: Pearson Education.

George J., Derrick D., Harrison A., Marett K., and Thatcher J., 2016. "The Dark Internet: Without Darkness There is No Light." *Proceedings of the Twenty-Second Americas Conference on Information Systems*, San Diego, California, August 11-13.

Gercke M., 2011. "Understanding cybercrime: a guide for developing countries." *International Telecommunication Union* (Draft), pp. 89, 93.

Gercke M., 2012. "Understanding Cybercrime: Phenomena, Challenges and Legal Response." *ITU*, 2012.

Ghosh S., and Turrini E., 2010. *Cybercrimes: A Multidisciplinary Analysis*. Springer.

Gilbert K., and Stephenson P., 2013. *Investigating computer-related crime* CRC Press.

Glenny M., 2011. *DarkMarket*. London [i.c.]: Misha Glenny.

Goodman M., 2008. "An Introduction to Cyber Crime and Terrorism: Problems and the Challenges" [online]. Available at: https://www.intgovforum.org/cms/workshops_08/IGF_dimensions_Marc-Goodman.pdf [Accessed 19 December 2018].

Gordon S., and Ford R., 2006. "On the definition and classification of cybercrime." *Journal in Computer Virology*, 2(1), pp. 13–20.

Gunjan V.K., Kumar A., and Avdhanam S., 2013. "A survey of cyber crime in India." *In Advanced Computing Technologies* (ICACT), 2013 15th International Conference on (pp. 1–6). IEEE.

Hamilton N., 2003. "The Mechanics of a Deep Net Metasearch Engine." In Isaías, Pedro, Palma dos Reis, António (eds.), *Proceedings of the IADIS International Conference on e-Society*, pp. 1034–6.

Hasbi A. H., and Mahzam R., 2018. "Cryptocurrencies: Potential For Terror Financing. RSIS Commentaries," No. 075, *Singapore: Nanyang Technological University*.

Holden A., (2015). "A new breed of lone wolf hackers are roaming the Deep Web – and their prey is getting bigger." *International Business Times*, [Accessed 19 June 2018]

Idika N., and Mathur A.P., 2007. "A survey of malware detection techniques." Purdue University, 48.

Imperva, (n.d). "Phishing attacks." Imperva. Available at: https://www.imperva.com/learn/application-security/phishing-attack-scam/ [Accessed 21 January 2022].

Joshua M., 2017. "What are the pros and cons of the Dark Web?" Available at: https://www.quora.com/What-are-the-pros-and-cons-of-the-dark-web [Accessed 15 December 2018].

Kharpal A., 2018. "The 'Deep Web' may be 500 times bigger than the normal web. Its uses go well beyond buying drugs." CNBC. Available at: https://www.cnbc.com/2018/09/06/beyond-the-valley-understanding-the-mysteries-of-the-dark-web.html [Accessed 23 November, 2018].

Kiesbye S., 2010. *Does the Internet Increase Crime*? London: [i.c.]. Gale Cengage Learning.

Lamond G., 2007. "What is a Crime?" *Oxford Journal of Legal Studies*, 27(4), pp. 609–632.

Li C., Jiang W., and Zou X., 2009. "Botnet: Survey and case study." In innovative computing, information and control (icicic), *2009 fourth international conference on Innovative Computing, Information and Control,* pp. 1184–1187. IEEE.

Lister M., Giddings S., Dovey J., Grant I., and Kelly K., 2009. *New media: A critical introduction.* Routledge.

Liu J., Xiao Y., Ghaboosi K., Deng H., and Zhang J., 2009. "Botnet: classification, attacks, detection, tracing, and preventive measures." *EURASIP journal on wireless communications and networking*, 2009(1), Article number: 692654 (2009).

Marcella Jr. A., and Menendez D., 2007. *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes.*" Auerbach Publications.

Margot P., 2011. "Forensic science on trial-What is the law of the land?" *Australian Journal of Forensic Sciences*, 43(2-3), pp. 89–103.

Matt E., 2018. "What is the Dark Web and How to Access it." *Tech Advisor*. Available at: https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/ [Accessed 16 December, 2018].

McGraw G., and Morrisett G., 2000. "Attacking Malicious Code: A Report to the Infosec Research Council," IEEE Software 17(5), September/October 2000, pp. 33–41. Malicious code is a side effect of bad software.

NCA Strategic Cyber IndustryGroup, 2016. "Cyber Crime Assessment." Version 1.2, July 7th, 2016.

Papanikolaou A., Vlachos V., Papathanasiou A., Chaikalis K., Dimou M., and Karadimou M. 2013. "Cyber crime in Greece: How bad is it?" *Telecommunications Forum* (TELFOR), 2013 21st (pp. 1–4). IEEE.

Papathanasiou A., Papanikolaou A., Vlachos V., Chaikalis K., Dimou M., Karadimou M., and Katsoula V., 2013. "Legal and social aspects of cyber crime in Greece." *International Conference on e-Democracy*, pp. 153–164. Springer, Cham.

Park H., Cho S., and Kwon H.C., 2009. "Cyber forensics ontology for cyber criminal investigation." *In International Conference on Forensics in Telecommunications, Information, and Multimedia* (pp. 160–165). Springer, Berlin, Heidelberg.

Parker D. B., 1976. *Crime by Computer*, Scribner.

Putnam T. L., and Elliott D. D., 1999. "International Responses to Cyber Crime." Available at: http://media.hoover.org/documents/0817999825_35.pdf [Accessed 19 December 2018].

Reyes A., Brittson R., O'Shea K, Steele J., Hansen J.R., Captain Benjamin R., and Ralph T., "Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors." Syngress, 2007.

Sachan A., 2012. "Countering terrorism through Dark Web analysis." *In Computing Communication and Networking Technologies* (ICCCNT), *2012 Third International Conference,* pp. 1–5. IEEE.

Sheils C., 2018. "THE DARK WEB and DEEP WEB: ACCESS THE SECRET INTERNET TODAY." *Digital.com*. Available at: https://digital.com/blog/deep-dark-web/ [Accessed 12 December, 2018].

Smith R. G., Holmes M. N., and Kaufmann P., 1996. "Nigerian Advance fee Fraud, Trends and Issues in Criminal Justice." AIC.

Taylor R., Fritsch E. J., and Liederbach J*., "Digital Crime and Digital Terrorism*. Pearson.

Tewari S. H., 2020. "Abuses of Cryptocurrency in Dark Web and Ways to Regulate Them." *SSRN Electronic Journal*.

Timothy S., 2018. "How to Access the Dark Web: Browsing Dark Web, TOR Browser, and Onion Websites." Web Hosting Secret Revealed. Available at: https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/ [Accessed 10 December, 2018].

Van Loon J., 2002. *Risk and Technological Culture: Towards a Sociology of Virulence*. London: Routledge. http://dx.doi.org/10.4324/9780203466384

Vlachos V., Minou M., Assimakopoulos V., and Toska A., 2011. "The landscape of cybercrime in Greece. Information Management and Computer Security." 19(2), pp. 113–123.

Walden I., 2007. *Computer crimes and digital investigations*. Oxford: Oxford University Press.

Wall D. S., 2005. "The Internet as a Conduit for Criminal Activity." 2005 (chapter rev. 2015) pp. 77–98, in April Pattavina (ed.), *Information Technology and the Criminal Justice System*, Sage Publications, 2005.

Wall D.S., 2007. *Cybercrime, The Transformation of Crime in the Information Age*. Polity Press.

Weimann G., 2017. "Going Darker? The challenge of dark net terrorism." Woodrow Wilson International Center.

Weimann G., 2016a. "Terrorist migration to the Dark Web." *Perspectives on Terrorism*, 10(3), pp. 40–44.

Weimann G., 2016b. "Going dark: Terrorism on the Dark Web." *Studies in Conflict and Terrorism*, 39(3), pp. 195–206.

Yar M, 2006. *Cybercrime and Society*, Sage Publications.

Yayla A. S., and Speckhard, A., 2017. "Telegram: The Mighty Application that ISIS Loves." *ICSVE Brief Reports*.

Zeviar-Geese G., 1998. "The State of the Law on Cyberjurisdiction and Cybercrime on the Internet." Gonzaga University.

Zerzri M., 2017. "The Threat of Cyber Terrorism and Recommendations for Countermeasures" [online]. Available at: https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf [Accessed 5 January 2019].

Chapter 12 Cyberwarfare and Cyberterrorism

Abstract

In Chapter 12, the concept of Cyberwar and its components is presented. Some of these components have already been presented in Chapter 11 within the context of Hacktivism, but here, the cyber threats are examined through the lens of national security. Methods like Web application attacks, Malware, DoS / DDoS Attacks, and Session hijacking are described here. Well known incidents are listed and analyzed, including the 2007 cyberwar against Estonia and 2008 against Georgia, the 2014-2018 cyberwar against Ukraine, the 2016 US Elections, etc. Moreover, the term "Cyberterrorism" is also highlighted here, as it refers to politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage at the national or international level. Historical events are listed here, and the ISIS' case is thoroughly analyzed.

12.1. Cyberwarfare

12.1.1 An Introduction to Cyberwarfare

Cyber warfare has been defined hacking by a nation or a state to attack the strategic or tactical resources of another nation or state's target. It targets any sensitive industry in the opponent's infrastructure. This includes military, defense, and weaponry manufacturers, weapon factories, the national electricity power grid, and many others (Forbes, 2017). In other words, cyber warfare is the actions of a nation or a state to invade another nation's computers or networks to cause damage (Clarke, 2010). Most developed countries can defend themselves from basic cyberattacks. However, experienced hackers supported by powerful countries can always deploy more multifaceted and, therefore, sophisticated attacks that can overpass such defense measures resulting in catastrophic civil or military damages (Forbes, 2013).

In cyber warfare, nations try to gain an advantage over each other and strategize for attack and defense. Usually, nations hire hackers to attack target computers and networks with sensitive resources of another country. This process resembles regular hacking: the hacker collects information on the target's system, figures out its weaknesses, and attacks the target to control or destroy it.

The concept of Cyber War is nourished by a well-founded fear, given the modern technologies, their capacities, and their vulnerabilities, and an imagination built up through apocalyptic rhetoric and fictions. The bestseller *"Cyber War: The Next Threat to National Security and What to Do About It,"* written by Richard A. Clarke in 2010, focuses on the American vulnerability in a fictional context of modern international conflict. In 1993, 25 years ago, John Arquilla and David Ronfeldt published a similar study entitled *"Cyberwar is coming!"* (Arquilla & Ronfeldt, 1993), where the two authors predicted new threats of non-state actors related to terrorists or activists. Cyberattacks can be envisaged as an augmentation of traditional military operations thanks to modern tools. In order to have a pertinent concept of cyber war, we have to set aside all the fictional imagery concerning this concept.

That is why the American Department of Defense defined Cyber Warfare as *"an armed conflict conducted in whole or part by cyber means. Military operations are conducted to deny an opposing force through the effective use of cyberspace systems and weapons in a conflict. It includes cyberattack, cyber defense, and cyber enabling actions."* This definition is interesting because it covers two different cases. The difference between a conflict *"conducted in whole"* and a conflict *"conducted in part"* by cyber means is probably not a difference of degree, but a difference of nature. Cyber means have already been used in past conflicts, for example, in 2007 in Georgia and later in Syria against ISIS.

Nevertheless, all military powers soon understood the need to be prepared or cyber defense and cyberattack. They now consider cyberspace a strategic operation domain, exactly like land, sea, and air. Nevertheless, the specificity is that cyberspace is not always a distinct field of operation but can complement traditional fields of operations and have effects in all dimensions of war. Thus, military powers are nowadays bound to develop new military technologies and strategies in a new arms race.

12.1.2 Modes of Operation and the Challenge to Reverse the Balance of Power

In many countries, cyberattacks and threats are considered important to national security today. It is though difficult to define the concept of a cyber threat. The vulnerability of different states or organizations became evident after attacks led by cyber hacktivists like *Anonymous*. Cyberattacks differ in nature, and the Center of Security Studies of Zurich classified these threats (Cavelty, 2010) as follows:

- Cyber-hacktivism, which refers to piracy or destruction of data.
- Cybercrimes and cyber espionage, mainly aiming at financial benefit.

- Cyberterrorism performed by non-state organizations, aiming to intimidate a government or population.
- Cyberwar, considered as attacks endangering the security of a State and its interests.

There are several modes of operation to apply cyberattacks; many of them have been presented in the previous chapter. These include Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks (see **Chapter 10**), implemented again by a group of computers. Another mode of operation aiming to collect confidential information or modify it could involve Trojans, for instance, able to collect and destroy confidential data, or worms able to cause computer dysfunction.

Generally, there are three different kinds of cyber weapons in use. The weaponry is used against physical infrastructure, such as computers, sources of electricity, communication cables, antennas, or satellites. Cyber weapons can be categorized as:

- Offensive weapons: different types of malware, such as viruses, worms, Trojan horses, and more. The result is the DoS actions.
- Dual use tools: network monitoring, vulnerability scanning, penetration testing, encryption, camouflage of content and communications.
- Defensive tools: firewall, disaster recovery systems (Tabansky, 2011).

The early incidents of international operations in cyberspace took place in 1999. As a response to NATO bombardment, Serbian hackers attacked Belgian internet websites. After a DDoS attack, NATO's website became unavailable for a few days. In 2007, during the Orchard operation, Israel attacked the Syrian means of aerial intrusion detection. This enabled Israeli aerial forces to bomb nuclear sites in Syria. In January 2009, French Rafale fighters could not take off for a mission because of an infection by a worm in the air traffic control services. These examples prove certain information and communications systems' interdependence, vulnerabilities, and critical roles. They also demonstrate that modern crises are tightly connected with operations over cyberspace vulnerabilities, which lie right at the heart of the potential to conduct a cyber war.

In order to develop an effective cyber defense, an organization has to secure every possible weakness in its IT infrastructure. In contrast, the assailant needs to discover vulnerabilities to conduct a successful attack. In cyber warfare, what counts is computing expertise. This feature may reverse the current equilibrium of powers: great military powers may not dominate cyberspace in the same proportion they dominate fields like at sea or in the air. On the contrary, small powers with high technological expertise may exert a powerful presence in cyberspace. This entails an asymmetry in military strategies between offensive tactics and defensive prospects.

The new digital Age has given rise to conflicts between countries deployed in cyberspace. Some examples are given below:

America – Russia

In September 2015, a hacker team called "*The Dukes*", which is linked to the Russian Government, hacked at least one computer system that belonged to the DNC. It was the first sign of a cyber espionage and information warfare campaign to derange the 2016 presidential election. What started as an information gathering attempt is believed to be ultimately shaped into an effort to damage one candidate, Hillary Clinton, and tipped the election to her opponent, Donald J. Trump. The White House's hesitance to respond meant the Russians had not paid a price for their actions, which could prove critical in discouraging future cyberattacks.

Russia and Estonia

In 2007, a series of cyberattacks occurred in Estonia. They were particularly effective because the Baltic state has implemented a broad spectrum of governmental services online. The attacks were generally conducted in Russia with state approval. This incident will be more thoroughly presented later in this chapter.

Iran and the United States of America

In September 2012, Iran was said to have conducted a series of Internet attacks on the computers of giants of the American financial industry, including *JPMorgan and Wells Fargo*, slowing down the servers and denying customers access to banking services. Iranians were subject to a financial embargo by the same Western banks (nationmultimedia.com, 2013).

Iran and Saudi Arabia

In 2012, Iranian hackers hit Saudi Arabia's national oil company, *Saudi Aramco*, nearly utterly destroying its corporate information technology infrastructure and bringing the company near collapse (Cyber warfare: Iran opens a new front, 2016).

China and America

Espionage was conducted by both sides, which was not regarded as an act of war, although the huge theft of data and the speed with which it could be exploited was unprecedented (The Economist, 2012). An example of an international conflict created by cyber security issues could be the developments involving leaks of classified documents about the US government's surveillance programs. Russia and China refused to follow the US requests to deport Snowden (see **Chapter 10**), the person behind the leaks. Hong Kong showed a clear lack of cooperation, arguing that *"the documents provided by the US Government did not fully comply with the legal requirements under Hong Kong law."* Leaders of both China and Russia applauded the decision to reveal the details of the US National Security Agency's secret surveillance program (Kshetri, 2014).

Eventually, an important feature is objectivity when clarifying the threshold, which defines if a cyber incident is considered an aggressive action interpreted as a national assault, and therefore, a military response can be justified. This can easily lead to the blurring of the conceptualization of the *cyber peace* state and the *cyber war* as its counterpart.

12.2 Cyberwar Incidents

In recent years, cyberwarfare has been deployed between confronted countries in several cases, introducing this new kind of offensive action globally and adding this new fourth dimension to conflict perspectives. Among them, Russia seems to be a pioneer in applying cyberwar techniques, forming an attitude tightly connected with its information security doctrine. Some remarkable incidents are presented in the following paragraphs in an attempt to outline the methods in use and their outcomes clearly.

12.2.1 The Case of Russia

In 2007, there were rumors that the Russian government had performed a cyberattack on Estonia's information infrastructure. This incident was neither the first nor the largest cyberattack that had been reported, yet it was the first digital offense to a country's national security. In 2008, Georgia faced a cyberattack while the confrontation with the Russian Republic continued. Between 2014 and 2017, cyber security companies detected cyber espionage in Ukrainian campaigns and military and security establishments.

However, by 2016, the reveal of a possible Russian interference in the US presidential election changed things, as we knew it so far. The evidence, as it will be analyzed next, proved that Russia interfered directly through cyber sources in the pre-electoral period, shaping the result of the elections.

12.2.1.1 Russian Cyber Policy

The Kremlin and the Russian secret services have evolved their approach to cyberspace in domestic and foreign policy since 2000. Initially, in 2000, Vladimir Putin signed the Information Security Doctrine as the first policy document of its kind (Soldatov & Borogan, 2018). The document lists several threats, including the manipulation of information (misinformation, the hiding of information, and the spread of fake news). It identifies as a major threat the desire of some countries to interfere and dominate Russia's interests in the global information realm (Russian Presidential decree no. 1895, 2000).

This content was generated by the Second Chechen War, when the Kremlin believed that liberal journalists and media could be a serious threat to the national security of the Russian Federation, mainly concerning the political stability of the regime (Soldatov & Borogan, 2018). Nevertheless, it was not until 2013, that Russia started speaking about cyber warfare and protecting the state's digital networks.

In 2013, the Ministry of Defense moved on with the creation of cyber troops due to Russia's war with Georgia in 2008 (Soldatov & Borogan, 2018). In the following years, the Russian government began to support financial and technological informal actors. The aid by the Russian secret services was not always easy to detect as they managed to hide all traces that connected hackers with the Russian state. That was the case of the cyberattack on Estonian websites back in 2007.

Cyber espionage and cyberattacks do not just aim to disorganize a state's society for a short time. Instead, hackers are willing to create a psychological impact. Russia aims to provoke destabilization among citizens to create the feeling that nothing is functioning and that the government is incapable of controlling things.

A very plausible reason explaining why Russia has followed such a policy in recent years lies in the low cost and low risk nature of this kind of operation. Russia's cyber foreign policy proves its ability to respond to crises and emerging opportunities while the Kremlin becomes even more unpredictable concerning when and where it will strike (Soldatov & Borogan, 2018).

A cyber conflict is not comparable to a conventional or a nuclear armed conflict. When a state launches a missile, it is impossible to deny the responsibility for this decision later. On the contrary, many who conduct such an action in a modern cyber conflict without being detected (Soldatov & Borogan, 2018). Russia realized this early and exploited this opportunity that cyberspace offers. However, the Kremlin is considered untrustworthy and is frequently suspected for being behind any major cyberattack in Western countries (Soldatov & Borogan, 2018).

12.2.1.2 Estonia 2007

Since the 1990s, Russian governments have attempted on many occasions to redefine the history of the Baltic States, where some memorials of World War II were vandalized and destroyed. In 2007, the Estonian government relocated the "Bronze Soldier" from the center of Tallinn to a military cemetery (Pernik, 2018). Russian state members spoke about deteriorating diplomatic relations if the Estonian government did not change its decision. In the next few days, the Kremlin posed restrictions on Estonian exports, Russian companies suspended contracts with Estonian firms, transits via Estonia were reduced, and train connections were suspended (Pernik, 2018). In addition, Russian speaking social media called for anyone possessing the necessary skills to launch cyberattacks against political parties and government websites by providing lists of targets, instructions, and attack means (Pernik, 2018).

The attacks lasted for three weeks and were committed against state institutions, political parties, and banks. Initially, the attacks were unsophisticated, consisting of denial of service and distributed denial of service, email spamming, and posting of automated comments. However, in April, more sophisticated and coordinated attacks targeted critical information infrastructure such as domain name servers, international routers, the network nodes of telecommunications companies and Estonia's data communication network (Pernik, 2018).

Estonia is supposed to be one of the most interconnected countries in Europe, and the failure of access to online banking services, the occasional denial of access to DNS services, and the disruption of mobile communications companies disturbed the Estonian society. Meanwhile, websites were mostly shut down and people received a great amount of spam to their email services almost daily (Pernik, 2018). The financial damage these cyberattacks caused in the Estonian public sector was almost €415,000, while Hansapank cyber security experts estimated that the cost for the biggest Estonian bank could range from €640,000 to €6.5 million (Pernik, 2018).

In the research for the attribution of responsibility, experts concluded that voluntary and "patriotic" non-state hackers who supported the Russian government carried out the attacks. However, due to the lack of technical evidence, the Estonian population doubted that the attacks were connected to Russia. Several Estonian politicians claimed that IP addresses that had been used belonged to the Russian government and framed these cyberattacks as a military threat (Pernik, 2018).

12.2.1.3 Georgia 2008

While a military conflict between Russia and Georgia started in August 2008, cyberattacks on Georgian websites were planned months earlier. The attacks targeted most of the state's institutional websites and many *.ge* domain addresses. The method used for these cyberattacks was similar to that of 2007 in Estonia. Russian speaking websites provided lists of targets and instructions. According to the Georgian Computer Emergency Response Team (CERT), the IP addresses that were used belonged to the Russian Business Network, which is suspected to have links with the Russian security services (Pernik, 2018).

Compared to a year earlier, the Georgian authorities discovered a sophisticated cyber espionage campaign, which detached sensitive and classified information related to Georgian national security in the networks of financial, institutional, and non-governmental organizations. This campaign was again attributed to the Russian secret services and had links to the military or state authorities (Pernik, 2018).

In 2008, Russia proved its ability to coordinate cyberspace actions, information acquisition, or disruption again, while cyber activities supported Russian military operations during the war (Pernik, 2018).

The incidents of 2008 marked the shift in military thinking because, from this point in history, cyberspace has constituted another dimension in political and military conflicts. NATO in 2016 recognized this aspect in the Warsaw Summit. The declaration states that: "we (the states) reaffirm NATO's defensive mandate and recognize cyberspace as a domain of operation in which NATO must defend itself as effectively as it does in the air, on land, and at sea" (NATO, 2017).

12.2.1.4 Ukraine (2014-2018)

The initial cyberattacks on Ukrainian websites started in December 2013but were unsophisticated. Hackers tried to cause damage to email accounts, broadcast stolen information online and sent mass text messages containing propaganda. Targets were mainly banks, political parties, new portals, and state institutions (Pernik, 2018).

A massive number of cyber espionage campaigns were detected and were linked to Russian hackers. Some of these campaigns targeted military and national security officials. Other cyberattacks targeted the Ukrainian energy sector (2015), Kyiv's s airport, and the financial sector. These attacks required long term planning and were carefully crafted. In the meantime, according to the Ukrainian Computer Emergency Response Team, traces of the Russian Advanced President Threat 28 (APT28) group were detected in 2014 in the Ukrainian Central Election Committee networks (Pernik, 2018). The group had been attributed to the Russian Military Intelligence.

The cyberattacks over a period of four years caused the Ukrainian government extensive economic losses and damages to digital and critical infrastructure, while Russia's cyberwarfare and integration of information were successful (Pernik, 2018). In this case, Russia proved its superiority in cyberspace, practicing and demonstrating its capability to detach critical information through the Internet.

12.2.1.5 US Elections 2016

It has been stated that cyber interference in elections matters the most because targets in these cases are not simply computers and websites. The attacks target the citizens conducting propaganda designed to affect individuals rather than computers, which is tailored probably by another state actor (Van De Velde, 2017). Such an incident questions national sovereignty and governmental authorities' power concerning their own population will. In this context, the political notion defines that public opinion has been violated, and the right to self-determination is at the center of the violation analysis (Ohlin, 2017). Therefore, those attacks are treated separately from other cyberattacks. As mentioned above, the cyberattack allows someone to act anonymously and hardly ever be punished. Due to its nature, the attack before or during electoral processes is even more difficult to handle as the election process takes place in a specific timetable, while most of the time there is no clear evidence that somebody acts under state control (Van De Velde, 2017). Nevertheless, once it is widely known, the potential to undermine citizens' support in the authorities, confidence in the democratic processes, and integrity of their government is high (Van De Velde, 2017).

In the 2016 US Elections, it is supposed that Russia used numerous cyber espionage teams to hack into American computers and email systems during the 2016 presidential elections. The military intelligence of the Russian Federation attacked at least one voting machine supplier during the American presidential election (Berghel, 2017). Theft of information has been detected along with selective dissemination of information, a propaganda campaign, and efforts to hack into nationwide voting systems (Van De Velde, 2017).

The cyber espionage team named "*Cozy Bear*" or "*ATP29*" (Sanger & Shane, 2016) penetrated the email account of Clinton's presidential campaign chair, John Podesta (Forcese, 2016). Meanwhile, the Russian unit *"Fancy Bear"* or *"ATP28"* hacked several emails of the Republican National Committee (Sanger & Shane, 2016). These teams managed to detach information, which was published later. In July 2016, private documents from Podesta's email account were leaked on WikiLeaks (BBC News, 2016) and other websites, while emails from the Republican National Committee were never posted online, despite the recorded hacking.

Russia's aim hypothetically was to distort American sovereignty and to help the candidate who was much more sympathetic to t Russian interests rather than the one who gained the public opinion (conservative Trump rather than liberal Clinton) (Ohlin, 2017).

Answering these allegations, the Russian President, Vladimir Putin, strongly denies this accusation by declaring: "We never engaged in that at a state level, and have no intention of doing so" (Associated Press, 2017). However, he accepted the possibility that some patriotic hackers committed it due to the unstable relations between the two states. On the contrary, a January 2017 assessment that presented the US intelligence community's findings concluded that "Kremlin ordered an extensive, multi-pronged propaganda

effort to undermine public faith in the US democratic process, denigrated Secretary Clinton, and harmed her electability and potential presidency" (Cole, 2017).

The significance of this event is that one superpower interfered in the other's national election using cyberspace. However, as Berghel underlines (Berghel, 2017), the only one to blame is the United States since much evidence was hidden by the intelligence services under the protective banner of classified sources, and American citizens were not informed. Moreover, he stated that it was a matter of time before the electronic election system would be hacked by state or non-state actors who aimed to destabilize the US internally.

12.2.1.6 The Brexit Referendum (2016)

Since the end of the Soviet Union, the United Kingdom has had strong ties with the Russian Federation and businesses between them are thriving. Even though these states were ideologically divergent, they were diplomatically close to each other due to convergent interests. Nowadays, their relationship has undergone severe friction due to the poisoning of a former Russian military intelligence officer, Sergei Skripal, and his daughter, Yulia, which occurred on British soil in the English town of Salisbury (Rodgers, 2018). However, the crucial and catalytic point in the progression of their deteriorated relationship has been the interference of Russia in the 2016 Brexit referendum.

On June 23, a referendum was held on concerning whether the United Kingdom should stay or leave the European Union. The British people voted to leave the European Union despite the advice of the foremost Westminster party leaders (Asthana et al., 2016).

Nevertheless, there is an ongoing investigation into Russian interference in the Brexit referendum, carried out by the UK Electoral Commission, the UK Parliament's Culture Select Committee, and the United States Senate. The Kremlin was accused of secretly backing a pro-Brexit vote (Holton & Faulconbridge, 2017).

It is no secret at all that Russia is determined to sabotage and divide the Western governments and, therefore, the institution of the European Union. By eliminating and isolating one of the wealthiest member states of the EU, it manages to weaken the West and can use this leverage for its profit.

Media reports claimed that numerous pro-Brexit tweets came from fake accounts originated in Russia. During the count-down of the referendum, the former British Foreign Secretary, Philip Hammond, implied that Russia would be the only country satisfied with a pro-Brexit result. Russia preferred not to make any comment (Rodgers, 2019).

The United States Senate suggested that Russia has sought influence in the Brexit campaign through "*disinformation, cyber hacking and corruption*" (Putin's Asymmetric Assault on Democracy, 2018). According to the *"The Times of London,"* Russia used X bots and trolls to disrupt the Brexit referendum. Russia engaged in an unconventional warfare against the UK voters. At the peak of the standby of the referendum, 45,000 messages concerning pro-Brexit were posted via Russian X accounts in the last 48 hours during the 2016 referendum (Mostrous et al., 2017).

Russians used a tactic of social media bots, which later that year was used again successfully during the US presidential elections. These fake social media accounts have the power to influence public opinion and politics in general and can create convincing online personas capable of influencing real people (Vagianos et al., 2019)

Furthermore, during the investigation that took place by the US Congress, it has been argued that *"the Russians used sophisticated targeting techniques and created customized audiences to amplify extreme voices in the campaign, particularly those on sensitive topics such as race relations and immigration"* (www.parliament.uk, 2018).

Russians used the X to shape their preferred opinion because it is the platform used more for *"connecting with people for information sharing purposes rather than personal interactions"* (Gorodnichenko, 2017).

Eventually, according to research conducted by *89up*, *Russia Today* and *the Sputnik,* 261 articles related to the EU referendum were published, and they all favored the positive Brexit vote (Gorodnichenko, 2017). These media articles were published between January 1 and June 23, 2016. Another research conducted by the Universities of Swansea and Berkeley, *"also identified 156,252 Russian accounts tweeting about #Brexit and that they posted over 45,000 Brexit messages in the last 48 hours of the campaign"* (Gorodnichenko, 2017).

12.3 Cyberterrorism

12.3.1 An Introduction to Cyberterrorism

Information warfare, as analyzed in the previous paragraphs, is an overarching concept that encompassing *cyberterrorism*. Information warfare is the gathering or use of information to gain an advantage over another party. Terrorism is defined as the actual or threatened use of violence by an individual or group motivated by ideological or political objectives. The goal of terrorism is to intimidate or coerce a government or its people. Cyberterrorism, however, cannot be as concretely defined and has spurred significant debate over precisely what it means. A panel of experts on cyberterrorism was convened in March of 2003, with one stating that "*if I cannot get to my e-mail for a few days, I am not terrorized.*" This illustrates the common misperception that a network disruption is an act of cyberterrorism. This would be considered more of an act of information warfare (Taylor et al., 2006).

Barry Collin of the Institute for Security and Intelligence states that cyberterrorism is *"hacking with a body count."* One of the most accurate definitions concerning cyber terrorism is:

Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or are costly nuisances would not be considered cyberterrorism. (Denning, n.d.).

According to the US Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents." Cyberterrorism is a component of information warfare.

The concept of cyberterrorism differs from that of hacktivism. For example, hacktivists like *Anonymus* act in the name of freedom and support reliable information. They consist of hackers who attack sites that promote child pornography, while the majority of their actions target government propaganda, organizations, and corporations that are applying, e.g., censorship. Their activity has been presented in Chapter 10. In 2015, they initiated cyberattacks on Turkish websites as a means of expressing their opposition to the Turkish government's association with ISIS. On the other side, the intentions and consequences of cyberterrorism involve more severe and permanent damage. This can include loss of life or economic collateral.

There are four categories of attacks that encompass cyberterrorism or information warfare:

1. Infrastructure attacks or those attacks designed to destroy a system that includes critical data.

2. Information attacks or attacks focused on demolishing or altering the content of electronic files or computer systems.
3. Technological facilitation or the use of cyber communication to distribute and coordinate plans for a terrorist attack, incite an attack, or otherwise assist in the facilitation of terrorism.
4. Promotion, which includes fundraising solicitation and recruitment.

12.3.2 Cyber Terrorism Throughout History

Since the debate over cyber threats started, the basic question for security policy makers has always been: Are the most dangerous actors, terrorists, enemy states, or just criminals? In other words, Will we have to deal with "cyberterrorism," "cyberwar" or just "cybercrime"? This debate has never really been solved. However, the Clinton administration focused on cyberterrorism (Colarik, 2006).

In January 1999, President Bill Clinton announced a $1.46 billion initiative to improve governmental computer security to protect against terrorist attacks that might target the nation's infrastructure, such as power plants, telecommunications, banking, transportation, and emergency services. The plan was outlined in a speech before the National Academy of Sciences. It detailed 10 points that aim to thwart threats from cyberterrorists as well as biological and chemical weapons. The total program would cost $10 billion. One previous online attack occurred in February 1988, when a group of Israeli and US teens broke into Pentagon computers. While officials quickly detected the break-in, it took several days to determine that it was an act of vandalism rather than foreign aggression. Last year, national security experts hacked unclassified Pentagon computers during an online war game that would have allowed them to disrupt troop movements, the Pentagon reported at the time (CNN.com, 1999).

"If terrorists are able to use encryption, they are not far from planning cyberattacks." Clinton made this very clear in December 2000 in his farewell lecture on foreign policy at the University of Nebraska at Kearney. In this speech, he named five principles for future US foreign policy:

- strengthen alliances like NATO,
- pay attention to Russia and China,
- confront local conflicts in other parts of the world,
- pursue global trade with a "human face,"
- face new security challenges like cyberterrorism and infectious diseases like AIDS.

He went on to say that one of the biggest threats to the future would be cyberterrorism, that is, people 'fooling' with computer networks, trying to shut down phones, erase bank records, mess up airline schedules, and generally doing things to interrupt the fabric of life (Eriksson & Giacomello, 2007).

Shortly after George W. Bush came into office in January 2001, the cyberthreats debate changed quite radically. Cyberterrorists were still taken into account, but the new government focused much more strongly on foreign governments as possible attackers. A linkage between the cyberterrorism perception of the Clinton years and the cyberwar fears of the first Bush year was the concept of "*rogue states."* This term, which had been abandoned by Clinton but was quickly revived by Bush, implies that some states will use terrorist means to attack the United States. Surprisingly, the first "rogue state" to be accused of planning cyberattacks against the US was not Iraq, Iran, China or North Korea, but Cuba. During the Senate Select Committee on Intelligence on the Worldwide Threat hearing in 2001, Defense Intelligence Agency director Thomas R. Wilson identified Fidel Castro's autocratic regime as a possible cyber attacker (Eriksson & Giacomello, 2007).

Shortly after he took office in 2009 Obama promised he would *"pursue a new comprehensive approach to securing America's digital infrastructure".* He said that "*this new approach starts at the top" and that "we will deter, prevent, detect, and defend against attacks."* Given the growing sophistication and determination

of state-sponsored cyberattacks, he was right to make it a top priority. On Obama's watch, the State Department, the White House, the Department of Energy, and the National Nuclear Security Administration were hacked. A Government Accountability Office report found that cyberattacks against government agencies climbed 35% between 2010 and 2013. As for the United States Office of Personnel Management (OPM), the inspector general has issued multiple warnings over the past eight years about glaring problems with its security systems. In fact, the same month Obama made his pledge, the IG issued a "flash audit alert" that "severely outdated" security procedures put its data at risk. Despite these warnings, hackers trolled around the OPM servers over a year and extracted Social Security numbers, addresses, dates of birth, fingerprints and highly sensitive data collected during security-clearance investigations on some 18 million federal employees. After that breach came to light in mid-2015, Obama announced a *"new Cyber Security National Action Plan" that would "address short- and long-term challenges when it comes to cyber security"* (Investor's Business Daily, 2016).

Some other documented cases of cyberattacks worldwide that have been reported are the following:

- In December 2010, PayPal became a cyberattack victim after it permanently restricted the account used by WikiLeaks to raise funds, citing its violation of the Acceptable Use of Policy as its reason. However, it did not only result in multiple boycotts from individual users but also caused hackers to move in.
- In 2012, *"Flame"* was discovered; a virus used to attack computer systems in Middle Eastern countries that run on the Microsoft Windows operating system. This new virus, used by hackers for espionage purposes, infected other systems over local networks, including over 1.000 computers from private use, educational institutions, and government organizations. It also recorded audio, including Skype conversation, keyboard activity, screenshots, and network traffic. It was discovered on May 28, 2012, by the MAHER Center of the Iranian National Computer Emergency Response Team (CERT), the CrySys Lab, and the Kaspersky Lab.
- Iran was subject to cyberattacks in June 2010 when its nuclear facility in Natanz was infected by Stuxnet, a cyber worm that was believed to be a combined effort of Israel and the United States, though no one claimed responsibility for its inception. The worm destroyed Tehran's 1,000 nuclear centrifuges and set back the country's atomic program by at least two years, as it infected over 60,000 computers. The Iranian government was also accused of its cyberattacks on the United States, Israel, and other countries in the Gulf, including their alleged involvement in the hacking of American banks in 2012.

As already mentioned, terrorist organizations use Internet resources for propaganda and recruitment. The Internet offers a variety of tools for such purposes thanks to its anonymity and the fact that it remains largely unregulated and readily available to the majority of people. Recruitment and mobilization are essential parts of terrorists' web presence. Terrorist groups aim to recruit new members, especially the young, by promoting propagandistic content through the net. A very characteristic example of such a terrorist organization is Hamas, a Palestinian Resistance Movement that is connected with many bombastic suicide attacks against Israel. Until the end of 2008, 1,162 people had been killed in terror attacks, and 40% of the victims were the result of attacks carried out by Hamas. Its goal is to establish an Islamic Palestinian state in place of the state of Israel, proclaiming jihad *(the holy war*) as the only means in order to achieve this. Hamas supports its ideology and recruits new members through numerous sites, while similar sites are used by jihadists of Syria also as an attempt to recruit new memberships.

12.3.3 Cyberterrorists' Tools

The tools that terrorists use are called *cyberplagues*. Cyberplagues include viruses, botnets, bots, and the already known DoDS, all analyzed in the following paragraphs. One of the most famous viruses is the *"I Love*

You" virus, which affected Web development and multimedia files spread through Microsoft Outlook address books titled *"Love Letter."* The total cost of that virus was over a billion dollars. China and Cuba have also developed programs to spread computer viruses like this against computers in the United States. Another method that terrorists use is data hiding, which is also known as stenography. This concept refers to a series of methods of secret communication between the members of a terrorist organization. The main idea behind this technique is to take a piece of information and hide it with another piece of data, such as an image, so that the final message is not disclosed to the public but only to the members of the organization. After the events of September 2001, reports claimed that Al Qaeda had been transmitting hidden data over the Internet.

12.3.3.1 Viruses

According to the world's largest security software provider, Norton Security, a division of Symantec, a computer virus, much like a flu virus, is designed to spread from host to host and can replicate itself. Similarly, as viruses cannot reproduce without a host cell, computer viruses cannot reproduce and spread without programming, such as a file or document. In more technical terms, a computer virus is a malicious code or program written to alter how a computer operates, designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document supporting macros to execute its code. In the process, a virus can potentially cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data (Norton, 2020).

12.3.3.2 Botnets

A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals. They are typically used to send spam emails, transmit viruses, and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today. The word Botnet is formed from the words" robot" and "network." Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all infected machines into a network of" bots" that the criminal can remotely manage (Kaspersky, n.d.).

12.3.3.3 Bots

A "*bot*" is a type of malware that allows an attacker to control an affected computer. Also known as "*Web robots,*" bots are usually part of a network of infected machines, known as a "*botnet,*" typically made up of victim machines stretching across the globe. Since a bot-infected computer does the bidding of its master, many people refer to these victim machines as *"zombies."* The cybercriminals that control these bots are called "*botherders"* or "*botmasters."* Some botnets might have a few hundred or a couple thousand computers, but others have tens or hundreds of thousands of zombies at their disposal. Many of these computers are infected without their owners' knowledge (Norton, 2019).

Bots sneak into a person's computer in many ways. Bots often spread themselves across the Internet by searching for vulnerable, unprotected computers to infect. When they find an exposed computer, they quickly infect the machine and report to their master. They aim to stay hidden until they are instructed to complete a task. After a bot takes over a computer, it can perform a variety of automated tasks (Norton, 2019).

12.3.3.4 Distributed Denial of Service Attacks (DDoS)

Cyberterrorists may also use denial-of-service attack methods to overburden a government's and its agencies' computers. Denial-of-service (DoS) attacks are designed to make a computer or network of computers unavailable to its users. As mentioned in **Chapter 10**, one common method of attack involves saturating the

target machine with external communications requests, to the point that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. On a networked computer, such attacks usually overload the server and affect all of its users. If an attacker uses a single host to launch the attack, this approach is classified as a DoS attack. However, if an attacker uses the capabilities of many systems (such as botnets) to launch simultaneous attacks against another host, this is classified as a DDoS attack. For this purpose, the attack can use viruses or other malware to infect several unprotected computers and then take control of them. Once control is obtained, the terrorists can manipulate these infected computers to initiate the attack, such as by using botnets to send information or demand information in such large numbers that the victim's server effectively collapses under the strain of processing the information. A stronger version of this attack, known as permanent denial-of-service (PDoS), can damage a system so badly that the system's hardware must be reinstalled or even replaced (Weinman, 2015).

12.3.4 Terrorism and the Dark Web

Terrorist groups have been active on numerous online platforms since the late 1990s. At that point, those organizations took advantage of the unregulated and anonymous nature of the internet, and maintained thousands of websites to transmit messages to their targeted audiences, carry out psychological warfare and propaganda, recruit supporters, coordinate etc. It appears that terrorists exhibited a capability of quick adoption and application of every emerging online tool. So, they were particularly active in video- and picture-sharing platforms, instant messengers, blogs, chatrooms, social media, etc. It is not surprising that globally popular platforms, such as YouTube, Instagram, X, and Facebook have been used by terrorists in order to post various propaganda content. More importantly, the internet has been used to provide information for acts of terror, such as technical details for explosives and weapons, maps, guidebooks, directions etc.

Hundreds of websites provide detailed instructions that can facilitate terrorist attacks in multiple ways. In general, for over two decades, terrorist groups have tried to advance their cause through the internet. However, the Surface Web was still risky given the fact that these online actions could be traced and monitored. On the contrary, the Dark Web offers terrorists the anonymity this inaccessible and invisible hidden part of the network provides. Indeed, the Dark Web facilitates terrorism. Terrorist groups may not have access to the broad audience of the Surface Web, but the obscurity and anonymity of the Dark Web allow them to communicate and coordinate more safely secretively. Besides, the counter-terrorism agencies try to trace and shut down Surface Web's terrorist websites and social media. It seems that the Dark Web is ideal for terrorist organizations facilitating their various extremist activities such as fundraising, sharing of instructions, coordination, purchasing weapons, purchasing fake documents and passports, recruitment, etc. (Weimann, 2016).

Due to the advances in information and communications technologies, the interest of terrorist groups in the Dark Web platforms is growing. In this context, a simple description of the terrorist's activities on the Dark Web would include their typical activities, carried out more secretly. Indeed, terrorists utilize the Dark Web in the same way as they have been utilizing the Surface Web for several decades. However, not only does the Dark Web offer privacy and anonymity, it also offers new "opportunities" and flexibility. Terrorist and extremist groups traditionally use the open internet to communicate with fellow terrorists, recruit new members, radicalize, spread their ideology and propaganda, raise funds, and coordinate acts of terrorism. The emergence of the Dark Wed shifted all these activities to deeper layers of the internet (Weimann, 2017). In this framework, 3 cases are briefly presented demonstrating the way that terrorist groups take advantage of the Dark Web applications:

Telegram

ISIS is one the biggest terrorist organizations, which heavily relies on the internet to communicate. In this framework, ISIS has been using popular social media platforms, but they have been mostly using Telegram. Telegram is an encrypted social media application that does not allow the messages transmitted through it to be tracked by third parties. One advantage of Telegram is that it has a large file hosting feature. The most important advantage of Telegram, though, is that it enables users to communicate securely given that one‐to‐one communications are secret and cannot be seen by others. Telegram is highly attractive to terrorists due to its prominent attributes of end-to-end encryption, ensuring the concealment of users' identities. Consequently, it is unsurprising that Telegram has emerged as a crucial communication tool employed by ISIS. (Yayla & Speckhard, 2017).

Bitcoins

The Dark Web has severely enabled money transfers and illegal purchases using virtual currencies such as Bitcoin and other cryptocurrencies. Indeed, these cryptocurrencies are very attractive to terrorists who consider them as a tool to purchase weapons and explosives in the Dark Web. In particular, cryptocurrencies constitute a decentralized financial system that allows terrorists to circumvent traditional banking institutions. So, Bitcoin and other cryptocurrencies are a useful financial mechanism for terrorists, which allows them to execute untraceable and anonymous transactions. In practice, cryptocurrency virtual platforms have fueled terrorism, strengthening their ability to fund their activities. Besides, it is not only that Bitcoin is practically the de facto currency of transactions on the Dark Web, but Bitcoins and other virtual cryptocurrencies lack a coherent regulatory framework that fosters the operations of terrorist groups (Hasbi & Mahzam, 2018).

Silk Road

Silk Road is a crypto market on the Dark Web, where illegal transactions and exchanges occur. In particular, Silk Road is a central digital platform that functions as a crypto market and facilitates the trade of goods and services using cryptocurrencies. Silk Road and other crypto markets utilize Dark Web technologies to conceal the identity and location of users and, hence, secure and hide the network for such trade interactions. So, Silk Road has turned into a black crypto-marketplace for drugs, weapons etc., and that eventually led law enforcement to shut down the Silk Road site (Finklea, 2015).

12.3.5 A Case Study of Cyberterrorism: ISIS

12.3.5.1 Mission

In order to better understand the various aspects of cyberterrorism, the case of ISIS (Islamic State of Iraq and Syria) is presented. Since cyberspace tends to be the new “battleground,” the so-called Islamic State has been very active and innovative in the cyber terror realm. As Giantas writes, *''ISIS is a pioneer in exerting cyberterrorism''* (Giantas & Stergiou, 2018), using the limitless features of the Internet more forcefully than any other group has done in the past, aiming to cause unprecedented fear. This extremist organization uses cyberspace more intensively and systematically than any other one in the past. The jihad (holy war) has physical and digital components. Simultaneously with the attacks in the real world, ISIS poses an active cyber threat by recruiting many experienced hackers with the necessary computing skills to hack into systems and do damage. They are also very active on social media in order to promote the message and culture of ISIS by defacing websites or social media accounts with text, images, and videos, glorifying the agenda of the group (Scott & Spaniel, 2016).

According to Choi et al. (2018), ISIS has not given up the basic premise of conventional terrorism but has expanded its activities in cyberspace exploiting technology to support its actions. In the first steps of its

technological engagement, the aim was not to cause death or physical harm but to create chaos and bring an aura of insecurity to European societies. According to CNN, within three years, ISIS has executed over 150 attacks in 30 different countries, causing the deaths of more than 2,000 people and injuring thousands more. At the same time, the ISIS members embrace cyberterrorism with the following argument: *"…we extend on the land and in the internet. We send this message to America and Europe. We are the hackers of the Islamic State, and the electronic war has not yet begun"* (Runkle, 2015).

The turning point in this electronic war, which has instantly transmitted the fear all over the globe, is thought to be the combination of the physical attack on the French satirical newspaper *Charlie Hebdo,* which was followed by a cyberattack on approximately 19,000 French websites. The main target of these cyberattacks was to support the spread of feelings of fear and insecurity among European societies, which were already in the air by the Paris shootings that led 12 people to death.

12.3.5.2 Structure

The most important characteristic of the cyberterrorism cultivated by ISIS is the fact that such attacks are carried out mainly by the caliphate's members but also by groups and individuals linked to the Islamic State, supporting their cause and goals (Flashpoint, 2015a). **Figure 12.1** shows the divisions connected and performing cyberattacks on behalf of ISIS. These divisions are:

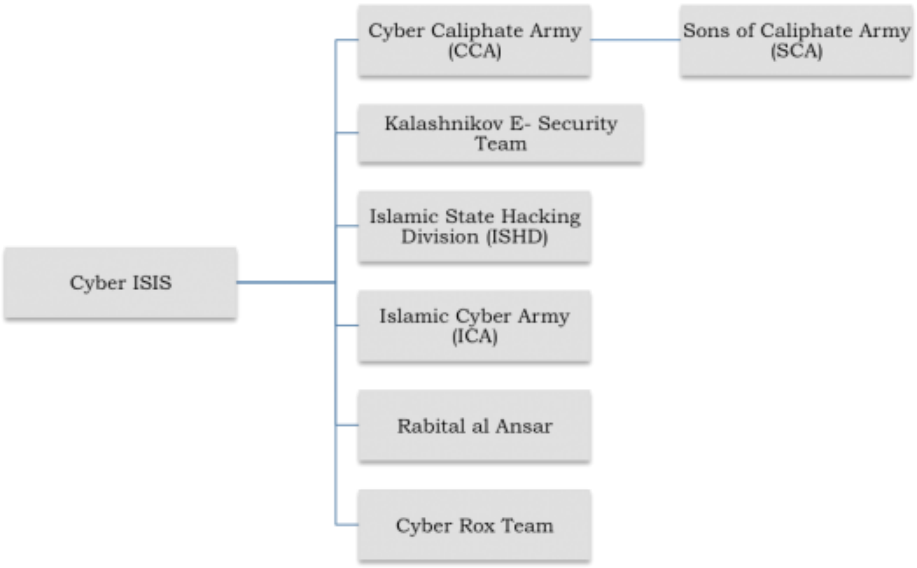


Figure 12.1 *The hacking groups that constitute the core of ISIS' cyber-terrorism (source: http://www.idis.gr).*

Cyber Caliphate Army (CCA)

This was one of the first cyberterrorist groups to support the Islamic State. The most crucial cyberterrorist attack of the CCA was on the X and YouTube accounts of the US Central Command. CENTCOM accounts were modified, appearing phrases and slogans such as *"American soldiers we are coming, watch your back"*, *"CyberCaliphate"* and *"I love you ISIS."*

Sons Caliphate Army (SCA)

The Sons Caliphate Army (SCA) was founded in 2016 as a subgroup of the Cyber Caliphate. In the first video the SCA released, security experts referred to the existing vulnerabilities and the rising cyber capabilities of ISIS. In 2016, for the first time, the Department of Justice charged Ardit Ferizi, the founding father of SCA, with cyberterrorism. He was accused of allegedly hacking into a military website and stealing the names, addresses, and other personal information of government and military personnel and selling it to ISIS.

Kalashnikov E-Security Team

Kalashnikov E-Security Team was a hacking group founded in 2016 that identifies itself as *"an expert on web-hacking techniques and exploits*" and has a great activity in cyberspace, providing ISIS mainly with technical support.

United Cyber Caliphate (UCC)

The most coordinated and essential actor in ISIS' cyber-terrorism is UCC. The group was created in May 2016 when several other hacking groups merged. On April 5, 2016, the group took responsibility for a cyberattack on the Embassy of Indonesia in France.

Islamic State Hacking Division (ISHD)

The Islamic State Hacking Division or ISHD was founded in 2015 while it was closely associated with Ardit Ferizi, a hacker from Kosovo, head of the group Kosova Hacker's Security (KHS), who launched several cyberattacks on websites of Greece, Israel, and Serbia. They are the promoters of the *Lone Wolf* and the supporters of ISIS.

Islamic Cyber Army (ICA)

In 2015, the Islamic Cyber Army (ICA) first appeared in cyberspace; while on September of the same year instrumented a series of attacks. The common feature of these attacks is that they include the hashtag *#UnderAttacks*. The main target of the Islamic Cyber Army directly or indirectly the United States.

Rabitat Al-Ansar

Rabitat Al-Ansar's initial role was to spread the ideology of jihadism and to recruit new members. In March 2015, Rabitat Al-Ansar's supporters claimed on their social media accounts that they would launch attacks against the USA. For this purpose, they used the *hashtag#WeWillBurnUSAgain*.

Cyber Team Rox (CTR)

CTR is a group of pro-ISIS hackers who are very active in website defacing and data breaches.

12.3.5.3 Jihad in the Internet

In recent years, jihad gained more and more supporters, not only from the Islamic world but also from Western Europe and America. The internet creates a concrete bond between the individual and the virtual Muslim community (Liang, 2015).

In 2014, a magazine called *Dabiq* was published online. *Dabiq* is translated into many languages including German, French, Arabic, and Russian. The magazine includes religious, political, and military content and is very influential in new members' recruitment. Except for Islamists, the magazine attracts all kinds of migrants, people holding military and administrative power, as well as engineers or other scientists, to participate in the holy war. Finally, the magazine outlines its future political strategy and identifies the two holy cities in Saudi Arabia and Jerusalem as future targets. The first two issues include a quote from Al Qaeda in Iraq founder Abu Musab al-Zarqawi, saying that *"the spark has been lit here in Iraq, and its heart will continue to intensify- by Allah's permission- until it burns the crusader armies in Dabiq."*

Because of its virtual nature, the Internet community has become idealized in the minds of surfers. This appeals to young Muslims suffering from social isolation or ordinary discrimination (Liang, 2015). The immediate responsiveness of Muslims to chat rooms and the notional context of the exchanged messages enhance the concreteness of this virtual community, including populated social media platforms. Participants in the global jihad are not atomized individuals but actors linked to each other through complex channels of direct or mediated communication where messages are spread globally and effectively.

12.3.5.4 Social Media for Daesh

As a reminder, the Islamic State is a jihadist group inherited from the Al Qaeda branch in Iraq, created following the overthrow of Saddam Hussein in 2003 and the occupation of the country by American troops. Over 110 countries provide fighters to the Islamic State, including Tunisia, Russia, France, Belgium, and Italy. DAESH is a transliteration of the Arabic acronym formed of the exact words that make up ISIS in English. It is usually used as *Daesh,* which is the Arabic name given to the Islamic State. Its ambition is to create a state entity governed solely by the rules of Islam. The quality of information is the number one issue, digital media is considered a weapon for Daesh, and jihadist groups are increasingly adapting to the evolution of the web. Social networks are tremendous accelerators that have made it possible to spread Daesh's propaganda (Shaheen, 2015). In this way, Daesh uses them to the maximum of their potential.

Following the attacks of September 11, 2001, in New York City, USA, the emergence of a new form of recruitment of the Islamic State has been envisaged, as the traditional recruitment in mosques was not that effective. Daesh, therefore, used social networking platforms to recruit jihadist apprentices with propaganda elements. In 2014, the number of young Internet users who left for Syria and were ready to adopt the ideals of a terrorist group increased by more than 110%. Passing through the mosque is not compulsory, and hundreds of young people who have not necessarily had contact with Islam decide to leave their country. Thus, Daesh's best-known technique is to recruit fighters via social networks, including X and Facebook, using a recommendation algorithm based on an Internet user's interests (Idahosa, 2017). It is, in particular, by watching propaganda videos (broadcasting images of assassinations, sermons calling for violent jihad, but also videos promoting the caliphate and sacralizing its components) on social networks that young people can see the corresponding spiritual content. At that point, the process of indoctrination and radicalization via social networking sites begins. To perfect this indoctrination, recruiters contact with Internet users and try to create connections based on their interests, as indicated in their profile. X, YouTube, and Facebook are among these, and their use is outlined below.

X has a high profile among young people, where Daesh has more than 70,000 accounts. This channel of communication has enabled it to carry out many terrorist acts in recent years. These X accounts download videos and propaganda images, inform, communicate, build diversified and globalized networks, identify potential targets, seduce, and recruit. Although networks such as X or Facebook delete accounts that promote terrorism, Daesh's digital supporters use the "Retweet" or "Share" buttons to achieve a high sharing capacity and greatly increase visibility and the number of users.

In 2014, X had over 284 million users, posting 500 million daily tweets, supporting over 35 languages. Jihadists use X to engage in real-time discussions to influence and recruit new members. In the fall of 2014, at least 45,000 X accounts were controlled by supporters of ISIS; 73% had an average of 500 followers (Forbes, 2018). Messages on X are written in perfect English by popular Islamist groups, sometimes in other languages also, to reach wider audiences. Furthermore, ISIS distinguishes itself from other groups on X through hashtags. For example, during the Football Cup of 2014, hashtags like *"#Brazil2014"* allowed them to approach new audiences. Other hashtags connected with ISIS are *"AllEyesOnISIS"* and *"#CalamityWillBefallUs."* The last one was used to threaten the US-led coalition campaign to bomb ISIS troops in Iraq (Idahosa, 2017). Isis uses *"X bombs"*, which redirect trending hashtags to X websites and content related to the Islamic State. The *Al-Battar Media Group*, which counts 32,000 followers, works constantly to mobilize X members to support ISIS releases through independent media wings.

There are many categories of ISIS X accounts: official and unofficial news accounts, regional accounts, and individuals commenting about the events in Syria and Iraq. The fact that some individuals are tweeting almost 200 times a day and their tweets are attracting tens of thousands of followers is indicative of the huge influence of ISIS on this platform.

ISIS also uses YouTube. As mentioned in Chapter 3, YouTube attracts 1 billion unique users worldwide every month. In addition, users watch over 6 billion hours of video each month, and 100 hours of video are uploaded to YouTube every minute. A study carried out by the first European Conference on Intelligence and Security Informatics in 2008 demonstrated that 50% of jihadists' videos contained *"martyr hailing"* content, an estimated 30% contained footage of suicide bombings, and another significant percentage contained educational content about Islam and the call to martyrdom. A considerable fact is that this kind of video is viewed by users from 18 to 24 years old.

The al-Hayat Media Center is the leading producer of ISIS video content. In July 2014, al-Hayat published a collection of 11 videos in English, which were filmed in high resolution and underwent skilled post-production editing. YouTube remains one of the most powerful means of recruiting. Al-Hayat Media Center produces an HD propaganda series known as *"Mujatweets",* which presents the everyday life of fighters in Syria and Iraq. The ISIS message is also spread by unofficial global activists who help circulate propaganda, known as tweeps, fanboys, and fangirls. In 2014, a trailer for an ISIS style videogame was uploaded on YouTube. In the trailer of the video game, players are dressed as ISIS fighters, blowing up targets and shooting police troops.

In June 2014, Facebook recorded a daily average of 829 million active users, and it has subsequently evolved into a decentralized platform for disseminating information. Foreign fighters in Syria also used Facebook pages are to invite friends to join jihad. The supporters of the Islamic State upload jihad fighters' pictures and videos.

Eventually, social networking sites play an important role in the recruitment of new jihadists as young people are more easily tempted, and indoctrination seems to progress fast.

12.3.6 Social Media Against Cyberterrorism

As a first step, the Anti-Terrorism Act of November 2014 strengthens the provisions related to the fight against terrorism. Some sites accused of promoting terrorism have been removed by the French government to prevent anyone from accessing them and to counter radicalization on the Internet. This would also include social networks, including X. The latter has launched a real battle against Daesh's partisan accounts on the social network by closing and deleting more than 10,000 accounts. For example, YouTube only deletes videos containing violent images and leaves propaganda videos that the terrorist group uses to spread its ideology and recruit. It should be noted that deleting a violent video takes several hours or even several days (Forbes, 2018).

Facebook also tries to address the issue of dangerous content shared on its platform and has already deleted more than 14 million terrorism-related content. Facebook claims to use several tools to combat this type of content, including automated detection tools that are constantly being improved. Based on machine learning, one of these tools is now able to evaluate messages that can support organizations such as Daesh or Al Qaeda. Thus, these actions are already making it possible to intensify the fight against cyber-terrorism on social networks. Indeed, since 2009, a website has allowed Internet users and professionals to report illegal content related to terrorism. The advances in the process of identifying and removing terrorist content have also intensified following the January 2015 attacks in Paris (Forbes, 2018).

An example of an effective fight against terrorism through social media is Israel. Israel, a country regularly attacked by adversaries, has become a world reference in cyber defense by developing a defense system based on social networks. Rather than being the victim of attacks, the country decided to anticipate and look for information directly on social networks and the Dark Net. The process then consists of identifying, listening, following up, and identifying the people speaking, as well as spying on places where things are being prepared, for example, on forums specializing in terrorism. After that, the teams integrate the enemy groups

to be aware of the whole D-day and to anticipate and prevent a new attack. They identify the hidden social networks of the Dark Net and infiltrate them by creating false identities to anticipate their actions. Once cyber-terrorists have been located, they will be neutralized by internal or external security officers (Forbes, 2018).

Today, most platforms are focused on a two-pronged approach to counter the terrorist use of their tools: human examination and the automated content blacklist that a human examiner had previously deleted. Platforms are also experimenting with a third category of automated scanning that can theoretically signal new messages that may encourage or promote terrorism and route messages for human review. However, these messages are largely limited to a few platforms and focused almost exclusively on text content. Unavoidably, the fight against terrorism cannot be fought without the support of social networking platforms, where extremism takes root and spreads rapidly. Social networks such as X, YouTube, or Facebook must help in the fight against the propaganda of terrorism and develop new technologies to improve further the automatic detection and removal of content inciting terrorist acts.

12.4 Conclusion

The frequency of cyber-attacks through the years has increased dramatically marking, a new era for foreign policies. Cyber interference is an unconventional form of warfare using information technology to disrupt and distort. What makes cyberattacks so harmful is the nature of the attack itself. In these cases, the targets are the citizens and the sphere of influence where propaganda is created. Awareness of security is increasing in an ever more threatening world. Whether these threats reside in the physical, digital, or both, the world's constant vigilance is required to ensure the future. Security is an ongoing endeavor that must continually improve against a dynamic environment of threats (Janczewski, 2008).

The Internet and social media are nowadays considered a vector of radicalization, a kind of incubator also for terrorists. They offer terrorists the opportunity to spread their message and terror, creating panic and terror among the public, recruiting, and guiding global strategies. The growing sophistication of the use of the Dark Web by terrorist groups has become an effective platform for terrorism and criminal activities as well (Weimann, 2016). The numerous abilities of this platform, such as the low cost of performing attacks, the blurry structure of legislation, and most importantly, the anonymity and absence of physical presence, but at the same time, the constant dependence of societies on the internet make it a very attractive field for extremists. On the other hand, it now seems more than vital for governments to develop their cybersecurity.

Counterterrorism agencies in many countries have responded to these new challenges, but the responses have often raised concerns about the prices we pay regarding civil liberties, privacy, freedom of expression, and more. We live in a dangerous world threatened by terrorism, and intelligence agencies, as well as social media platforms, should do their utmost to protect society against terrorist plots. However, they must also do it intelligently, ethically, and with minimal harm to our democratic values (Weinman, 2015).

References

Arquilla J., and Ronfeldt D., 1993. “Cyberwar is Coming!” *Comparative Strategy*, Vol 12, No. 2, Spring 1993, pp. 141–165.

Cavelty D. M. 2010. "Cyberthreats." *The Routledge Handbook of Security Studies*, London, New York: Routledge.

CNN.com, 1999. “Clinton commits $1.46B to fight cyberterrorism.” [ONLINE] Available at: http://edition.cnn.com/TECH/computing/9901/26/clinton.idg/ [Accessed 14 May 2017].

Financial Times. 2016. “Cyber warfare: Iran opens a new front.” [ONLINE] Available at: https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3 [Accessed 8 April 2017].

Finklea K. M., 2015. Dark Web. Congressional Research Service.

Flashpoint a., 2015. "The Islamic State Hacking Division": The Ardit Ferizi Network. p. 2. Available at: https://www.flashpoint-intel.com/wp-content/uploads/2015/10/Flashpoint_ArditFeriziNetwork_Oct20151.pdf [Accessed 8 May 2017].

Flashpoint b., 2015. "Islamic State-Linked Hacker and Abu Hussain Al Britani Associate Arrested for Leak of US Military and Government Personnel Information." Available at: https://www.flashpoint-intel.com/blog/cybercrime/islamic-state-linked-hacker-and-abu-hussain-al-britani-associate-arrested-for-leak-of-u-s-military-and-government-personnel-information [Accessed 19 May 2017].

Forbes, 2013. "How Does Cyber Warfare Work?" Available at: http://www.forbes.com/sites/quora/2013/07/18/how-does-cyber-warfare-work [Accessed 13 March 2017].

Forbes, 2018. "Brexit: Is Russia Getting What It Wanted?" [ONLINE] Available at: https://www.forbes.com/sites/jamesrodgerseurope/2018/12/10/brexit-is-russia-getting-what-it-wanted/#23ec7c374cc7 [Accessed 22 May 2019].

Forbes, 2018. “Can We Finally Stop Terrorists From Exploiting Social Media?” [ONLINE] Available at: https://www.forbes.com/sites/kalevleetaru/2018/10/09/can-we-finally-stop-terrorists-from-exploiting-social-media/ [Accessed 16 May 2019].

Forbes, 2018. “The Fight Against Terrorism Online: Here's The Verdict.” [ONLINE] Available at: https://www.forbes.com/sites/nikitamalik/2018/09/20/the-fight-against-terrorism-online-heres-the-verdict/#1fc9a8424dc5 [Accessed 17 April 2019].

Forbes, 2018. “Where Do Terrorists Go When They Are Kicked Off Social Media Platforms?” [ONLINE] Available at: https://www.forbes.com/sites/nikitamalik/2018/10/18/where-do-terrorists-go-when-they-are-kicked-off-social-media-platforms/#32a6459e3e9c [Accessed 21 June 2019].

Forbes, 2019. "Russia On Brexit: We're Not Gloating." [ONLINE] Available at: https://www.forbes.com/sites/jamesrodgerseurope/2019/01/16/russia-on-brexit-were-not-gloating/#130564cb704c [Accessed 6 May 2019].

Forcese C., 2016. “The ’Hacked’ US Election: Is International Law silent, faced with the Clatter of Cyrillic Keyboards?” *Just Security*. https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/

George, J., Derrick D., Harrison A., Marett K., and Thatcher J., 2016. “The Dark Internet: Without Darkness There is No Light.” *Proceedings of the Twenty-Second Americas Conference on Information Systems*, San Diego, California, August 11-13.

Giantas D., and Liaropoulos A., 2019. *Cybersecurity in the EU: Threats, frameworks and future perspectives*.

Giantas D., and Stergiou D., 2018. "From Terrorism to Cyber-Terrorism: The Case of ISIS." *SSRN Electronic Journal*. https:doi.com/10.2139/ssrn.3135927

Gorodnichenko Y., Pham T., and Talavera O., 2017. "SOCIAL MEDIA, SENTIMENT AND PUBLIC OPINIONS: EVIDENCE FROM #BREXIT AND #USELECTION, *Royal Economics Society Conference*, 12th Annual Conference - Warsaw International Economic Meeting. Available at: https://eml.berkeley.edu/~ygorodni/Brexit_Election.pdf

Grabosky P., 2014. School of Regulation and Global Governance (RegNet) The Evolution of Cybercrime, 2004-2014. "RegNet Research Paper No. 2014/58." Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2535605

Hasbi, A. H., and Mahzam R., 2018. "Cryptocurrencies: Potential For Terror Financing." *RSIS Commentaries*, No. 075, Singapore: Nanyang Technological University.

Idahosa S., 2017. "International Terrorism: The Influence of Social Media in Perspective." *World Wide Journal of Multidisciplinary Research and Development*. 3. 86-91.

Immenkamp B., Sgueo G., Voronova S., and Dobreva A., 2019. "The fight against terrorism." Retrieved from https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/635561/EPRS_BRI(2019)635

Investor's Business Daily, 2016. *Cybersecurity Woes Get Still Worse Under Obama*. [ONLINE] Available at: https://www.investors.com/politics/editorials/cybersecurity-woes-get-still-worse-under-obama/ [Accessed 30 May 2016].

Iqbal Z., 2016. "CYBER TERRORISM: A CASE STUDY OF ISLAMIC STATE," *Journal of Social Sciences.* Retrieved from https://www.academia.edu/39565196/CYBER_TERRORISM_A_CASE_STUDY_OF_ISLAMIC_STATE

Janczewski J. L., and Colarik M. A., 2008. "Cyber Warfare and Cyber Terrorism." Information Science Reference.

Kaspersky, 2020. What is a Botnet?" [ONLINE] Available at: https://usa.kaspersky.com/resource-center/threats/botnet-attacks#.WFu8iLnp0ox [Accessed 30 April 2016].

Kent A., 2006. "Hacktivism and Politically Motivated Computer Crime." *Network Risk Management*, LLC. Retrieved from https://web.archive.org/web/20080227132540/http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf

Kshetri N., 2014. "Cybersecurity and International Relations: The US Engagement with China and Russia," *FLACSO-ISA* 2014, University of Buenos Aires, Available at: http://web.isanet.org/Web/Conferences/FLACSOISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf [Accessed 8 April 2017].

Liang C. S., 2015. "Cyber Jihad: Understanding and Countering Islamic State Propaganda." GCSP Policy Paper 2015/2 - February 2015.

Limnéll J., 2013. "Le cyber change-t-il l'art de la guerre?" *Sécurité globale*, vol. 23, no. 1.

Lister M., Giddings S., Dovey J., Grant I., and Kelly K., 2009. *New media: A critical introduction*. Routledge.

nationmultimedia.com. 2013. "Cyber warfare is the new threat to the global order." [ONLINE] Available at: http://www.nationmultimedia.com/opinion/Cyber-warfare-is-the-new-threat-to-the-global-orde-30203813.html [Accessed 8 April 2017].

NATO, 2017. Warsaw Summit Communiqué. [ONLINE] Available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 15 June 2019].

Norton, 2020. "What is a computer virus?" [ONLINE] Available at: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html [Accessed 24 March 2016].

Ohlin J. D., 2017. "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review*, vol. 95: 1579. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?referer=https://scholar.google.gr/andhttpsredir=1andarticle=2632andcontext=facpub

Pernik P., 2018. "Preparing for Cyber Conflict: Case Studies of Cyber Command." *International Centre for Defence and Security*, Tallinn, Estonia.

PUTIN'S ASYMMETRIC ASSAULT ON DEMOCRAC IN RUSSIA AN EUROPE: IMPLICATIONS FOR US NATIONAL SECURITY (2018), A MINORITY STAFF REPORT PREPARED FOR THE USE OF THE COMMITTEE ON FOREIGN RELATIONS UNITED STATES SENATE, US GOVERNMENT PUBLISHING OFFICE, WASHINGTON US. Available at: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

Reuters, 2017. "UK investigates Brexit campaign funding amid speculation of Russian meddling." [ONLINE] Available at: https://www.reuters.com/article/us-britain-eu-investigation/uk-investigates-brexit-campaign-funding-amid-speculation-of-russian-meddling-idUSKBN1D157I [Accessed 30 May 2019].

Rid T., 2011. "Cyber War Will Not Take Place." *Journal of Strategic Studies*, vol. 35, n 1.

Runkle B., 2015. "Is the Islamic State a Cyber Threat?" [ONLINE] Available at: https://warontherocks.com/2015/09/is-the-islamic-state-a-cyber-threat/ [Accessed 19 May 2017].

Russian Presidential decree No. 1895, 2000. "Doctrine of Russian Information Security." http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Sachan, A. 2012. "Countering terrorism through Dark Web analysis." Computing Communication and Networking Technologies (ICCCNT), 2012. *Third International Conference* (pp. 1–5). IEEE.

Sanger D. E., and Shane S., 2016. "Russian Hackers Acted to Aid Trump in Election, US says." *The New York Times*. https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?_r=0

Scott J., and Spaniel D., 2016. *The Anatomy of Cyber-Jihad: Cyberspace is the New Great Equalizer*. CreateSpace Independent Publishing Platform.

Shaheen J., 2015. "Network of terror: how DAESH uses adaptive social networks to spread its message," NATO Stratcom, Riga, November 2015. [ONLINE] Available at: https://www.stratcomcoe.org/network-terror-how-daesh-uses-adaptive-social-networks-spread-its-message [Accessed 12 March 2019].

Soldatov A., and Borogan I., 2018. "Russia's approach to cyber: the best defense is a good offence, Hacks, Leaks and Disruptions." Chaillot Paper, No.148. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Tabansky L., 2011."Basic Concepts in Cyber Warfare - Institute for National Security Studies." *Military and Strategic Affairs*, Volume 3, No 1, May 2011. Available at: http://www.inss.org.il/uploadimages/Import/(FILE)1308129610.pdf [Accessed 14 Mar. 2017].

Taylor W. R., Caeti J. T., Loper D. K., Fritsch J. E., and Liederbach J., (2006), *Digital Crime and Digital Terrorism*, Pearson.

The Economist, 2012. "Cyber-warfare: Hype and fear." [ONLINE] Available at: http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber [Accessed 8 April 2017].

The Guardian, 2016. UK votes to leave EU after dramatic night divides nation. [ONLINE] Available at: https://www.theguardian.com/politics/2016/jun/24/britain-votes-for-brexit-eu-referendum-david-cameron [Accessed 13 May 2019].

The New York Times, 2016. The Perfect Weapon: How Russian Cyberpower Invaded the US [ONLINE] Available at: https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [Accessed 8 April 2017].

The Sunday Times, 2017. "Russia used Twitter bots and trolls 'to disrupt' Brexit vote." [ONLINE] Available at: https://www.thetimes.co.uk/article/russia-used-web-posts-to-disrupt-brexit-vote-h9nv5zg6c [Accessed 27 May 2019].

Vagianos D., Al Zoampie S., and Spettel S., 2019. "The Rise of Social Bots In Global Cyberpolitics: Convenience In Cyberpower Redistribution." *Cyberpolitic Journal* (ISSN: 2587-1218), Volume 4, Number 7, 2019, pp. 70–89.

Van De Velde J., 2017. The Law of Cyber Interference in Elections. Available at http://dx.doi.org/10.2139/ssrn.3043828

Ventre D., 2011. *Cyberattaque et cyberdéfense*, Paris, Lavoisier.

Warsaw Summit Communiqué, NATO, July 9, 2016. Available at https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Weimann G., 2015. *Terrorism in Cyberspace: The Next Generation*, Columbia University Press.

Weimann G., 2016. "Going dark: Terrorism on the Dark Web. Studies in Conflict and Terrorism," 39(3), pp. 195–206.

Weimann G., 2016a. *Terrorist migration to the Dark Web*. Perspectives on Terrorism, 10(3), pp. 40–44.

Weimann, G., 2017. "Going Darker? the challenge of dark net terrorism." Woodrow Wilson International Center.

www.parliament.uk., 2018. "Russian influence in political campaigns." [ONLINE] Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36308.htm#footnote-121 [Accessed 24 April 2019].

Yayla A. S., and Speckhard A., 2017. "Telegram: The Mighty Application that ISIS Loves." ICSVE Brief Reports.

Chapter 13 Privacy, Cybersecurity and Surveillance in the Digital Age

Abstract

Chapter 13 explains the notions of Information Privacy and Cybersecurity in the Digital Age. Humanity's exposure to the disclosure of personal data and personal information is analyzed, followed by Cybersecurity issues, which represent the way of protecting this information from theft or damage to software or hardware, but also from disruption or manipulation of personal data. In the world of social media, where the user-generated content is diffused across digital social networks, Privacy and Cybersecurity are becoming increasingly importance. The term Surveillance Society is also introduced where governments, corporations, criminal organizations, or individuals can monitor computer activity and data stored on hard drives or being transferred over computer networks. Mass Surveillance techniques are presented and the revelation of E. Snowden on the Mass surveillance planned and organized by the NSA and the FBI is presented here as a Case Study. Eventually, the issue of Censorship in the digital age and the moral consequences that it has brought to society and in governance are presented. Several examples are listed, including North Korea and Turkey but China's case is the most representative one and is thoroughly presented here.

13.1 Introduction

The Internet is increasingly used for economic, political, and social activities. This exposes its users to risks of divulging data and personal information. The Internet offers enormous opportunities to all users, but at the same time, it also harbors risks to privacy and personal data. Controlling the disclosed information is becoming challenging and the legal context can only handle a few times the rapid expansion of an industry that collects and sells sensitive information through an increasing variety of scenarios.

Privacy creates many challenges for governmental institutions through new advancing technologies, which may be abstruse for most people, including the Internet of Things, electronic e-shopping, and social media websites. These technologies collect, store, and use personal for surveillance and marketing purposes. Companies, marketers, governments, and many other actors can use personal data for various purposes, including targeted advertisements according to the user's online profile and history. The Internet of Things refers to the devices that collect and transmit data via the internet for several purposes. It is estimated that over 26 billion connections operate globally, transmitting, in many cases people's private information.

Although such technological shifts, benefit society at large, they raise issues related to individual privacy. Illegal collection and processing of online personal data was quickly recognized as an important contemporary issue and is addressed by law enforcement authorities nowadays.

13.2 Privacy in the Digital Age

13.2.1 Definition

Privacy concerns exist wherever Personally Identifiable Information (PII) or other sensitive information is collected and stored in digital form or otherwise. A broad definition of information privacy (Solove, 2004) corresponds to "*the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.*" The same definition states, "*Improper or non-existent disclosure control can be the root cause for privacy* issues."

Internet Privacy is a subset of Information privacy. It involves the rights of personal privacy concerning the storing, repurposing, provision to third parties, and displaying information about oneself via the internet. Privacy concerns have been articulated from the beginning of large-scale computer sharing. It can entail personally identifying information (any information used to identify an individual, age, address etc.,) or non-PII information, such as a site visitor's behavior on a website.

According to the Organization for Economic Co-operation and Development (OECD), the definition of personal internet data is any information related to the identification of an individual. This definition is very general and involves the following kinds of personal data (OECD, 2013b):

- Contents that an internet user has created, including blogs, photos, videos, and annotations.
- Behavioral data like browser history and e-shopping information.
- Social data, including contacts and friends in social media.
- Location data like house address, GPS, and IP address through a user's phone or PC.
- Demographic data like age, sex, nationality, salary, religious or political beliefs, etc.
- Private data like a name, bank account details, or criminal record.

13.2.2 Personal Data Management Processes

Personal Data management processes include the stages of collection, storage, processing, and distribution (**Figure 13.1**). Many actors work on these stages either in a legitimate way (voluntary concession of personal data) or in an unlawful way (secret user monitoring) and provide the data to third parties.

The actors in these processes can be companies, public organizations, NGOs, or individuals. Also, they can work in some cycle phases. For example, some Data Brokers that typically do not use personal data but analyze and sell them. For instance, an airlines company can keep, analyze, and use personal data from customers for specific sales to every customer according to their characteristics.

There are three kinds of collection of personal data via the internet (OECD, 2013b). First, it is the volunteer way where a person can share personal data on his own, like through one profile on social media. Second, it is the observed way when data are collected and stored legally based on browser history, for example, web browsing preferences and location data in case of using a cell phone. Third, it is the inferred way when personal data needs to be analyzed through smart applications, sensors, etc., for example, credit ratings.

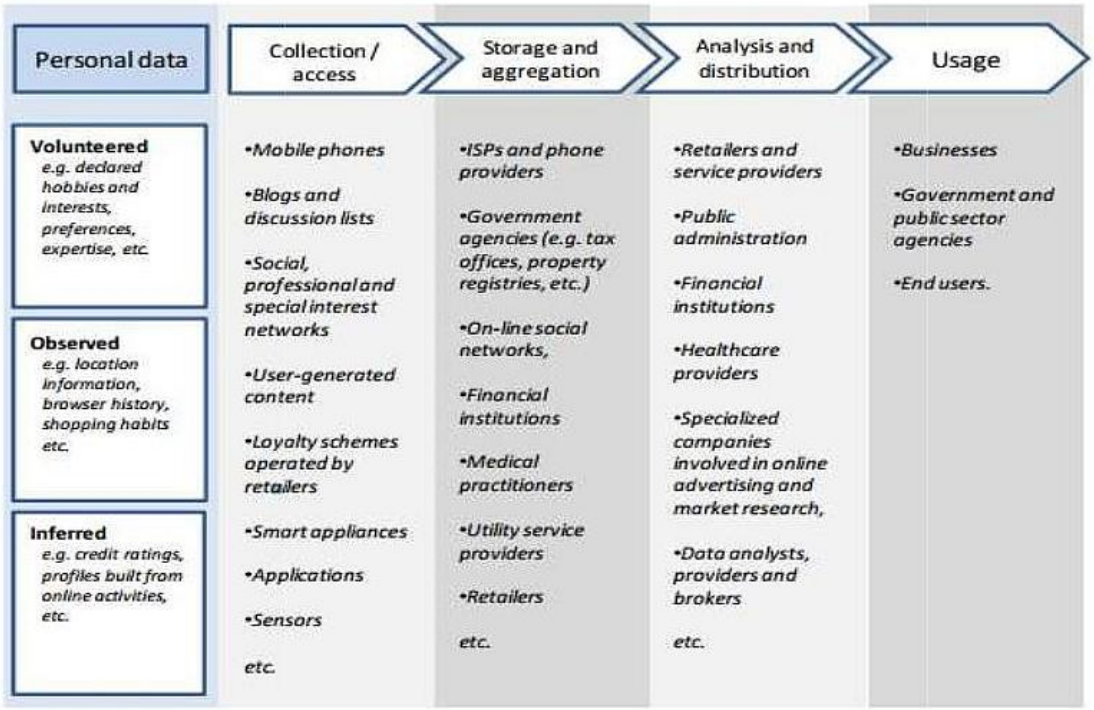


Figure 13.1 *Personal Data management processes (OECD, 2013a).*

13.2.3 Basic Techniques

The basic techniques involved in the above-described personal data cycle are the Cookies, the Web-Bugs, the Click- Stream, and also the Deep packet inspection. Their description is given below.

Cookies

HTTP Cookies refer to data stored on a user's computer that assists in automated access to websites or web features. They are always a common concern in Internet privacy and the most popular way to gain access to personal data. Most advertisers use cookies in order to track their users online (*The Wall Street Journal*, "What they know").

Cookies can be stored on a computer or other “smart” devices connected to the Internet, such as a smartphone or tablet. They allow a site to “remember” and identify users’ actions while browsing. Cookies are used to maintain state information as users surf the Web. Each cookie is unique to a browser and contains some anonymous information.

There are session cookies and persistent cookies. Session cookies are stored in memory, while persistent cookies are placed on the hard disk. Persistent cookies are stored in the Cookies folder under a user profile folder or the Windir\Cookies folder.

The Adobe Flash Player uses flash cookies to store information at the user's computer (used for tracking users' Internet activity). Evercookies are JavaScript-based applications that produce cookies in a web browser that actively “resist” deletion by redundantly copying themselves in different forms.

Cookies can also be First-party or Third-party. First-party cookies are cookies that are associated with the host domain. Third-party cookies are cookies from any other domain. When using third-party cookies, many companies do not have any contact with consumers, to track users' navigation on various websites. Although the consumer has chosen to visit a website with first-party cookies, the third-party cookies may still exist and keep tracking without warning (Hoofnagle et al., 2012).

Generally, cookies are used for many different reasons, such as improving users’ online experience by protecting their preferences, or providing targeted advertising content (Kristol, 2001). While most cookies are perfectly safe, some can be used to track content without your consent. Worse, legitimate cookies can sometimes be spied upon if a criminal gets access.

Web-bugs

Web bugs are also known as” *beacons,*” “*action tags,*” “*clear GIFs,*” “*web tags*” or “*pixel tags*” (Gilbert, 2008). They are small documents sized 1x1-pixel used on webpages and emails to unobtrusively, usually invisibly, allow checking that a user has accessed some content (Olsen, 2002). The fact that they are usually invisible and that they are not stored in a device, is the main difference between cookies. Users can only become aware of being monitored if they inspect the HTML code of the website in question. Using such bugs, companies, and organizations can track the online behavior of web users and record the duration of a visit to a website. Actors doing such tracking were mainly advertisers or web analytics companies. Social networking sites also started to use these techniques, for instance, through buttons that act as tracking beacons (Mann & Reitbauer, 2017). Web bugs can give important information about the users’ interests. According to research, 96% of the Top 50 companies involved in Web business use at least one web bug (Tucker, 2010).

Click-Stream

Click-Stream, also known as clickstream analysis or clickstream analytics, is the process of collecting, analyzing, and reporting aggregate data about which pages a website user visits (Search customer experience, 2016). There are two levels of click-stream techniques: traffic analytics, and e-commerce analytics. Traffic analytics are about the server level and track how many pages are served to a user, how long it takes for each page to load, how often the user hits the browser's back or stop button, and how much data is downloaded before the user moves on (Search customer experience, 2016). E-commerce analysis uses click-stream data to understand the effectiveness of a site as a channel to the market. It deals with what pages the shopper lingers on, what the shopper puts in or takes out of a shopping cart, what items the shopper purchases, whether the shopper uses a coupon code and the shopper's preferred payment method. Clickstream is considered most effective when used with other techniques because of the large volume of data that can be acquired and processed.

Deep Packet Inspection

Deep Packet Inspection (DPI) is a type of data processing that inspects in detail the data being sent over a computer network and usually takes action by blocking, re-routing, or logging it accordingly (Geere, 2012). Deep Packet Inspection enables advanced network management, user service, security functions, internet data mining, eavesdropping, and censorship (Porter, 2005). This methodology is employed by Internet Service Providers (ISPs), and a number of scholars contend that it is associated with illicit surveillance of telephone conversations, while the organization retains the ability to monitor individual communications. DPI is used by many corporations and larger institutions, telecommunications operators and governments (Bendrath, 2009).

13.2.4 Rules and Legal Context Regarding the Right to Privacy

United Nations (UN) is the main international organization that maintains international peace and security, promotes human rights, gender equality, and more. Throughout the years, the UN adopted many resolutions regarding the right to privacy in the digital age because technological development has enabled many individuals to use communication channels that can improve their lives. Nonetheless, companies and governments got the opportunity to take up surveillance practices, data collection, and monitor individual behavior, which may violate the human right to privacy. Consequently, it is becoming the most important human rights issue of the modern age because it is essential to human dignity, and it supports other rights, such as freedom of expression and information, freedom of association, and freedom of speech.

The resolutions were created to protect citizens' privacy worldwide, human rights and fundamental freedoms from threats, harassment, and insecurity caused by "unlawful or arbitrary" surveillance. It states that peoples' offline rights must also be protected online and that people worldwide should enjoy freedom of speech and belief. Also, it encourages States, organizations and business enterprises "*to promote an open secure, stable, accessible and peaceful ICT environment*" and "*to inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency and policies that allow for the informed consent of users, as appropriate.*"

Encryption and anonymity are the measures that are encouraged to be taken in order for the data to be protected and to increase the confidentiality of the individuals who share data in the digital environment. Anonymity is legally safeguarded, and various methods exist for concealing one's identity on the internet, including the utilization of Virtual Private Networks (VPNs). TOR, a specialized browser, facilitates untraceable access to websites. In addition, on the internet, there can be a high level of toxicity regarding online interactivity between individuals, such as cyberbullying, and grooming (explained thoroughly in Chapter 14). Cyberbullying refers to verbal or psychological harassment carried out by a group or individuals through online services and many users targeted by these methods turn out to be profoundly marked, most of them, in extreme cases, even attempting suicide. For this reason, the EU Agency ENISA (European Network and Information Security Agency) has launched a report on cyberbullying and online grooming, aiming to diminish bullying over the internet for teenagers and children because they represent an easy target. The primary function of ENISA is to serve as a Center of Expertise for the European Union and its Member States, by providing guidance and suggestions on effective measures and protocols in information security. Through this report, the Centre of Expertise aimed to enhance the information infrastructure and networks in order to safeguard young individuals from the potential dangers of online grooming and cyberbullying. This report provides detailed recommendations on enhancing the security and privacy of teenagers and children in the online sphere, with a focus on the necessity of managing and supervising potential risks. Furthermore, it urges governments to implement measures for monitoring and preventing such incidents. Under those circumstances, the European Union and the Council of Europe try to strengthen new challenges to the privacy and security of personal data. Besides these international organizations, many states took into consideration data protection principles through numerous national and international consultations. For example, the

United States, Germany, France, and the United Kingdom have passed laws since the 1970s that aim to establish a context for fair information practices to give citizens and consumers' confidence in what is happening with their personal information by governmental and business actors. More than 100 countries have national laws and rules regarding data protection and those laws must be enforced based on several basic international principles that privacy organizations and experts worldwide wrote. Additionally, several other countries are passing laws to protect citizens' data.

The European Union is putting some effort into enhancing the privacy of its citizens. It does so through the General Data Protection Regulation (GDPR), a law that applies to European organizations that want to collect data about customers and people in general. In May 2018, a new version of this law was used. The law states that personal data may only be processed for a justified cause. In addition to this, the processing must be proportional and the best of all alternatives. The justified cause means that the reason for collecting data must be justified. Proportional means that the extent to which the subject's privacy is violated must be in accordance with the cause that the data serves. The processing must be the best of all the alternatives, which means that the data collector should declare that it cannot reach its goals in a better way.

To make sure that the law is followed to the letter and spirit, it is important to be strict in checking whether companies follow the law as it was intended. Recently, in Lisbon at the Web Summit, Margarethe Verstager, the European competition commissioner expressed her concerns and disapproval of the attitude of big companies such as Apple, Google, and Facebook. Evading laws and regulations seem to be a common practice for these companies, also when it comes to privacy issues. Those companies are sometimes fined for their practices. Google, for example, had to pay €2.4 billion to the EU because it had manipulated results from its search engine. However, it is important that also smaller companies are supervised and receive penalties if they are found to be in violating EU rules in order for the GDPR to work effectively.

13.2.5 Legal Context in Greece

The Constitutional Revision of 1975 was completed in 2001, and new needs for protecting personal data under the infiltration of technology in all areas of life characterized the consolidation of Social Rights. Thus, the constitutional basis for the protection of personal data can be found in the constitutional provisions consolidating the right to protection of privacy (Article 9, 1st paragraph, passage B of Constitution), the right to protection of human dignity and free development of personality (Article 5 of Constitution), as well as the more specific right to protection of personal data (Article 9A of Constitution).

Specifically, Article 9A of the Constitution states that: "Everyone has the right to protection from the collection, processing, and use, especially by electronic means, of personal data, as specified by law. Personal data protection is ensured by an independent authority established and operates as specified by law" (Resolution of April 6t, 2001). Furthermore, the provision of Article 9A of the Constitution, according to which "Everyone has the right to protection from the collection, processing, and use, especially by electronic means, of personal data, as specified by law" leads to the enhanced protection of personal data mainly given its processing by electronic means. It is, therefore, obvious that a legal order response mechanism is established against the negative effects brought about by new technologies and which acquires constitutional distinction (Σωτηρόπουλος, 2005).

In this way, the regular provision of Article 9, 1st paragraph, passage β΄ of the Constitution, which proclaims the principle of the inviolability of private life, is supplemented by Article 9A of the Constitution in order to protect the individual from modern informative technology, in cases where the collection of personal data affects the realm of secrecy of private life (Γέροντας, 2002). Therefore, it is the right of the individual to maintain a core in his private life that the state will not be able to penetrate if doing so negates the essence of the individual right and restricts civil liberties.

Indeed, the right to informational self-determination, in other words, the individual's right to know, decide, and determine what information concerning him will be disclosed to others and who may collect and process information concerning him, constitutes a manifestation of the right to privacy protection. The above implies that the protection of personal data extends to private life since, in the modern reality of the society of information and communication, not only the inviolability of the private information realm but also the free and unhindered development of personality, in general, is at stake.

The right to protection of personal data, as defined by provision 9A of the Constitution, relates to interventions in the private realm in light of the most modern forms of offense. Examples of forms of offense about technological developments that are part of contemporary reality are social media (Μάνεσης, 1981). It should be stressed that Article 8, 1st paragraph of the ECHR provides that: “Everyone has the right to respect for private and family life...” from which the ECtHR derives the right to protection of personal data, which even extends to the information about the public life of the individual. Undeniably, Article 9A of the Constitution is inextricably linked to the provision of Article 2, 1st paragraph of the Constitution for the protection of human dignity (provided it is designed to prevent the risk of making the individual a simple information object) and Article 5, 1st paragraph of the Constitution which is the constitutional basis of the right to free development of personality.

Finally, in the range of personal data, we can include all elements of the public and private realm of an individual’s activities. So, information related to the name, image, religious or political beliefs, medical confidentiality, and sexual preferences of each individual are part of the broader range of personal data. In conclusion, the regulatory scope of Article 9A of the Constitution concerns the registration and use of data through computers.

13.2.6 Anonymity for Privacy?

Anonymity and privacy are not synonymous. Something done anonymously remains unattributed to a known actor even if the act itself is made public. Something done privately is intended to be known only by a limited group of trusted parties. Free speech on the Internet is facilitated by anonymity, which allows individuals to express themselves openly without fear of persecution or discrimination.

Anonymity on the Internet protects individuals from persecution, discrimination, and embarrassment. People can also express opinions without scruples and fear of retribution or discrimination by a more powerful majority. In countries that are enemies of the Internet, where censorship is applied, the internet can play a crucial role and, in some instances, can lead to profound impacts. Virtual communities played a pivotal role in cultivating successful revolutions in Egypt, Libya, and Tunisia (the Arab Spring, see Chapter 12) and in the failed attempts to instigate reform in Iran and in the ongoing conflict in Syria. Consequently, the Internet’s freedom and anonymity, cherished and espoused in many democratic countries, are often considered enemies in societies where authoritarian regimes circumscribe social beliefs and political realities. In these countries, Internet liberties are prohibited by legislative and technical methods such as content filtering and erasing accounts.

Obviously, anonymity can also have dire implications. It can help criminals in a variety of ways, such as money laundering, drug trafficking, terrorism, hacking, fraud, child pornography, hate crimes, and bullying (see Chapter 11). It can also help terrorist groups diffuse beliefs or recruit new members and create distributed, layered, and resilient organizations.

13.2.6.1 Anonymity Technical Issues

There are several techniques which allow for anonymity on the Internet:

- Anonymizers,
- Mix networks (Tor, Java Anon Proxy),
- Peer-to-peer networks (Freenet and I2P)
- Anonymous operating systems (TAILS and Whonix).
- They are described in more detail below:

Anonymizers

Anonymizers are tools that attempt to make Internet activity anonymous or untraceable. In these cases, a proxy server implements anonymous Web browsing by being interposed between a client device and the rest of the Internet. Such a proxy server accesses the Internet on the user's behalf, hiding the client device's identifying information. This Proxy server handles user requests and forwards them to the target server.

Mix network

Mix networks are routing protocols that create hard-to-trace communications using a group of servers known as mixes. These proxy servers take in messages from multiple senders, shuffle them, and send them back out randomly to the next destination. This breaks the link between the request source and the destination, making it harder for eavesdroppers to trace end-to-end communications.

Peer-to-Peer (P2P) Networks

P2P networks provide a basic form of anonymity. An anonymous P2P communication system is a peer-to-peer distributed application in which the nodes that share resources or participants are anonymous or pseudonymous.

Anonymization Operating Systems

They are operating systems that have been designed to be anonymous on the Internet. They usually come with Tor, encryption, and many countermeasures prohibiting online tracking.

13.2.6.2 The Onion Router (TOR)

Tor, short for The Onion Router, is free and open-source software for enabling anonymous communication. It uses a free, worldwide (**Figure 13.2**) volunteer overlay network consisting of more than six thousand relays to direct Internet traffic while concealing a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace the Internet activity to the user. Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities unmonitored.

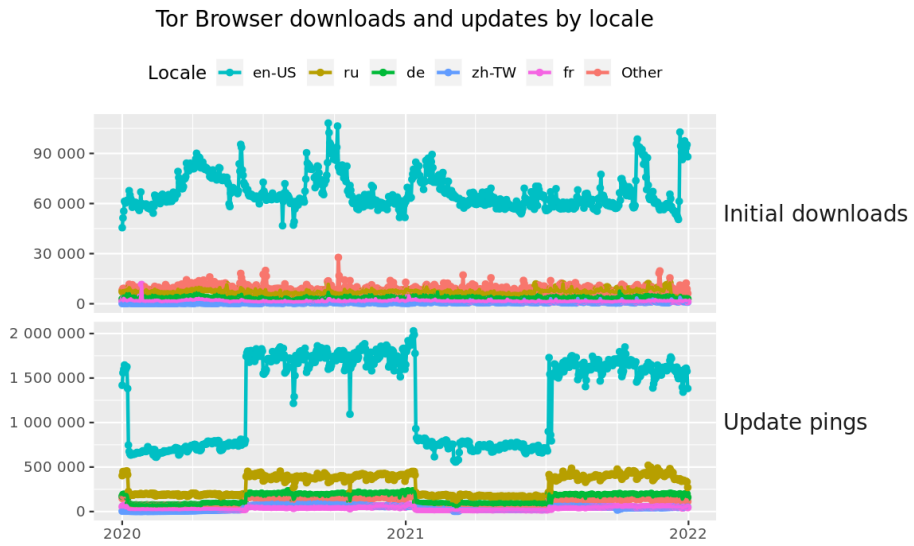


Figure 13.2 *Tor Browsers downloads and updates in years 2020 and 2021 by locale (Source: The Tor Project, https://metrics.torproject.org).*

Tor was initially developed within the US Navy, aiming to protect communications. Today, it is used daily for various purposes by civilians, the military, journalists, law enforcement officers, activists, and many others. Tor's projects motto is to "*protect yourself against tracking, surveillance, and censorship*" and "Stand up for privacy and freedom online." On the other hand, the anonymization of the Tor network is also attractive for people carrying out illicit online activities, such as selling and purchasing illegal merchandise. Illegal websites selling drugs, and weapons, or involved with child pornography are very often hosted within Tor.

Tor is markedly slowing browsing speed. However, alternatives have been developed to increase this speed. Hornet is a high-speed onion routing network that leverages next-generation architecture to make user tracking more difficult. This low-latency onion routing system enables end-to-end anonymous channels. It has been designed as a quicker and more secure alternative to Tor, processing traffic for a practically unlimited number of sources.

The Tor project embodies even its messenger system, the "*Torchat.*" It is a peer-to-peer anonymous instant messenger that uses Tor Onion services as an underlying network and provides cryptographically secure text messaging as well as file transfers. As expected, data traffic is encrypted and it is very difficult to view who is communicating with whom and where a given client is physically located. TorChat is free software licensed under the terms of the GNU General Public License (GPL).

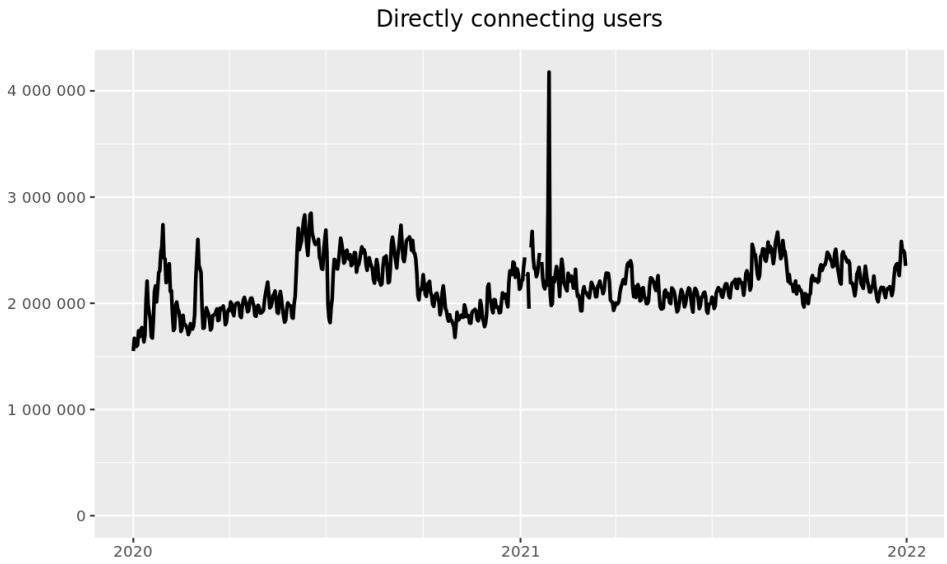


Figure 13.3 *Directly connected Tor users in 2020 and 2021 (Source: The Tor Project, https://metrics.torproject.org).*

Figure 13.3 shows the number of directly connecting users globally in 2020 and 2021. The Tor metrics webpage indicated specific related events in the period of observations. In the 2020-2021 time window (**Figures 13 & 13.3**), two events are mentioned: the blocking of Tor bridges during elections in Tanzania and the Internet shutdowns in Belarus, during protests following a presidential election. As of October 27, 2020, on the eve of Tanzania's 2020 general election, the testing of Tor resulted in many timeout failures, suggesting that access to Tor might have been blocked there. Regarding Belarus, in August 2020, the first major disruption occurred on election day, August 9, 2020, coinciding with the protests that erupted as soon as the election results were announced.

Table 13.1 *Top-10 countries by estimated number of daily ToR clients in 2020 and 2021. (Source: The Tor Project, https://metrics.torproject.org)*

Country	Mean daily users
Russia	10441 (20.53 %)
Iran	8973 (17.64 %)
United States	5999 (11.80 %)
Germany	1976 (3.89 %)
Belarus	1651 (3.25 %)
China	1594 (3.13 %)
India	1416 (2.78 %)
United Kingdom	1295 (2.55 %)
Turkey	1174 (2.31 %)
France	898 (1.77 %)

In 2016, only in Russia, there were about 240,000 households that used Tor services for anonymity on the net. In 2014, Russia offered 3.9 million rubles ($110,000; £65,000) in a contest seeking a way to crack the identities

of users of the Tor network. The Russian interior ministry made the offer, saying the aim was “to ensure the country’s defense and security.: Of course, Tor hinders not only Russian deputies; it can be a worldwide problem. The National Security Agency (NSA), the largest information security service in the US, has repeatedly attempted to develop attacks against people using Tor even though the software is primarily funded and promoted by the US government. In July 2014, the German ARD news reported that the NSA targets the privacy-conscious and that for the NSA every person, who is only interested in the Tor network is suspicious. Two servers in Germany—in Berlin and Nuremberg—are under surveillance by the NSA.

Table 13.1 shows the top 10 countries by estimated mean number of Tor daily users connecting via bridges from January 2020 to December 2021.

13.2.7 Privacy in Social Media

Personal Data Protection (PDP) is an important component of privacy. The growth of possibilities for automated information processing, remote access to different information resources and network communications development has changed the technological aspects of personal data processing. New forms of communication in global Information Systems (IS), such as information sharing, social media, cloud services, etc., have created barriers to enforcing basic directives for PDP. Therefore, the need to apply stronger requirements to data protection policy and information security in all internet communications arises, including Social Networking sites.

The initial step in this direction was the European Commission's proposal the to permit personal data of individuals to be processed only for a short period. Then, it must be removed after completing the legitimate reason for processing. The primary responsibility of data controllers is to ensure reliable protection of collected and processed personal data in social media, and providers must apply the principle of “privacy by default”, considering that only a quarter of online social network users feel in complete control of their I data.

Privacy in social media is concerned with securing users’ information and defending the users’ rights. The task of Social media platforms is to prevent unauthorized access, viruses, and illegal data transfer to third party. Several challenges of social media to PDP are summarized below.

13.2.7.1 Personal Data Protection Issues in Social Media

An important obligation of data controllers is to build a reliable Personal Data Security System (PDSS) that informs each user clearly, understandably, and transparently about handling personal data issues. For example, sensitive data is often required during registration to proceed to use resources on social media platforms. Individuals should know the purpose of registering these data to the platforms. Another issue might be the obligation of the controllers to guarantee easy access to the user’s data. This allows the user’s rights to revise, access, block, or delete their data in the profile, a fundamental right guaranteed by data protection laws. Moreover, access to a profile may also be a problem. The controller must guarantee that each user can apply the restrictions to their profile access to prevent unauthorized access and incorrect dissemination of personal information.

International data transfer is another eventual problem of privacy in social media platforms. According to the main principles of PDP, personal data may be transferred to another country or other countries if their level of PDP is adequate. Data transfer between different service providers is a typical procedure in social networks, as the nodes (servers, clients, storage, etc.) may be located anywhere in the world. Any personal information uploaded to social media must be protected according to the rules of PDSS. Social media users must be informed about all possible data transfers from one service provider to another within or outside the territorial borders of a country.

Moreover, users wishing to delete data from their profiles should be assured that it will be permanently deleted. Sometimes, data may be transferred to another service provider, and a copy of the data can be stored in a different place or places. Furthermore, it is also possible that the information deleted or removed by a user has been passed to a third party before deletion. Data protection legislation gives strict rules for deleting personal data in traditional cases. Nevertheless, when it comes to social media, the regulations lack clarity and specificity. In many cases, the social media platforms point out issues like that in their policies, but that does not necessarily mean they comply with the data privacy laws. Moreover, the European Union had asked Google to delay the onset of the new privacy policy to investigate the issue and ensure that it does not violate EU law. It is true that in many cases, the updated policies have not been approved by certain countries like Canada and Germany, which have both held investigations into the legality of Facebook against respective privacy acts in 2010. There have been incidents in which certain policies have been rejected or asked to be altered for a platform to operate legally in a country.

Eventually, the technical implementation of appropriate measures for information security is an important issue for data controllers. These measures should counter all forms of destruction or loss of personal data or illegal processing. Service providers must guarantee the effective protection of personal information. However, implementing additional or more effective data security measures increases the cost of PDP procedures and can be a reason for aborting the application of certain measures.

13.2.7.2 Privacy Incidents in Social Media

Even though there has been substantial progress in technical developments regarding social networks, violations that halt any real, transformative change related to privacy issues are still encountered. Here are some examples:

WhatsApp

WhatsApp originally prided itself on privacy until Facebook bought it. WhatsApp then announced that, under its new terms and conditions, it would share personal information with its parent company, Facebook, claiming that these changes were in the user's best interest, assisting in fighting spam and increasing business-to-consumer communication.

Uber

Uber updated its app to track users' locations even when not using it. Uber claimed it was just data collection and analysis to improve the pickup and drop-off experience. As a result, Uber was fined for providing unauthorized third-party access to drivers' personal information and using aerial tracking to identify riders.

Fitbit

The year 2016 saw a surge in fitness trackers, one of which is Fitbit, which, although a helpful service, revealed a lack of data protection. This is due to outdated measures for information security that should protect sensitive patient data. In such a case, Health related information was shared with companies such as Fitbit which could forward this data to potential advertisers.

Pokémon Go

Pokémon Go became a worldwide phenomenon. However, Pokémon Go's full functionality requires access to a user's entire Google account on iOS, including location data, email and browsing history. Pokémon Go tracks where users go, how they get there, and how long they stay. There have been worries that the app itself could lead children astray and even put them in harm's way.

Snapchat

Snapchat's Spectacles help users survey, record, and post a view without the permission of those caught on video. Users would surely be less likely to express themselves freely if they felt they were being recorded at all times. Such technology can be considered as invasive.

Facebook

In the 2010s, personal data belonging to 87 million Facebook users was collected without their consent by British consulting firm *Cambridge Analytica*, predominantly to be used for political advertising. The data was collected through an app called "This Is Your Digital Life," developed by a company named *Global Science Research* in 2013. The app collected the personal data of the users' Facebook friends via Facebook's Open Graph platform. Cambridge Analytica used the data to assist the 2016 presidential campaigns of Ted Cruz and Donald Trump. It was also widely accused of interfering with the Brexit referendum. However, the official investigation recognized that the company was not involved "beyond some initial inquiries" and that "no significant breaches" occurred.

The Newsfeed Timeline

Social media sites and search engines use algorithms to change the time order. Major sites such as Facebook and Instagram radically change algorithms, changing people's news feeds. As a result, news feeds and timelines are not shown to the public in real time; the algorithms of Facebook, Snapchat, Instagram, and X manipulate them to display posts and content they assume the population wants to see. The fact is, that algorithms ruin relevancy and introduce delay. While news feeds are meant to be objective, these equations make them subjective, and this is accomplished by mining what users do online. Hence, people are violated twice by the invasion of privacy and the control of what they see, what they do not see, and when they see it.

X, Facebook, and Instagram

In 2016, an act of racial profiling and user surveillance was made public when X, Facebook, and Instagram were called out by the California branch of the ACLU (American Civil Liberties Union) for sharing user data with a social media monitoring tool that tracks activists' conversations. Facebook was similarly called out in 2016 for allowing advertisers to exclude specific "Ethnic Affinities," which the company unveiled by collecting facts about users' likes and friends, which can be considered a racist act and a violation of federal law.

Yahoo

A few years ago, Yahoo announced that 500 million user accounts had been breached. It was revealed that Yahoo had allowed US intelligence agencies to read through its users' messages in search of red flag phrases or keywords. Yahoo also announced that one billion user accounts had been hacked in 2013.

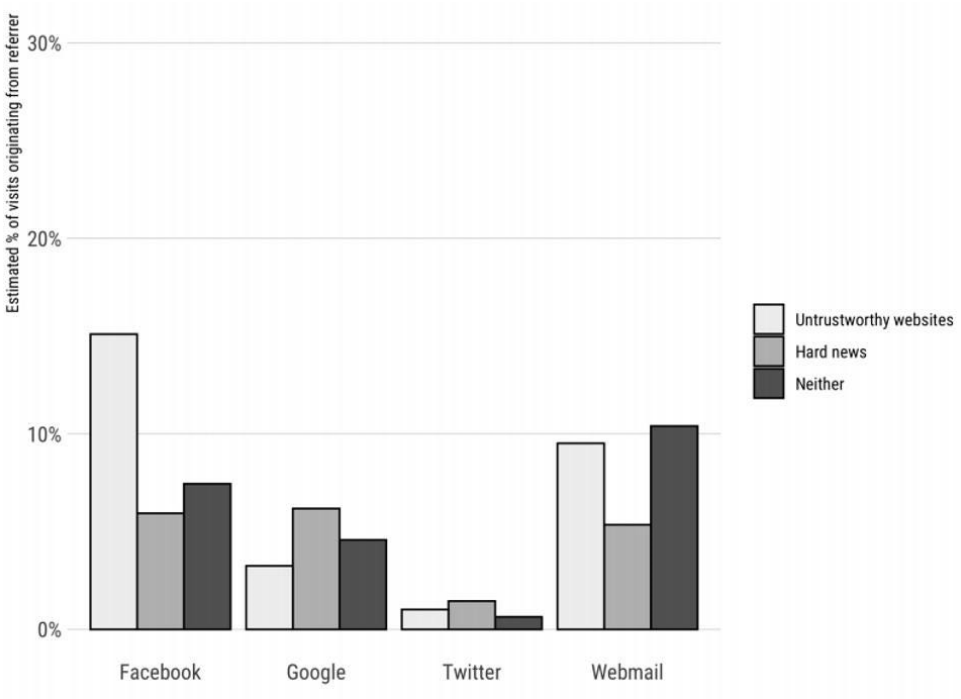


Figure 13.4 *Referrers to untrustworthy news websites and other sources (Source: Guess et al., 2020).*

Eventually, an issue indirectly related to data privacy is the phenomenon of fake news. Data privacy may offer a more precise solution. Data privacy laws like the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) do not address fake news or harmful speech. As mentioned earlier, their main goal is to give users greater control over their personal data, allowing people to check what data has been stored, opt out of data sharing, or erase their data entirely.

Data privacy laws can render disinformation a weapon without a target, by limiting access to information that enables personalized ad targeting and polarization loops. Without detailed data on users' political beliefs, age, location, and gender that currently guide ads and suggested content, disinformation is more likely to be lost in the noise.

Facebook is the most capable perpetrator of spreading fake news (**Figure 13.4**). This is according to a study published in *Nature: Human Behavior*. A team of researchers from Princeton University tracked the internet use of over 3,000 Americans in the lead up to the 2016 presidential election. They found Facebook to be the referrer site for untrustworthy news sources over 15% of the time. By contrast, Facebook referred users to authoritative news sites only 6% of the time. **Figure 13.4** below depicts the size of the effect.

There is, however, another side to the privacy issues described above; it is coming from the social media websites themselves, namely their possibly insufficient privacy policy, bugs, or lack of attention to the users´ privacy. The following paragraph will present a representative example of the Facebook security breach of September 2018.

13.2.7.3 The Facebook Security Breach of September 2018

In June 2013, one of the *White Hat* hackers discovered a bug inside the Facebook system. This computer security specialist breaks into protected systems and networks to test and assess their security. The bug left around 6 million phone numbers and e-mail addresses exposed to anybody with at least some connection to the people whose information was unprotected. This occurrence primarily arose due to the introduction of a feature on Facebook aimed at increasing user registration and account creation, namely the option to upload personal contact lists. Consequently, the platform was able to generate friend suggestions by cross-

referencing these lists with those of other individuals. Unfortunately, it also left these matching contacts extremely vulnerable to the bug, that was later fixed and affected users were notified (Newcomb, 2018).

By February 2018, the Belgian Commission for Protection of Privacy (CPP) had had enough of Facebook breaking Belgian and European privacy laws by collecting its Belgian users' private information and tracking people more accurately on third-party websites through cookies. The court demanded that Facebook delete all illegally collected data (including people who were not Facebook users), or it would be fined up to 125 million dollars. The court said that Facebook informs people "insufficiently about gathering information, the kind of data it collects, what it does with that data, and how long it stores it" (Bartunek, 2018). According to the Belgian ruling, the platform not only does not inform people, but it does not have the consent to collect and store personal information in the first place (Gibbs, 2018). Facebook eventually complied with this ruling and even launched a campaign stressing the importance of users´ privacy (Bartunek, 2018).

The security breach of September 2018 mentioned in the previous paragraph) was probably the worst failure of Facebook by that time. Cambridge Analytica was a political data consultancy company hired by the US president Donald Trump´s 2016 election campaign. Before that, the firm provided its services to a wide range of clients such as Mastercard, the New York Yankees baseball team, various Joint Chiefs of Staff in the White House, and Republican presidential candidate Ted Cruz, who first wanted to use the sensitive data harvested from Facebook to gain an advantage over Donald Trump (Davies, 2015). During Trump´s campaign later, when Ted Cruz failed, Cambridge Analytica gained unauthorized access to personally identifiable information (PII) and Facebook accounts of approximately 87 million users and later used this data to possibly influence voters´ behavior by targeting them with all kinds of ads and e-mails (Granville, 2018). Even Facebook´s CEO and co-founder Mark Zuckerberg´s data was reportedly accessed by Cambridge Analytica. After this, Facebook failed to restore its users´ trust. A survey conducted by the Ponemon Institute in April 2018 showed, that only 27 percent of the respondents could say that "*Facebook is committed to protecting the privacy of my personal information.*" This number was around 79 percent in 2017 (Kuchler, 2018).

Facebook may have gained a small amount of its users´ trust since the Cambridge Analytica scandal. However, it would soon lose it when a cyber-attack left nearly 50 million accounts exposed to attackers, meaning a security breach believed to be the biggest in the company´s 14-year history. According to Facebook, this was only possible due to a security hole that remained unnoticed for more than a year after the site introduced the "*view as*" feature in July 2017. This feature allowed people to see what their profile looks like to other users (Wong, 2018). Ironically, the feature was meant to give users more control over their privacy, which made the whole affair even more embarrassing for a company such as Facebook.

Nevertheless, the hackers took advantage of this hole and exploited it. They were able to steal access "tokens," basically a form of a digital key, giving anyone having them in possession a possibility to not only log into a person's account (given that the attacker owns this person's token) but also to take complete control of this account. These tokens were initially introduced for the users to stay logged in throughout multiple browsing entries and not have to enter their password whenever they want to open Facebook.

According to the social network's VP of Product Management, Guy Rosen, the social media platform first noticed unusual activity on September 14, and by Tuesday 25, it was identified as a cyberattack by Facebook's engineers. Two days later, Facebook patched the hole, reset the tokens to avert accessing any further information, and notified all users who might have been affected. Rosen also said that it was not clear who was behind the attack but suggested that it could be the work of an organized group.

The chief executive of a cyber security company, Senseon, David Atkinson, said that the details of this breach "*indicate that this hacker is toward the sophisticated end of the spectrum,*" suggesting that it could be not only an organized group but a nation state attack. It also came in handy just weeks before the US midterm elections, where Facebook was a big target, especially for Russian agents who have been messing with multiple

US elections in the past. In early October, the company changed the number of attacked users from 50 million to 30 million and informed that the attackers could have accessed around half of those accounts (Rodriguez, 2018).

Hence, the attackers gained access to the accounts of millions of people and were able to get to their profiles personal information such as name, birthdate, phone number, e-mail address, relationship status, or religion, but also could have gotten into apps like Instagram or Spotify because these apps were giving users an option to log into their system through their Facebook account (Isaac & Frenkel, 2018). However, the social media platform found no evidence of hackers accessing third-party apps or other Facebook owned apps, e.g., Messenger or WhatsApp. VP Guy Rosen also said that the attackers did not get their hands on any credit card information associated with any member´s account and that nobody reported to the company anything about any stolen information being laid out and accessible on the Dark Web.

After discovering this security hole, the first and immediate reaction was Facebook's ordering its engineers to fix it, followed by calling the relevant law enforcement and even the FBI to investigate who was behind the attack. The social media platform also notified the affected users about what personal information might have been stolen and advised them to be highly alert for suspicious e-mails, calls, or messages. Finally, the company introduced a security notice page where every user could check whether his or her account had been affected.

This security problem also gained much attention from various governments, starting with the US Congress, since Facebook is originally an American company. One of the Democratic Senators from Virginia, Mark Warner, who is one of the top Facebook critics, said that "*this is another sobering indicator that Congress needs to step up and take action to protect the privacy and security of social media users,*" which sparked a big debate on this topic.

13.2.8 Artificial Intelligence and Privacy

Artificial Intelligence (AI) is envisaged to be the next revolution in the field of technology. Nowadays, smart computers perform more than a billion instructions per second, which is definitely a huge technological accomplishment. However, AI goes a step further. Instead of just following pre-programmed instructions, AI exhibits learning capabilities to technology. However, a clear and consistent definition does not exist, mainly because "intelligence" is a complex term to define. A test for AI that is often used is the so-called "Turing test." The main idea of this test is that if a computer can "fool" a person into believing that he is a human instead of a computer, the computer must be "intelligent" (Mauldin, 1994). This test was founded by Alan Turing in 1950 when he proposed the so called "Imitation game," and he predicted that around the year 2000, computers would exist that could fool an average person for 5 minutes.

Nowadays, data streams from smartphones and other online devices expand the volume and variety of information about every aspect of our lives and bring privacy issues into the foreground. Artificial intelligence is likely to accelerate this trend. Much of the most privacy-sensitive data analysis today, such as search engine algorithms and recommendation engines, is driven by AI applications, such as machine learning. As artificial intelligence evolves, it increases the ability to use personal information in ways that can intrude on privacy interests (Kerry et al., 2020).

An example of a procedure such as the one described above is the case of chatbots. |These robots emulate human behavior by discussing certain issues serving a variety of applications with Internet users (Kouroupis et al., 2022). In these cases, Internet users get involved in acquiring personal data through chatbots with their consent to train them and get back services they have been designed for. In Chapter 15, the case of chatbots for Customer Relationship Management (CRM) will be presented.

However, as expected, disclosing personal information to a robot raises many privacy issues. While users appreciate the guidance and support a chatbot can provide, they also must share a large number of personal information with the chatbot to receive, e.g., correct recommendations. By doing this, some network entities store a lot of data about users, who are sometimes unaware of this situation.

Data protectionists criticize how companies collect and use our data, highlighting that users must be aware of the data they share, such as their location, name, or previous history. Most users look at the convenience of talking with a bot, ignoring the consequences. For example, research from the University of Northeastern supports that Amazon's Alexa bot records "accidentally" everything we say. So, this personal assistant collects data even when a user does not interact with it. It has been proven that Alexa is activated by herself several times and records as much as 40 seconds of audio information each time. Amazon knows everything about every customer, by tracking location and creating vast meta-data, either accidentally or not, (Kouroupis et al., 2022). Although it benefits marketing strategies, Amazon can share users' information with other organizations (Kojouharov, 2018).

Another similar example is Google Assistant. This bot recommends nearby places to eat, informs about the weather, and personalizes certain needs. However, it has been argued that sometimes users are being recorded without saying the trigger phrase "Hey Google." There are witnesses that personal assistants like Siri, Cortana, and Google have been activated because they thought someone said the 'wake up' word. Moreover, it has been argued that Google suggests a search term, or an advertisement based on a conversation users had with another person (Morrison, 2020).

The increase of bots in chat platforms is rapid. What is missing is that as these interfaces evolve, a data control shift occurs from users to Messenger or Facebook. Not only do companies who upload their bots in these platforms store users' data, but also Facebook and Messenger have the right to do that according to their policies. Both have the potential to become strong data brokers. All conversations or transactions within these platforms are also stored and filtered based on personal users' IDs and can be sold to governments or other organizations. A great example is the "Cambridge Analytica" scandal described before, where a politician used a personal quiz initially approved by Facebook. Because of this scandal, developers could not upload temporary new chatbots on Facebook's platform (Skandali, 2018). For this reason, Digital Liberties organizations have already expressed concern about these trends, and several technical solutions have been proposed. One such idea for Facebook could be to introduce private channels with a high level of encryption between the user and the chatbots so that Facebook would know the bots with which a user interacts but not their conversation (Harkous, 2016).

13.3 Cybersecurity

13.3.1 Definition

Cybersecurity protects information systems from theft, damage, disruption, and manipulation of user data. More concretely, it represents all the methods used to protect personal or governmental data or companies' information from being stolen, contaminated, or destroyed by malicious programs, persons, or other states, but also how personal information is used and protected on the Web. According to *IT Governance*, Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

The concept of cybersecurity first appeared in the 1990s and was used to defining the risks that could affect computer networks and the devastating effects of the rising threats. Cybersecurity falls within cyberspace, the environment where communication over computer networks occurs. According to Joseph

Blankenship (2013), the term cybersecurity was preferred by 15% of the questioned people besides information security (47%), network security (12%), IT security (9%), and Internet security (6%).

Statistically, there is an annual cost of identity theft of $37 billion and an average cost varying from $1 million to $57 million spent by companies to recover after being victims of large cyberattacks. Moreover, according to the Global Security Industry Alliance, an average company loss of $234,000 per cybersecurity breach exists.

Cybersecurity issues can be divided into identity, risk, and incident management. The first refers to the difficulty of finding if identity data have been compromised. It is often impossible to track identity breaches because systems are often incapable of distinguishing between the original identity possessor and the impostor. Risk management is usually associated with risk and awareness. The affected parties usually think of their loss after a cyberattack and do not care about the vulnerability of their system. They are often critical and evaluate the necessity of certain cybersecurity measures, and they do not manage sufficiently their risk. I Incident management refers to how governments or businesses handle a large-scale security breach.

13.3.2 The CIA Triad

There are three basic cybersecurity principles (Brathwaite, 2021): integrity, availability, and confidentiality (**Figure 13.5**). Confidentiality refers to protecting information from being accessed by unauthorized parties. This means ensuring that only authorized users have access to information. When information is read or copied by someone without authorization, the result is known as a loss of confidentiality. For some types of information, confidentiality is a very important feature. Examples include research data, medical and insurance records, and government investment strategies. Some of the critical security controls that you can use to maintain confidentiality are encryption, strong Passwords, 2FA (Two factor authentication), IAM (Identity and Access Management), proper technical controls and physical locks and doors (Brathwaite, 2021).

Figure 13.5 *The three principles of Information Security. (Source: Brathwaite, 2021)*

Availability of information refers to ensuring that authorized parties can access the information when needed. This means ensuring that the information is accessible to authorized people whenever needed. In order to do this, there are several practices such as off-site backups, disaster recovery and business continuity planning, redundancy, failover (backup systems), virtualization processes, and proper monitoring of the environment to address security issues as soon as possible (Brathwaite, 2021).

Integrity is the trustworthiness and dependability of information. This means protecting information from being modified by unauthorized people and ensuring that the information is trustworthy and accurate. Some controls that can be used to maintain integrity are hashes, secure backups, and user access controls (Brathwaite, 2021).

Contemporary information security management recognizes the urgent need to involve individuals and processes, and the most traditional issues of technology security to ensure the quality of information and cybersecurity in all modern organizations. A new method of analysis, a community-based cyber security exercise, is needed to test security issues throughout the system. All security measures mentioned above, along with firewalls, intrusion detection software, and high-level encryption, must be appropriately set up to provide adequate security.

13.3.3 Primary Actions for Cybersecurity

Taking into account the transnational nature of Information Technology and cyberspace, the technical and legal challenges in ensuring the security of Information Systems and Networks, as well as the relevant impacts on socio-economic life, the primary actions for creating a secure cyber eco-system include a series of enabling processes, immediate actions and collaborative efforts within the state and beyond, which covers the following:

- Creating a favorable legal environment to support safe and secure cyberspace, adequate trust and confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders, and effective prosecution.
- Protection of IT networks, gateways, and critical communication and information infrastructure.
- Effective cybercrime prevention and prosecution actions in all the ICT applicable environments.
- Installation of 24×7 emergency response and crisis resolution mechanisms in cyberspace and crisis management through effective preventive, predictive, protective, response, and rehabilitation actions.
- Creating the necessary awareness of the situation regarding the threats to information and communication technology infrastructure (ICT) to identify and implement the appropriate response.
- Proactive preventive and reactive mitigation measures to approach and neutralize source problems and support creating a global security ecosystem, including public-private partnership agreements, exchange of information services, bilateral and multilateral agreements with applicable overseas state agencies, security agencies, and security vendors.
- Policies, promotions, and actions for compliance to International Security best practices and conformity assessment (Product, Procedure, Technology, and People) and incentives for compliance.
- Internal development of appropriate security and technology techniques through frontier technology research, solution-oriented research, concept proof, pilot development, etc., and the development of secure IT.
- Data protection during the process, handling, storage, and transfer and protection of sensitive persons and information to create a necessary environment of trust.
- Creating a cyber-affected culture for responsible behavior and user actions.
- Regularly check online security archives, such as those maintained by incident response, for security alerts and technical advice. Regularly check with vendors for the latest fixes and keep systems current with upgrades and patches.
- Audit systems and networks as well as regularly check logs. Many computer security websites report that insufficient control data is being collected, so detecting and tracing a cyber-attack is difficult.

At a state level, information security and information systems actions must be done at different levels in E-Governance. It is, therefore, the responsibility of the State to bring in sufficiently strong legislation (see Chapter 11) to discourage and put down the misuse of the Internet and other cyber media for any nefarious activities. Nevertheless, besides the government's actions, other stakeholders such as Internet service providers (ISPs), large businesses, and home users are also required to enhance cyberspace security. Employees with daily access to e-government systems must be properly trained in all the latest cybersecurity challenges as part of their job. Bowen et al. from the Department of Computer Science at Columbia University suggested a model to measure, quantify, and evaluate the human factor in cybersecurity issues that showed that the human factor is of great importance and that proper training can significantly contribute to making users fully cognizant of potential threats (Bowen et al., 2011).

13.3.4 Cybersecurity in Different Areas

13.3.4.1 Cybersecurity for States

As stated above, a state must adopt a national cybersecurity strategy. Today, if a country cannot control its cyber assets, it is not secure. Examples of nation-on-nation cyberattacks abound, while criminal-on-nation attacks occur daily, as presented in **Chapter 12**. If a country does not have secure systems, its citizens are vulnerable to privacy invasion. The financial institutions that support the economy are vulnerable to theft with insecure cyber systems, and a country's critical infrastructure is always at risk if a country is not mature.

There are annual reports that rank countries globally based on several cybersecurity indices. The International Telecom Union (ITU) produces an annual Global Cybersecurity Index. This Index is the most thorough ranking of country-by-country maturity. The report looks at countries in terms of their maturity in terms of legal, technical, organizational, capacity building, and cooperation. There are also indices provided by companies such as *Analytics Insights*, *CyberDB,* and *Comparitech*. At the time of writing, the diverse listings of the top five countries, according to 4 different cybersecurity indexes, are presented in **Table 13.2**.

Table 13.2 *Top-5 countries according to ITU, Analytics Insights, CyberDB, and Comparitech listings for 2021 (Source: https://cipher.com).*

	ITU	Analytics Insights	CyberDB	Comparitech
1	United Kingdom	**USA**	**USA**	**Japan**
2	USA	**Russia**	**Israel**	**France**
3	France	**Israel**	**Russia**	**Canada**
4	Lithuania	**China**	**Canada**	**Denmark**
5	Estonia	**Spain**	**United Kingdom**	**USA**

In Greece, the National Cyber Security Strategy is implemented by the National Cyber Security Authority, which was founded to bridge the organizational and coordination gap among the stakeholders involved in cyberspace security in Greece, both in the public and private sectors. Furthermore, the National Cyber Security Authority evaluates, revises, and updates the National Cybersecurity Strategy, if required, every three years at the latest (ENISA, 2016).

The National Cyber Security Strategy consists of two phases: the development and implementation of the Strategy in the initial phase and its assessment and review in the second phase. These phases determine

a continuous lifecycle, in the sense that the National Strategy is first developed and implemented, then assessed according to predetermined assessment indicators, and, if necessary, revised and updated (ENISA, 2016).

The stakeholders involved are divided into two levels: strategic and operational. The National Cyber Security Authority is a high political and governmental stakeholder with extended competencies, that monitors, implements, and bears overall responsibility for the National Cyber Security Strategy. The National Cyber Security Authority exercises its competencies by contributing to a National Advisory Body/ Forum in which all the public and private sector stakeholders cooperate closely with the national Computer Emergency Response Team (CERT). Within the framework of its competencies, it monitors, coordinates, and evaluates the work by the stakeholders involved to achieve the strategic actions and objectives. The operational level includes, among others, the Computer Security Incident Response Teams –CSIRTs, also known as Computer Emergency Response Teams–CERTs, of the public and private sector, who are responsible for dealing with cyber incidents as per their competencies (ENISA, 2016).

13.3.4.2 Cybersecurity for Banks

Information security is of utmost importance in the banking sector. However, banks have always been subject to cyberattacks. According to previous investigations, banks invest in cybersecurity just enough to make customers trust them (Longitude research, 2013). This may happen due to the lack of internal resources and the banks' approach to cybersecurity from a return-on-investment perspective.

SecurityScorecard (Security Scorecard, 2017) conducted research by analyzing 7111 financial institutions in the US and found out that in the top 20 commercial banks, 75% are infected with malware, and 95% possess a low-security level with US Commercial Bank registering the lowest level of security comparing, with other financial organizations in the top 10. Moreover, the main issues found by *SecurityScorecard* are related to the SSL configuration and the e-mail system.

Banks must first re-evaluate existing back-office and front-end controls and processes to protect data as it travels across the enterprise. They should include additional verification layers and security systems with multi-level checks to ensure safe transactions across different channels. Moreover, new technologies can establish new ways to prevent cyberattacks. Cloud computing, for instance, can provide a very high level of data protection, especially for sensitive data that includes customer information. Blockchain technology on the other hand, can allow data and funds to be transferred in a fully secure manner thanks to sophisticated coding and encryption.

13.3.4.3 Cybersecurity for People

According to *InternetLiveStats* (2014), over 3,4 billion people use the internet. Regarding cybersecurity, *Norton Security* says that 76% of them know they need to protect their information online even if they do not do anything about it, and 35% have at least one unprotected device. Concerning Wi-Fi, 87% of people have this a kind of network at home, but only 34% secure it. Only 29% of consumers know and use a public wireless connection properly without entering personal data online when connected (Norton, 2016). For example, *Avira* offers users a new application called Phantom VPN, which secures financial transactions, passwords, and other private files and prevents advertisers from tracking customers by giving them the impression of anonymity from an ever-changing location (Avira Operations GmbH, 2016).

All these statistics show that users are vulnerable and exposed to many dangerous and unknown risks. Indeed, there are a lot of available solutions, given that users are aware. In an article published by The Guardian, some advice is presented to protect personal computers and information: an updated operating system, an antivirus, a secure browser, applications that can prevent attacks using JavaScript, closed ports, a

firewall, and many other tricks which can make a computer safer (Schofield, 2015). For example, Bitdefender, a security provider, offers *TrafficLight. This* free cross-browser add-on intercepts, processes, and filters all Web traffic, blocking malicious content and making a browser more secure. It also offers *Safepay*, a protected browser that emulates a sealed environment that is designed to keep online banking, e-shopping, and any other type of online transaction private and secure, including a manager password for speeding up online shopping and protecting against fraud, phishing, viruses, and keylogging.

13.4 The Surveillance Society

13.4.1 Target Surveillance and Mass Surveillance

"Government surveillance" is defined by *dictionary.com* as a noun that states "close observation or supervision maintained over a person, group, etc., especially one in custody or under suspicion" (Merriam-Webster.com). The word was also taken from the French word "*surveiller*", which means to watch over, and was adopted and changed to the English word surveillance.

Before technological advancements, surveillance on a large scale was difficult to achieve and very costly but as technology got cheaper and cheaper, mass surveillance proliferated. However, it was not until the terrorist attacks on New York's World Trade Center, or more recent attacks on European soil in countries such as France or Germany, that mass surveillance and security began to expand. Technological advancements, especially in developed countries with internet access, have made mass surveillance a very easy task. Most of the population is engaging in activities such as using social media, through which massive amounts of data are generated and processed by tech giants and governments. Companies like Google or Facebook have been implicated in huge scandals regarding data privacy and collecting data (e.g., Cambridge Analytica).

According to *USLegal,* mass surveillance is characterized as the distributive close observation of an entire population or a substantial fraction of the entire population. Nowadays, governments perform mass surveillance of their citizens to protect them from dangerous groups such as terrorists and criminals and maintain social control. The disadvantages of mass surveillance are that it often violates the right to privacy and the political and social freedoms of individuals. It is also argued that mass surveillance will result in the creation of a totalitarian state or electronic police state. So, although there are downsides to mass surveillance, there has to be a trade-off between privacy and security, as both are essential for democratic societies to prosper.

Unlike "target" surveillance, mass surveillance does not address certain individuals. Mass surveillance is also called "non-directional" or "dragnet" surveillance. This refers to the situation where hundreds, or millions of information about hundreds, or thousands, or millions of people are collected daily.

13.4.1.1 Post 9/11 Surveillance in the United States

In the wake of the 9/11 terrorist attacks in the US, contemporary society has witnessed a proliferation of surveillance technology (Tai, 2005). 9/11 attacks on American soil were a decisive marker in the shift toward a culture of control in the US (Cohen, 2010). After the attacks, the US Congress adopted a document over 300-pages, namely the USA PATRIOT Act. The act aimed at improving the capacity of US authorities to detect and deter terrorism. The law, whose title is an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, would have done nothing, according to the Justice Department, other than to extend the application of tools already used against drug dealers and organized crime. It has allowed authorities, including intelligence agencies, to use surveillance and listen to telephone calls to investigate terrorist offenses. Cohen (2010) argues that the Patriot Act was signed without careful examination by Congress and provided a pretext for restricting civil rights, particularly privacy and the

right to be kept informed. The respective legislation gave new powers to the Department of Justice, the National Security Agency (NSA), and other federal agencies regarding the internal and international surveillance of electronic communications and eliminated legal barriers that prevented law enforcement agencies, intelligence agencies, and defense structures from sharing information about potential terrorist threats and coordinating counter-terrorism efforts.

The National Security Agency (NSA) was founded in 1952 to provide an effective, unified organization and control of the communications intelligence activities of the United States conducted against foreign governments and to provide integrated operation policies and procedures about it. It is responsible for collecting, monitoring, and processing information, foreign and domestic. Between 2001 and 2007, the NSA conducted the famous warrantless surveillance or warrantless wiretapping through the Terrorist Surveillance Program. Vast amounts of data were collected from people on the US territory and US citizens by the NSA. Mark Klein, a former AT&T technician, claimed that in 2003 he discovered a secret room at an AT&T building in California, where the company was providing the NSA with access to data it was transferring to other companies.

In February 2016, Apple declared in a press release that the FBI asked Apple to design a backdoor program to disable the encryption of a terrorist's iPhone. Apple publicly declined, not only because this tool could be used to undermine the privacy of law-abiding citizens worldwide permanently but fearing to open the floodgates for governments requesting access to a technology used by billions of people, a fear shared by security experts and cryptographers. A few weeks later, the FBI announced that they had hacked the phone themselves, essentially confirming that they had lied to the public about the need for a backdoor, which inputs how trustworthy spy agencies are in the dispute about privacy and security. It was particularly worrying that the NSA could turn on your iPhone microphone or activate your laptop camera without you noticing.

13.4.1.2 China's Surveillance State

The *Economist* has named China "the first digital totalitarian state in the world." Considering what China has become in terms of surveillance since 2014, this is a very accurate description. China is racing to become the first country to implement a pervasive system of algorithmic surveillance. China's communist party-state is developing a social credit system in which the citizens score to incentivize "good behavior." According to the Chinese government, the system will use big data to build a high-trust society where individuals and organizations follow the law. It will assign social credit scores to each entity based on behavior, translated into various rewards and punishments (Koty, 2019). With the help of big data both will happen in real time (Strittmatter, 2019). The social credit system was first proposed back in 2007.However, it was not until the summer of 2014 that it was put into place by the State Council of China to "increase vigilance towards honesty and credibility within the society." In Western mass surveillance, facial recognition is used to identify criminal suspects. In China, facial recognition is used on everyone, without exception. Furthermore, the country wants to dominate the artificial intelligence industry, maintain control over every aspect of society, and maintain constant surveillance. The new system is part of China's anti-corruption program and is called Sky Net. This program was launched in 2015 to locate and capture fugitives and corrupt politicians, but now it has evolved into something much more advanced. The system is connected to 20 million cameras, it identifies the person's gender, age, skin color, clothing characteristics, and even unique features. Besides, it can recognize vehicles by brand, model, color, and type of vehicle and know if they are being driven or parked.

The Xinjiang Chinese region is one of the most supervised places in the world. Security points with identification scanners are located in the stations, on the streets, in the area, and outside. Facial scanners record the faces of those who come and go from hotels, malls, and banks. Police are using mobile devices to scan people's smartphones in search of encrypted applications, politically charged videos, or other suspicious content. To use gas, drivers use an ID card and look at a camcorder. Xinjiang could be described as an echo of

the dystopia of the novel *1984* by George Orwell. Chinese Communist authorities use electronic mass surveillance devices to find, investigate, and incarnate Muslims living in the Xinjiang region. In the region live about 13 million Uighurs, who are Muslims.

Communist China is criticized by international organizations about human rights issues and its re-education centers, where over 1 million people are placed, who are practically imprisoned there. The Chinese state actively denies these accusations and the human rights abuses in Xinjiang, trying to justify mass surveillance as a measure against the three evils of "separatism, terrorism, and extremism."

13.4.1.3 Mass Surveillance in the European Union

Well established European democracies are also racing to install automated technologies such as border controls, predictive policing, safe cities, and facial recognition systems. Chinese investments are the leading suppliers of AI Surveillance in Europe. There is an increasing number of safe city surveillance case studies posted on Huawei's website from countries such as Germany, Italy, the Netherlands, and Spain; the reasons for this are the control of migration and terrorist threats. In October 2015, the Court of Justice of the European Union passed the Safe Harbour Agreement. The goal of this agreement was to allow data sharing to be transferred from EU citizens to the US, which seemed a shock because the European leaders and legislators condemned the ethicality of mass surveillance carried out by the NSA not so long before that. This came as a response to the terrorist attacks across Europe, especially because of the Paris attacks. Following the November 2015 Paris attacks, France expanded its already extensive anti-terrorism laws by giving law enforcement greater powers to conduct house raids and place people under house arrest. Within weeks, evidence emerged that these powers were being used for unintended purposes, such as quashing climate change protests. Illegal migration has played a role here; in the same year, 2.2 million people were found to be illegally present in the EU.

In 2016, the French port city of Marseille initiated a partnership with the Chinese telecommunications equipment company ZTE. The partnership sought to establish the Big Data of Public Tranquility project. This project aimed to reduce crime by establishing a vast public surveillance network featuring an intelligence operation center and nearly one thousand intelligent closed-circuit television (CCTV) cameras. The number was set to double by 2020 (Feldstein, 2019). Local authorities trumpet that this system will make Marseille "the first safe city"' of France and Europe. In Germany, there has been a spark in debates after the German Ministry of Interior prepared an act in which the powers of the Intelligence Agencies would be extended by allowing them to supervise the journalists' communications.

In late 2016, the most significant intelligence legislation in recent German history was amended. Negotiations were made in secret for a year, and a brief legislative process to codify new rules about the authorization, practice, and oversight of foreign data collection by the Bundesnachrichtendienst (BND), Germany's foreign intelligence agency. As opposed to other European countries, since this year German intelligence law contains particular restrictions on the collection of foreigners' data, foreigners will not be notified in regards to the surveillance measures; moreover, German legislation uses the term strategic surveillance as surveillance that involves the collection, without proper purpose, without a target, of a quantity of wholesale data. In 2018, the European Union began testing a new technology called *iBorderCtrl*. The technology was implemented in three countries, Greece, Hungary, and Latvia; the main purpose was to screen migrants at border crossings. Individuals were asked questions about their countries of origin and circumstances of departure. An AI-based lie-detecting system evaluated the answers. Although, in theory, this may sound like a good solution to protect the EU borders, this technology is flawed in practice. For example, lie detection is considered pseudoscientific because there is no sufficient conclusive evidence that the lie detector could be a reliable technology, and it is very likely that it will discriminate against various groups of people, like Muslims, immigrants, or people that could be perceived as a threat for that particular country.

13.4.2 Mass Surveillance Legal Framework

The tragic events of 11/9 made it clear across the developed world, especially in the US, that the modern globalized era of free movement of people, goods, and information hides new risks, that we have not seen before in human history. The fact that an Arab terrorist group succeeded in such a hit in the heart of Western civilization showed noticeably, on the one hand, that there is no absolute security for any state and, on the other, that the traditional security structures are no longer adequately effective. Therefore, particular emphasis was given to preventing such tragic events by monitoring the communication between people who can be considered potential public enemies.

As mentioned earlier, the Patriot Act of the US was adopted during the chaotic aftermath of 9/11, following the procedure of urgency by Congress without discourse, just three weeks after the tragedy. It was signed by President Bush on October 16, 2001, without a report from the House of Representatives, the Senate, or the meeting of the legislative committees. The law is a submissive variant of the anti-terrorism Law of 2001 and introduced dozens of constitutional changes to increase the operational power of information services and law enforcement agencies. It contains provisions that may extend the rights of the State to monitor and intercept private communications and even gives the FBI access to sales of bookstores and records of libraries, from which they can form their own opinion about the political beliefs of citizens through a program called Carnivore. Plus, the Patriot Act allows the US government to get information transferred via the Internet and to intervene in people's civil liberties through the use of advanced technologies. It also allows law enforcement agencies to use new communications technologies without resourcing to Congress. The assertion that the United States regarded the monitoring of global electronic communications as exclusively their duty would be an inaccurate representation (Gibb, 2006).

The US government has pushed all democratic regimes worldwide to strengthen their laws regarding the use of new and future technologies of telephone trapping. A little after the 11/9, the former director of the FBI, Louis Freeh, was exploited by the Bush administration to travel to the developing countries of Eastern Europe, Asia, and Africa to promote the idea of telephone trapping. The US also has argued that it would be desirable to ensure that all telephone trapping technologies are manufactured with integrated capacity of surveillance, or in other words, their purpose was to outlaw the construction of any communication equipment that cannot be spied (Gibb, 2006).

Today, in most countries, the list of surveillance operations and details about the time they take place are published. This happens to show that legal activities, such as journalism, environmental activism, human rights, trade unionism, religious activities, and political differences, are not subjected to arbitrary monitoring and that those groups of people are not listed as targets simply because they may have conflicting interests with the authorities.

In Europe, Member Countries have established an appropriate legal framework that allows the enforcement authorities to obtain judicial orders (or another authorization form) for monitoring sessions in the public telecommunications networks. However, the same is not true for Great Britain. A few years ago, it would have been unthinkable for the British government to admit that it was hacking into people's computers and collecting private data on a massive scale. Now, these controversial tactics are about to be explicitly sanctioned in an unprecedented new surveillance law (Gallagher, 2016).

In November 2016, the UK's Parliament approved the Investigatory Powers Bill, dubbed the "Snoopers' Charter" by critics. The law, expected to come into force before the end of the year, was introduced in November 2015 after the fallout from revelations by National Security Agency whistleblower Edward Snowden (presented in the following paragraphs) about extensive British mass surveillance. The Investigatory Powers Bill retroactively legalizes the electronic spying programs exposed in the Snowden documents and expands some of the government's surveillance powers.

Perhaps the most controversial aspect of the new law is that it will give the British government the authority to serve Internet Service Providers (ISPs) with a data retention notice, forcing them to record and store logs for up to 12 months showing websites visited by all of their customers. Law enforcement agencies can then obtain access to this data without any court order or warrant. In addition, the new powers will hand police and tax investigators the ability to hack into targeted phones and computers with the approval of a government minister. The law will also permit intelligence agencies to sift through bulk personal datasets that contain millions of records about people's phone calls, travel habits, internet activity, and financial transactions, and it will make it legal for British spies to carry out foreign-focused large-scale hacks of computers or phones in order to identify potential targets of interest. "Every citizen will have their internet activity logged for 12 months, including the apps they use and the communications," says Eric King, a privacy expert and former director of "Don't Spy On Us," a coalition of leading British human rights groups that campaigns against mass surveillance. King argues that the new law will cause a chilling effect, resulting in fewer people feeling comfortable communicating freely with one another. He cites a Pew survey published in March 2015 that found that 30 percent of American adults had altered their phone or internet habits due to concerns about government surveillance. To placate some of its critics, the government has agreed to strengthen oversight of the surveillance. The Investigatory Powers Bill introduces a judicial commissioner, likely a former senior judge, who can review spying warrants authorized by a government minister. It also bolsters provisions relating to how police and spy agencies can target journalists to identify their confidential sources. New safeguards will mean the authorities must seek approval from the judicial commissioner before obtaining a journalist's phone or email records; previously, they could obtain this data without any independent scrutiny. If the law undermines encryption, it may never come to light. The government included a section in the law that criminalizes unauthorized disclosures of any information related to its surveillance orders, which could potentially deter any whistleblowers or leakers from coming forward. The punishment for breaches is a prison sentence of up to 12 months, a fine, or both. Though the Investigatory Powers Bill will soon come into force, it will likely face several lawsuits. At least three ongoing cases could result in changes to some of its provisions. One of these cases is a major challenge in the European Court of Human Rights, which could potentially rule the government's mass collection and retention of data to be illegal (Judgments from the European Court of Human Rights remain binding in the UK, despite its vote to leave the European Union).

Here are some of the most well-known surveillance agencies worldwide:

- Russia's Federal Security Service (FSB),
- The UK's Government Communications Headquarters (GCHQ),
- Canada's Communications Security Establishment Canada (CSEC),
- The Australian Signals Directorate (ASD),
- New Zealand's Government Communications Security Bureau (GCSB).

In Greece, the lifting of secrecy for public authorities is permissible only under conditions and procedures laid down by Article 19 of the Constitution and the laws implementing it (essential guarantee, judicial authority, control of the ΑΔΑΕ). In particular, interference by a public authority is allowed only by the domestic law, is generally accessible, and governed under precise conditions and circumstances, provided it is necessary in the context of actions developed in a free and democratic society, in the interests of national or public safety, for the prevention of disorder, to prevent criminal acts, or for the protection of rights and freedoms of third parties (Χοχλιούρος, 2006). Generally, Article 17 of the UN Commission of Human Rights requires that "the integrity and confidentiality of correspondence should be guaranteed *de jure and de facto*. The monitoring, whether electronic or carried by other means, the interception of telephones, telegrams and other communications, the direct phone capture and recording of the dialogue should be banned" (HRC, n.d.). This

contradicts the patriotic US law and also a variety of other Acts in the rest of the world. Therefore, most of the interceptions carried out by the security services are illegal, and people being monitored do not wish to be forced to justify their behavior by cross questioning in Court. In the US, however, there is no such reservedness simply because the Patriot Act facilitates, to the maximum level, the justification of secret surveillance, even for innocent people (Gibb, 2006).

13.4.3 Modern Surveillance Systems

13.4.3.1 Biometry

Biometric is defined as a technique to identify a person based on specific biological, genetic or behavioral characteristics, considered personal and unchanged. These can be the shape of hands, iris, face shape, fingerprints, and genetic fingerprints. The transformation of these characteristics into digital fingerprints renders biometrics the most advanced method for identifying an individual, constituting a means of identity for the person. This means that whereas previously the core elements identifying the person were mainly anthropometric ones (height, color of eyes, fingerprints, shape of face), biometrics nowadays succeeded in gathering in a digital fingerprint a wide set of data and information that identifies more accurately the uniqueness of any person's identification.

The citizen's relationship with the state entity dictates the identification process. Therefore, the knowledge of the State for the identity of the citizen is a condition of its functioning on both its internal and external space of the borders. Passports, identity cards and Visa for foreigners constitute, thus, fundamental elements of the state power by controlling the activities and movements of persons and shaping international affairs. Nevertheless, with the removal of borders between EU countries, the mass mobility of the population, and the use of new technologies, the traditional method for individual identification could not serve the needs and the feasibility of controlling and monitoring. In addition, the evolution of crime technology and the appearance of transnational crime forms made territorial surveillance ineffective and traditional identification outdated. Thus, the solution was sought in biometric technology, which is considered technologically advanced and credible for authentically identifying people, dragging up the adoption of new smart technologies to address risks.

Biometric surveillance relied on a political and legal justifying background, which included modernizing government services, combating bureaucracy, counter terrorism and organized crime, controlling migration flows and protecting citizen’s security. The last argument was what ensured the tolerance of public opinion towards the generalization of biometric surveillance, if not the acceptance of it (Παπαθεοδώρου, 2009). With biometric surveillance, the national borders no longer constitute limits for collecting and processing data; on the contrary, they are reset depending on the surveillance needs.

This new context has brought significant changes in the context of criminal policy. It also established the preventive intervention to reduce the risk, implemented the operational and functional interconnection of biometric databases, introduced new classifications for suspicious and undesirable people or groups, and introduced geolocation techniques using GPS for those deemed to pose a risk to public safety.

The purpose of biometric surveillance is to make the global village a large control zone, in the perimeter of which suspicious or risky individuals and groups are tracked down (Παπαθεοδώρου, 2009). This zone comprises all information parameters and electronic data and remains under the guidance or exploitation of countries with advanced knowledge and cutting-edge technology. In the control zone, the only object of management is the information related to the life of people in any form, such as their movements, their physiognomy characteristics, their genetic fingerprint, their beliefs, habits, or behaviors, so that the data collected can be exploited through information technology networking.

The modern use of biometrics includes, on the one hand, its wide-scale implementation in passports, identity cards, and other travel documents to facilitate the pumping of the largest volume of information and, on the other, the establishment of central databases that will process the collected data. In this way, continued safety is shielded to exist independently, beyond, and above the political options of countries or organizations.

The starting point for the generalization of biometric surveillance worldwide was the events of 9/11. Since 2002, the US imposed the generalization of biometrics for other countries while they were already applying biometric surveillance of foreign citizens wishing to enter the US before implementing it for US citizens. Europe sided with this decision, and indicatively, in 2005, the European Council decided to launch the use of retention, storage, and processing of telecommunications data of 400 million European citizens because the creation of wide databases may contribute to the prevention and detection of criminal acts.

In recent years, any foreigner entering the US has been ranked systematically by the security forces in one of the three following categories: trustworthy, questionable, or risky. The entrance in one of these three categories signifies the way of reception and treatment by the authorities without the alleged degree of risk having any specific forensic or criminal basis. The risk, just like the security, is now identified through impersonal categorization, such as political or religious beliefs, national origin, and social activities, which exceed the limits of crime prevention and impose the treatment of individuals as unwanted. The unwanted carrier of a vague risk is monitored closely, has limited access to certain services and goods and is isolated and rejected preventively.

Based on a respective classification, the EU creates databases of undesirable foreigners or unwanted demonstrators, expanding control and surveillance in a growing population group. In this context, the surveillance power of security authorities is strengthened while the safety of civil rights is steadily declining. The principles of proportionality, prevention, and social protection take a symbolic nature, whereas the electronic safety activities come to overlap with evolutionary natural dynamic, the whole human, and social activities (Παπαθεοδώρου, 2009).

The Information Commissioner's Office in Great Britain, the UK's independent authority set up to uphold information rights in the public interest, finds that out of the DNA databases in Britain, 40% were colored citizens, 13% were Asians, and only 9% were white. Racial hyper-criminalization provides conditions of increased social discrimination and xenophobic attitudes while at the same time criminalizing or victimizing large groups of the population. The annexation of European security policies with the respective globalized US practices produces the denationalization, privatization, and, to some extent, the depoliticization of the criminal policy. Electronic monitoring as a means of prevention in public and private places, using biometrics to strengthen security or the electronic surveillance of offenders as suppression from the tissue of the enlarged social control with intense shades of criminality nowadays. The problem is not the evolution of technology but the use of it in a world that is changing rapidly with worldwide interaction, which, through specific policies, chose to address the major social deficit and the new risks by resorting to the hypertrophic shield of the penal State. It is, in fact, the abolition of the traditional Social Contract and the subordination of democracy to "surveillance" (Παπαθεοδώρου, 2009).

13.4.3.2 Artificial Intelligence Surveillance Systems

The daily surveillance of ordinary people through closed-circuit television becomes even more alarming when combined with other recent developments. In Britain, the Home Office has had routine interceptions for at least ten years without needing to apply for a warrant from some judge. Moreover, in recent years, they have experimented with software designed to recognize faces in the crowd through a photographic data bank set-up by records of arrests and passport service, as well as from other government departments that require

photographic ID identification. The precision of facial recognition, however, is controversial, unlike the DNA examination and the recording of the iris.

Because the recording material of the camera is huge and needs many person-hours for the analysis and processing, the new system of electronic cameras, known as neural, allows the camera to distinguish normal from suspicious behavior and send it to the operator. The software isolates the relevant field of the tape and gives it priority so that the monitor will see what happens at the moment, detect the people involved, and call security personnel for help. Both public and private entities use this software, and although costly, it is a fast system, efficient, and precise enough to be considered the future of surveillance. At the same time, there is the *Spectiva* system. It automatically records sounds and films with the ability to transmit, and it can identify and isolate dialogues from a wide area. The system's camera is programmed to act on a vast range of probabilities suggested by the security company that has installed it.

Generally, modern surveillance systems based on artificial intelligence are considered the future of surveillance, and with the rapid development of artificial intelligence, they are continuously improving and individualizing.

13.4.3.3 Mass Surveillance Systems

In the US, tapping and interpretating signals from the Department of Justice, the FBI, and the DEA penetrate all communication systems by including broadband Internet access and Voice Over Internet Protocol (IP). While members of society are discussing on the phone, surfing the web, or engaging in everyday transactions online, without knowing it, they leave traces of personal information conceived automatically and kept in computer software.

Menwith Hill station in Great Britain has been revealed to be under the protection of the NSA and accountable only to the US President and his advisors on national security. It is supposed to be the connecting link between the American army and the sections for collecting information in space, and they can listen to any signal and conversation taking place in Europe, South Africa, and Western Asia. The American side does not officially admit the existence of such a base and refuses entrance to visitors, even Members of the European Parliament (MEP). The satellites that providing information for those regions are visible from Menwith Hill rather than the US. The intercepted signals are believed to include all telephone calls, messages from mobile and satellite phones, emails, faxes, radio signals, and all forms of telecommunication. According to the reports, if a signal passes through an antenna, or radio links, or microwaves satellites, the station can collect, analyze, elaborate, and retransmit it automatically in the US. It has also been revealed that just in 1992, *Menwith Hill* station was intercepting 2,000,000 messages per hour, most of which, apart from about 13,000, were rejected before being filtered to reach the 2,000 that met the criteria for forwarding. The most powerful means by which the USA spies on its enemies, and citizens, are the KH satellites. The exact number of these satellites is unknown; however, it is generally accepted that there were around 200 until 2005 in stable orbit and there are dense clusters of them located above "troublesome" locations such as the Middle East and North Korea.

KH satellites are the key to the operation of ECHELON, the most extensive system for collecting information of all time, which, by sweeping telecommunications worldwide, could detect and identify suspects for criminal and terrorist acts using the NSA's communications networks and GCHQ's (Government Communications Head Quarters), allowing remote intelligence partners to contact computers in each collection site and receive results automatically. They are digital cameras in orbit equipped with very powerful lenses capable of analyzing objects 12cm in size on the ground. The data collected by the satellites KH is theoretically used for collecting military information and scientific research. The NSA and the CIA are assumed to be the data recipients, but it is still known from data provided in US courts that law enforcement agencies

have used this equipment to spy on US citizens who were considered potential terrorists, criminals, and troublemakers.

Eventually, thanks to the widespread availability of high-definition satellite images from numerous non-military sources, even the less prosperous countries can gain automatic access to satellite surveillance as long as they pay for it.

13.4.4 Edward Snowden Leaks

In June 2013, the world came to the harsh realization of global mass surveillance programs after the biggest leak in the NSA's history. The man responsible for the most significant leaks in US political history was Edward Snowden, a former technical assistant for the Central Intelligence Agency (CIA) and former defense contractor for *Booz Allen Hamilton*. At that time, he was working for *Booz Allen Hamilton* as an infrastructure analyst for the National Security Agency office in Hawaii, where he copied the last set of documents he wanted to reveal. In May 2013, Snowden flew straight to Hong Kong to launch the initiation of the disclosure procedure. He said that he chose the particular city because "they have a spirited commitment to free speech and the right to political dissent", and because Hong Kong was one of the few places in the world that could and would resist the US government's orders.

13.4.4.1 The Incident

In June 2013, a former National Security Agency (NSA) contractor, Edward Snowden, became known for leaking a massive trove of classified documents (Kharpal, 2017). More specifically, he perpetrated the most damaging public leakage of classified information in US intelligence history.

Based in Hawaii, Snowden collected top-secret documents regarding NSA domestic surveillance practices that he found disturbing and leaked them. Then, he fled to Hong Kong, where he secretly met journalists from *The Guardian* and a filmmaker, Laura Poitras. The Newspapers began releasing those documents (leaked information on the PRISM-NSA program in cooperation with several European countries that allow real-time information collection electronically), which had details about the monitoring of American citizens. A flood of information followed. Both domestic and international debate ensued.

In 2013, *The Guardian* reported that the NSA was collecting the telephone records of millions of Americans (BBC.com, 2014). The Press published the secret court order directing company Verizon to hand over all its telephone data to the NSA on a daily basis. The document shows that, the communication records of US citizens have been collected under Obama's administration, regardless of whether they are suspected of any wrongdoing (Greenwald, 2013a). That report was followed by revelations that the NSA tapped directly into the servers of nine internet platforms (Facebook, Google, Microsoft, Yahoo) to track online communication in a surveillance program (Prism). This program has extracted and stored data from SMS messages to gather location information, contacts, and financial data. The documents also revealed that Government Communications Headquarters (GCHQ) had used the NSA database to search for information on UK people. Another program (Dishfire)also analyses SMS messages to extract information such as contacts from missed call alerts, location from roaming and travel alerts, financial information from bank alerts, and payments and names from electronic business cards (BBC.com, 2014). The information is classed as "metadata," or transactional information and does not require individual warrants to access. The collection would allow the NSA to comprehensively understand who an individual contacted, how and when, and possibly where. NSA's mission has transformed from an agency exclusively devoted to foreign intelligence gathering to focusing increasingly on domestic communications (Greenwald, 2013b). *The Guardian* newspaper and Channel 4 News reported that the US had collected and stored almost 200 million text messages per day across the globe (BBC.com, 2014).

Technically, the NSA could not do this alone. There has been a whole mechanism relying on a network of international partners helping each other collect information worldwide, especially the intelligence agencies of Australia, Canada, New Zealand, and the United Kingdom. Along with the United States, they are known as the "Five Eyes." Moreover, the United States has relationships supporting data sharing with Belgium, Denmark, France, Germany, Israel, Italy, Japan, The Netherlands, Norway, Singapore, Spain, South Korea, and Sweden (Reitman, 2015).

Edward Snowden told the *South China Morning Post* that the NSA had led more than 61,000 hacking operations worldwide. He also mentioned that targets included the Chinese University, public officials, and businesses. Snowden confessed: "We hack network backbones that give us access to the communications of thousands of computers without having to hack every single one" (BBC.com, 2014).

After the big disclosures, the UK was quite supportive. Prime Minister called on newspapers to stop publishing the leaked NSA files to avoid government action. The British foreign minister stated that the GCHQ gathered intelligence from phones and online sites but that it must not concern individuals (Solms & Heerden, 2015).

Following the disclosures, the US charged Snowden with violations of the Espionage Act. Snowden found asylum in Russia, where he continues to live until now.

13.4.4.2 Impact and Effects on Global Surveillance

Some people called Snowden a hero; other people called him a traitor. It is all in the eye of the beholder. The truth is that the aftermath of the Snowden case was huge and really important for the global community. The phenomenon referred to as "the Snowden effect" has gained widespread recognition and exerted significant influence on society. Currently, Snowden states that he cannot return to the US as the American government's Whistleblower Protection Act is not valid for him, as his work as a government contractor. His lawyer is trying to secure Snowden's return to the US. Despite all of Cacheris' efforts, Snowden's return is unlikely to happen as the US Prosecutors have recognized that he will be accepted back in the US only if he returns the classified documents he has in his possession (Kelley, 2019).

Due to the surveillance disclosures, the US President, Barack Obama, in 2013, announced that the intelligence surveillance programs must be reformed to balance between ensuring US citizens' security and maintaining their privacy (Madhani & Jackson, 2013). In January 2014, Barack Obama proposed a plan to the NSA that could reform how phone calls are recorded and stored in the NSA database (Ackerman & Roberts, 2019). There was public outrage as it was thought that the only reason this reform happened was the disclosures made by Edward Snowden, and otherwise, nothing would have changed in the surveillance programs. Also, it has been stated that whistleblowers should not be mistreated, and their safety should be ensured (Allam, 2014).

In Europe, government leaders from all European Union member states have reacted to Edward Snowden's surveillance disclosures. David Cameron, the Prime Minister of the UK, expressed his total dissatisfaction with the articles published mainly by *The Guardian* and urged them to publish nothing more about this matter to avoid internal political turmoil (Watt, 2019). As for the German federal government, it stated that the number of German citizens who had been targeted was unknown and demanded explanations from the US government.

As previously mentioned, Edward Snowden was perceived as a hero by many people, not only in the US but also in other countries. This impacted the formation of political movements concerning privacy and human rights. In particular, the "*Restore the Fourth*" movement had been formed in the US. *Restore the Fourth* was a political movement that took place in over 80 US cities and it was coordinated via the Internet (Kelly, 2013).

In addition, another movement formed in the USA was called "*Stop Watching Us*" and its aim was to oppose the actions of the NSA.

Global surveillance has changed on a large scale thanks to the disclosures made by Edward Snowden. Internet companies are considered to value transparency to a greater extent now, and, as a result, their customers are more satisfied. By the time *The Guardian* and *The Washington Post* published articles about the *PRISM* surveillance program, tech companies such as Apple and Facebook made an enormous effort to save their reputation by changing their legal policies (Timberg, 2014). These companies now notify their users when a surveillance request will be made. Telecommunication companies have also made some changes to their operation. *AT&T* and *Verizon* were threatened with lawsuits because of privacy violations and data given to the NSA. As a result, they decided to disclose transparency reports to keep their reputation clear and attract more customers (Berkman, 2014).

It is widely admitted, though, that Snowden's biggest impact was on the internet communications of everyday users. Microsoft, Yahoo, and Google made an effort to secure their users' internet rights by providing encryption to their services. Moreover, the Cyber Intelligence Sharing and Protection Act, a bill about information and communication that would concentrate on cybersecurity, was shelved until further notice because of the Snowden disclosures (Sanger, 2013). This is one of the most important effects that Snowden had on Congress as this bill, which was rated negatively by most civil liberties advocates, would have let the NSA collect even more personal data of American citizens as well as it would have decreased transparency of tech companies (Reitman, 2013).

Along with Edward Snowden, the public's voice greatly impacted global surveillance as it pushed internet companies and political actors to have greater respect for users' rights. By the time Snowden made these revelations, American citizens had started to inform themselves about their civil rights and placed these matters of privacy high (Greenwald, 2013b). Snowden had an important impact on the global community and is nearly close to achieving his goal as he says: "I did not want to change society. I wanted to give society a chance to determine if it should change itself."

13.4.4.3 Implications of US Relations with Russia and Other Countries

As expected, the incident above played a significant role in the country's foreign relations, especially with Russia, concerning Edward Snowden's living in Moscow as a Kremlin guest. There are two aspects of US-Russian relations beyond the Snowden affair. First, there are limits to the United States' ability to persuade Russia to cooperate. Second, Russia's stance is not the only barrier. Hong Kong also refused to extradite Snowden. There has been far greater tolerance internationally, even among the US public mind, toward him. Amnesty International even called governments around the world to reject the extradition requests (American Progress.org, 2013).

The Russian President, Vladimir Putin, affirmed that Snowden was in Moscow but has not committed any crimes in Russia and will not be contained by Russian authorities, despite warnings from the US Government (Solms & Heerden, 2015). He believes Snowden was wrong to leak US spy secrets, but that does not make him a traitor. The President states: "He did not betray the interests of his country, nor did he transfer any information to any other country that would damage his people."

Putin also agreed that US surveillance had become too intrusive and criticized US eavesdropping on its own allies (Osborn & Powell, 2017). We can also consider the incident an opportunity for Russia to use Snowden to point the West as hypocritical successfully. However, in 2017, NBC News reported that the Russian government was considering handing him over to the US to curry favor with President Donald Trump.

From what was stated above, the Snowden effect was tremendous for US Diplomacy, making it more complicated. The country's international relations were influenced negatively, forcing the President to put out diplomatic fires.

Many countries around the world supported Snowden's beliefs. As we know, the Russian government denied requests to extradite Snowden. In addition, Snowden was offered asylum in Venezuela, Nicaragua, and Bolivia. Snowden thanked Russia for giving him asylum and said that "in the end the law wins."

One of the big surprises was *The Guardian's* reports. The NSA monitored the phones of 35 world leaders after being given their numbers by another US government official, and a total of 38 embassies and missions have been targets of spying operations. Countries targeted included France, Italy, Greece, and America's non-European allies such as Japan, South Korea, and India. The Guardian also reported codenames of alleged operations against the French and Greek missions to the UN and Italy's s embassy in Washington (BBC.com, 2014).

At the same time, there have been angry reactions to the NSA for spying on the European Union offices (American Progress.org, 2013). Political leaders reacted to Snowden's disclosures. The French President, Hollande, complained about the surveillance operation against France. The German Chancellor, A. Merkel, also called the President to complain that her private mobile was tapped. Then she stated that: "Spying among friends is not on" and that "trust will now have to be rebuilt" (Bryant, 2013). The relations between the US and Germany reached a significant low.

In a draft report released by the European Parliament, the committee presented the findings from a six-month investigation. This report called on the authorities to halt mass surveillance programs as they feel they can affect freedom of the press, freedom of thought, freedom of speech and the potential to abuse of information gathered against political adversaries.

Furthermore, Snowden received a nomination for the Nobel Peace Prize for "contributing to transparency and global stability by exposing a US surveillance program" (Solmes & Heerden, 2015), and the European Parliament passed a resolution deciding to call on EU member states to "drop any criminal charges against Edward Snowden, grant him protection and consequently prevent extradition or rendition by third parties, in recognition of his status as whistle-blower and international human rights defender." It also proposed to "call on national leaders to publicly commit to respecting the will of the European people and offering Snowden asylum" (Juerveton, 2014).

Mexico was also annoyed that their President had been snooped upon. And so did the Brazilian President, who discovered that her private communications had been tapped and she canceled her state visit (Bryant, 2013). The Brazilian President threatened to downgrade commercial ties with the US. In addition to canceling the state visit, the government canceled a $2.5 billion deal for Boeing's F/A-18 fighter jets, accepting a contract for Swedish Saab's JAS 39 Gripens instead (Solmes & Heerden, 2015).

Finally, a plane carrying the Bolivian President was forced to land in Austria after suspicion that Snowden might be on board. The Bolivian defense minister claimed that the US was behind the cancellation of flight plans, which can be seen as intimidation. This incident caused outrage among the South American nations calling it a "grave offense to their region," causing an emergency meeting of the Union of South American Nations. The President of Argentina stated that this episode was a reminder of colonialism that was thought to be a thing of the past. Ecuadorian President renounced US trade benefits after US Senator Menendez urged Correa to deny Snowden asylum (Solmes & Heerden, 2015).

In addition to foreign ministers and presidents, many US based technology companies reacted strongly. Persons, companies, and nations were affected by the leaks. Some secure email providers had to close down due to NSA and other government pressures to reveal their secret keys. The US lost $25-$35 billion in cloud computing-based revenue. The trust in the US was degraded, impacting the US's status. Lavabit (secure email

service) was shut down by the owner, who stated that he would rather shut down his company than "become complicit in crimes against the American people." Technology companies outside the US say they are gaining customers from US based Technology companies as they do not want to entrust their confidential information to the large US internet companies for fear of the NSA's surveillance programs. Microsoft lost the business of the government in Brazil and IBM is spending millions of dollars to set up data centers outside the US to ensure their customers that their information is safe (Solmes & Heerden, 2015).

13.4.4.4 Legal Gray Zones and the Public Opinion

From the Snowden incident described in the previous paragraphs, it is evident that where states used to rely on traditional police work and methods, their capabilities are developing along the technical innovations that the 21st century has introduced. This, in combination with the rise of the perceived threat of foreign and homegrown nontraditional enemies such as right-wing extremists and Islamic terrorism, is one example of what motivates states to adopt increasingly intrusive laws, all in the name of safety for the general population and national security (Fuchs et al., 2012). This is, however, a simplified view of the question at hand. It is not a matter of being against or for what the state says the surveillance is meant to achieve. Western liberal states and their judicial system are based on proportionality; in short, whatever legal measure is taken, must be proportional to the suspected crime or its intended effect while being weighed against other interests, such as integrity questions (Naarttijärvi, 2013).

This raises some important questions that are difficult to answer: Can the state refer to an increasing risk of terrorist attacks to motivate further digital surveillance legislation? Most likely, this information will be classified, making it impossible for the public and media to check the validity of these claims (Naarttijärvi, 2013). While the state use of digital surveillance against its citizens can be and is motivated by the nation's security (Stalder, 2006), it comes at the cost of the individual's private integrity, which is protected by the UN's human rights declaration (Naarttijärvi, 2013).

While the UN's formulation does not cover much as to get more countries to ratify it, the European Convention goes further. While it has proved to be difficult to define what is meant by "private integrity" and "privacy" (Naarttijärvi, 2013), it is, among other things, generally considered to protect from infringement on the individuals physical and psychological integrity. In a series of cases, the European Court of Human Rights found that relatively non-intrusive measures, such as collecting data about dialed phone numbers, can infringe on individuals' privacy rights (Naarttijärvi, 2013). Therefore, a legal framework supports the decision to use a measure like this and is not to be used arbitrarily.

While the purpose of using surveillance on an individual can have clear benefits, it also means that it is not compliant with the values that private integrity is meant to protect (Tréguer, 2016). The right to privacy protection can be seen as a basis for democracy. If the state persecutes a person because of, i.e., political opinions, it can be considered a form of censorship. This raises the question of how to deal with organizations that are anti-democratic and violent, which in turn might motivate a higher degree of personal integrity infringement. It is, therefore, clear that too far-reaching surveillance of the public is threatening liberal democracy and human rights.

In a European context, it is important to remember modern history when studying European reactions to state surveillance. The Second World War had long-lasting effects on European democracy and meant authoritarian rule for large parts of Europe for different periods. France's Vichy government (Tréguer,2016) collaborated with Nazi Germany and adopted an authoritarian form of ruling with the persecution of political opponents and Jews, among other groups. For Germany, the effects were even more profound (Schultze, 2015), with the Gestapo being active for more than a decade, and after the war, the Stasi spread fear among the population of DDR. With this in mind, it is not difficult to understand why Germany's chancellor Angela

Merkel, who grew up in East Germany, and why the German government reacted strongly to the news of alleged American spying on both her and the population of Germany, sparking a diplomatic crisis between the two countries (Schultze, 2015).

Because of this, it is not difficult to understand why the NSA's spying was so controversial among the general populations of countries all over the world, particularly within Europe. Polls in Sweden indicated that 55% of the population says that it is not acceptable that FRA (Försvarets radioanstalt, National Defence Radio Establishment) collects data on the citizens, with 80% saying that it is unacceptable that foreign intelligence agencies collect data on Swedes (Larsson & Runesson, 2014). Polls in the UK suggested that governmental surveillance is important to more than 80% of the population and that around half of the population thought that Snowden did the right thing, with 32% thinking that what he did was wrong (Bakir et al., 2015). Also, 64% of the British thought the UK government did not protect the citizens' personal information (Fuchs & Trottier, 2017).

While public opinion has proved to be strong and widespread, as the UK polls mentioned earlier show, it has not been translated into action, and it is considered by many that no real or lasting change has been achieved (Tréguer, 2016). As a global matter, everyone must find common ground that makes people involved look past their eventual differences and mobilize around them (Haunss, 2015).

13.4.5 Assessment

Security is the primary and ultimate aim of any rational state. Collecting information helps achieve that goal. When the appropriate agencies can gather data such as phone call logs, credit card use or face recognition through public street cameras, they can identify targets easily, track their moves, and finally apprehend them. After, for example, a murderer has fled the scene, the police can scan through public CCTV cameras and find the suspect, or where he is headed, and thus, they can react fast enough before the suspect can completely get off the grid. There have been many ISIS-affiliated cases, where terrorists moved from one country to another to get to their final destination and execute the terrorist strike. Secret services and the police in those countries could communicate with each other and provide the correct information that has been assembled, which may be the route that the terrorists have taken or where they arrived from, and, of course, photographs showing the faces of the suspects.

Edward Snowden highlighted in an interview that modern surveillance technologies are now being used on the homefront and not only on the war front, as was the case in the past. In the same interview, it is said that surveillance is not being used exceptionally anymore, but we have moved to "the surveillance of everyone." In the wake of the Boston Marathon bombing on April 15, 2013, the FBI released two blurry photographs of the two suspects after three days of sifting through a large pile of camera footage. These two photographs were shot by a store's cameras. CNN mentions in the same article that, after a bombing in London in 2005, it took weeks for the investigators to analyze the city's CCTV camera footage. So, having compared the incidents, it is made clear that domestic surveillance for security (or other) reasons has improved vastly over the past years.

Despite its improvement over the years, the question that inevitably comes to the forefront is whether government surveillance has prevented large-scale attacks. In a White House review panel on NSA surveillance in December 2013, it was stated that mass collection of telephone information has not been "essential in preventing attacks." Two weeks after the Edward Snowden leaks in 2013, US President Barack Obama said that the NSA "averted at least 50 threats" due to surveillance, not only in the United States but abroad as well. Members of Congress added more cases to the 50 threats mentioned by President Obama, making them 54. According to US Senator Patrick Leahy, though, only 13 of the 54 cases had some connection to the United States, and they were not all part of a terrorist plot. The majority of those involved "providing material support,

like money, to foreign terror organizations." The National Security Agency director Keith Alexander testified in 2013 that more than 50 terrorist plots had been thwarted since the 9/11 attacks. In another testimony by the same Committee, officials spoke about a prevented terrorist plot to blow up the New York Stock Exchange (NYSE), which would have huge repercussions not only in the United States but also on a worldwide scale, given the fact that Stock Exchanges are globally interconnected and constitute a huge part of our economic system. Regarding the 9/11 attacks, General Alexander has said that if the surveillance programs were up and running prior to the tragic event, US officials would have known that the terrorists were in San Diego and communicating with an already known al Qaeda safehouse in Yemen and thus, they would potentially be ready to prevent the attacks.

In a final assessment, it is difficult to judge if government surveillance programs have been effective enough in putting a wall between domestic or global terrorism and citizen or state safety. As mentioned above, there are cases where bulk information collection has prevented terrorist plans. Regarding that, Edward Snowden stated that surveillance programs are being used to spy on citizens, not ensure safety. It all comes down to the question: In a liberal world, what is more important, the human right of free speech or the thwarting of terrorism in a way that both violates this right? Had it produced any large-scale result, the rhetoric might have been different. Nevertheless, digital mass surveillance has not stopped the attacks in Paris in November 2015, the vehicular assault in Nice in2016, or the December 2016 Berlin attacks.

Despite the controversy of whether government surveillance has paid off in preventing terrorist attacks or not, it is commonly accepted that eavesdropping on citizens constitutes an act of violation of human rights and constitutions. Especially in the Western world, it should always be kept in mind that democracy is a hard fought and earned privilege, and its violation poses a contradiction between the very nature of Western countries and this type of governmental strategy.

13.5 Online Censorship

Censorship derives from the Latin word "censura," which is the suppression of the publication of ideas, texts, photographs, movies, or other information. The origin of the term censorship goes back to the office of censor, established in Rome in 443 BC. The censor was an elected magistrate whose authority was supreme.

Three types of censorship have been exercised in history:

- Censorship by religious authorities: In the artistic field, many paintings were censored by adding vine leaves or clothes to the original works to veil the nudes on display, such as Adam and Eve being expelled from the paradise of Massaccio.
- Censorship by civil authorities during the Enlightenment under Louis XV, where the Bookshop controlled all texts in the process of being printed.
- Postal censorship during the First World War, when some letters from the combatants to their relatives were intercepted by the authorities not to reveal the terrors of war.

Today, general censorship occurs in various media, including speech, books, music, films, and other arts, the press, radio, and television. Governments, private institutions, and other controlling bodies can conduct it. Specifically, online censorship restricts what information can be put on the internet or not. It is deployed in a variety of forms across the globe. For example, social media have been constantly "under fire" by many authoritarian (or not) regimes around the world (**Figure 5.1**).

A prevalent example of online censorship is the case of North Korea, which is among some of the most extreme in the world, with the government able to take strict control over communications. All media outlets are owned and controlled by the North Korean government. As such, all media in North Korea get their news from the Korean Central News Agency. The media dedicate a large portion of their resources toward political

propaganda. North Korea is ranked at the bottom of *Reporters Without Borders'* annual Press Freedom Index, occupying the last place in 2017. Internet access is not generally available in North Korea. Only some high-level officials are allowed to access the global internet. In most universities, a small number of strictly monitored computers are provided. Other citizens may only access the country's national intranet, called Kwangmyong (Talmadge, 2014). The North Korean *Ullim*, an Android-based tablet computer available since 2014, has a high level of inbuilt surveillance and controls. The tablet takes screenshots of apps the user opens and saves browsing history (Williams, 2017). However, the People's Republic of China (PRC) is the most famous case of surveillance and censorship globally and will therefore be thoroughly presented in the following paragraphs.

13.5.1 General Context

Throughout history, censorship was imposed on the press, books, and art in many European countries. Over the years, it has been abolished in Great Britain (1694), Sweden (1766), Denmark (1770), and France (1789). However, occasionally it has been applied again, depending on policy or regime changes. In the fields of radio and television, censorship is often dictated by the perceptions of each government.

In the international and European spheres, freedom of expression is guaranteed by the European Convention on Human Rights (ECHR), where Article 10 secures it throughout the range of communication, from press to commercial media regardless of the type. The right to express an opinion is related to the right to information, that is, the right to simply transmit events without interceptions or comments. The exercise of freedom may be subject to certain conditions, limitations, or sanctions, which are prescribed by law and are necessary measures in a democratic society, including:

- national security,
- territorial integrity,
- public safety,
- the defense of order and the prevention of crime,
- the protection of disclosure of confidential information,
- ensuring the authority and impartiality of the judiciary.

Still, the International Covenant on Civil and Political Rights, ratified by Law 2462/1997, Article 19, guarantees freedom of expression. The primary forms of spiritual freedom are general freedom of belief, conscience, and expression. Therefore, guaranteeing freedom of opinion means securing the democratic system and vice versa.

Censorship of the Internet is the control or restriction of access and content that can be published or displayed online, as regulators or private initiatives have enforced it. Individuals and organizations may exercise a policy of censorship on moral, religious, or professional grounds, comply with social standards, intimidate, or fear legal or other consequences.

The extent of censorship on the Internet varies from country to country. While most democratic countries have moderate censorship on the Internet, other countries have come to restrict access to information, such as news, to prohibit online deliberation between citizens. Censorship of the internet can be applied around events such as elections, protests, or riots for several reasons. Government agencies have various tools to implement restrictions, but internet freedom advocates often try to overcome these obstacles and filters.

The modern debate in the public sphere revolves around the duality of values, on the one hand, freedom of speech and expression, and on the other, around the restriction to the protection of individual or collective rights and identities, another form of which is the controversy surrounding the so-called "political

correctness." In this type of approach, however, the political or ideological assignment is not clear, which in absolute terms is only one of the two opposing positions: left/progressive and right/conservative, often in cooperation and unanimity, thus confusing their ideological positioning. Each side in this argument can blame the other for enforcing censorship.

The post-modern treaty in the 21st century, the increasing flows of information, and technologically mediated online communication contribute to sharpening the struggles around the power of speech and censorship. They may, however, be blunted through many obscure faces and suggestive forms of censorship or euphemisms and under the accent of the extreme freedom of speech and the multitude of possibilities for communication.

In the paragraphs below, some descriptive cases of limiting or controlling Internet access and content for political reasons will be presented, along with the techniques allowing such interventions.

13.5.2 Online Censorship Techniques

Online surveillance and censorship are closely intertwined, as surveillance can occur without censorship, but censorship cannot occur without surveillance. Online censorship can take multiple forms, from filtering and blocking content to monitoring and penalizing users who access certain content. For governments to apply censorship, they have two options: to block and implement the technological process of blocking or to create legislation or policy to compel “autonomous” technological firms to do the blocking and surveillance. Technically speaking, Internet censorship can be applied with a variety of tools and strategies that prevent information from reaching users. Therefore, “internet censorship” is not a piece of software or one point of blockage but can occur at one point on the net, function as a blanket filter for all connections in a country or be micro-focused on individual sites, machines, and even keywords. Below, some standard internet censorship technologies are presented.

DNS Tampering

In authoritarian regimes that have control over domain name servers, officials can “deregister” a domain hosting nefarious content. This makes the website invisible to the browsers of users who wish to access this site because translating domain names into a site IP address is prevented.

IP Blocking

Governments with control over internet service providers (ISP) can blacklist certain IP addresses of websites that they want to ban from visiting. Requests to these websites are monitored by surveillance computers that have a blacklist of IP addresses. On requesting a visit to one of these forbidden sites, the ISP drops the connection, causing it to fail. If the target website is hosted on a shared hosting server, all sites on the same server are blocked, even if they are not targeted for filtering.

Keyword Filtering

IP address filtering is the technique that only blocks websites explicitly blacklisted. In the case of blocking information relevant to a topic, it is difficult because not only are there billions of websites, but new ones are created all the time, making it nearly impossible to create a fully updated list of sites of forbidden content. A more effective way to do this is to use URL filtering. This mechanism scans the requested Uniform Resource Locator (URL) string for specific keywords. In case the URL includes these forbidden words, the connection is reset.

Packet Filtering

This is one of the most recent and most sophisticated internet censoring technologies. In packet-switched networks like the Internet, telecommunication traffic is sliced into packets. Packets are relayed over the network using routers and reach their receiving computer according to their IP address. IP address filtering can only block communication based on where packets are going to or coming from. This technique does not take into account the actual content data. In order to do so, deep packet inspection should be done to examine that can search for banned keywords. Communication identified as containing forbidden content can be disrupted by dropping the connection. In this case, users may receive an error message in their browser, which may not indicate that they are being censored.

Censorship Software

For security reasons, some countries require special software or Trojans (Policeware or govware) installed in computing devices that filter internet content. In China, for instance, all PCs must be sold with software that allows the government to update computers with an ever-changing list of banned sites regularly. This technique is commonly used in the United States to set up filtration systems in libraries, schools, and public internet cafes.

Port Control

Specific port numbers can also be blacklisted, restricting access to services such as Web or email. This is often done by corporations who wish to restrict certain usage by their employers while at work, for example, instant messaging.

Applying the above-described techniques is often disguised as a technical error or connection problem, and that is why it is difficult to determine whether internet censorship is applied, which technique is being used, or who is blocking. This also makes it difficult to circumvent censorship. While some devices, such as proxy servers or virtual private networks (VPN), are widely used to get around filters, they may not work in all cases.

13.5.3 The Case of China

13.5.3.1 Historical Overview

In the 80s, China's leader Deng Xiaoping put in place multiple political reforms targeting economic growth while envisioning an extensive modernization plan for China. He famously quoted on Western influence, knowing its potential negative impact: "*If you open the window for fresh air, you have to expect some flies to blow in.*" So, when, in 1994, internet technologies reached the nation, Jiang Zemin, the successor of Deng, carried his political ways on socioeconomic ramifications. He understood it was a big opportunity for the global market stage but did not want any "flies" to blow in. So, he set out to discover a filtering method while also maintaining the accessibility framing of the internet. A Chinese resident and computer scientist named Fang Binxing met the solution to this endeavor by developing a surveillance program called "*Golden Shield.*" Applications of this program involved, among others, inspection of data received or sent along with a sophisticated feature of blocking IP addresses and domain names.

After a couple of years, in 2000, in partnership with the Ministry of Public Security, the Shield project was launched under the auspices of "*China Security 2000,*" aiming to improve the performance of the public security and welfare sector. Thus, one of the most iconic dilemmas of the modern era was born. On the one hand, the internet and its information flow were boosting the economy, while on the other hand, risking a democratic wave was on the way through ideology diversification of ideas, undermining the ongoing nationalistic political status. The program first adopted the task of promoting the implication of advanced

data, information, and communication technology (ICT) to strengthen central police control, increasing responsiveness and crime combating capacity. Its major applications in Chinese lifestyle included access to every citizen's record, plus the linkage of national, regional, and local security, all in an organized server body under Beijing's guidelines. Until 2002, the Golden Shield was developed significantly as internet users boomed unexpectedly. The notable result of these adjustments was the shift of the project from a generalized online content control tool to a continuous content filtering firewall projected on an individual level, tapping into everything, earning its press nickname as the "*Great Firewall.*"

In the same year, authorities decided to ban Google, followed by establishing a public pledge proclaimed as "Self Discipline for China's Internet Industry." The pledge came down to four main principles: patriotic observance of the law, equitability to justice, trustworthiness, and honesty. The document was officially signed by more than one hundred private and domestic companies, one of which was Yahoo.

By mid-2006, the total number of Chinese internet users had already reached 123 million. This meant that China had surpassed every country in the number of internet users except for the United States. Over half of the Chinese users had access to broadband internet, and the number of Chinese citizens who used instant messaging services had more than doubled. By 2012, people were using the web to hold their officials accountable for certain incidents that the law ignored. Users organized polls and graphics for the online spread of news and opinions on various platforms, sometimes exposing the government's propagandistic tendencies and usually disposing evidence, or even worse, destroying it. It happened to such an extent that in 2013, the Chinese leader Xi Jinping publicly stated that "the internet has become the main battlefield for the public opinion struggle." Later the same year, he also personally attended the Central Cyberspace Affairs Commission, whose goal included overseeing and guiding the government's bureaucratic standards on the complicated management of China's sub-internet-exclusive environment. Ultimately, a pattern of authority derived limitations and a climax of public unrest occurred as the nation's core disengaged progressively from the rest of the world.

Nevertheless, due to high internet penetration rates in Chinese society, there have been high expectations as many believed that this new technology could facilitate political change and transform China into a democratic regime. However, in reality, these expectations were never met. The Chinese Communist Party (CCP) had already managed to restrict internet use, achieving its utilization and turning it into a tool of control. Although the internet did not succeed in transforming the political landscape in China, many optimists pointed out the almost unlimited potential of the technology to generate liberating effects and the fact that internet users could somehow use new technologies to limit governmental control and create a more open society (Zheng, 2008).

Social media has become a pervasive and transformative force for Chinese citizens. It has changed not only how citizens express their opinions and share information but also how the CCP rules and communicates. The CCP now heavily invests in addressing citizens using social media and seeks to control the speech on these platforms. The Internet and social media platforms have altered the fabric of China's civil society. All areas of public concern are being discussed in cyberspace, which means there is not only a technological and economic change in China but also a political one. The rise of the Internet and social media has led to a partial liberalization of the political climate. This partial liberalization has caused concerns to the CCP about the Internet's and social media's potential to facilitate efforts to erode the regime's authority. As a result, the CCP has made new efforts to try and control this new landscape (DeLisle et al., 2006). The CCP had to benefit from the economic growth that the Internet brought to the country but always maintained control and censored anything that could negatively impact the regime.

There is a constant battle between the CCP and the netizens of China, but the censorship that the people experience does not seem to have improved over the years; in fact, the rules are stricter now than ever.

Internet freedom reached a new low in 2019 as the risk of citizens being detained or imprisoned for sharing or accessing information online has multiplied. The CCP is targeting many different categories of individuals and even plain X users (which is blocked) in China; users can only gain access to it using circumvention tools such as virtual private networks (VPNs) (Cook & Truong, 2019). In addition, the Chinese government s lists individuals deemed to threaten national security and public order. The list contains severe criminal offenders, people released from prisons or labor camps or drug users. However, in practice, a far broader range of people is monitored since they are considered key individuals by the authorities. The lists also contain petitioners, members of banned religious groups like *Falun Gong*, and those involved in "stability maintenance" or "terrorist" activities, two terms often applied to rights activists, protesters, and members of ethnic minority groups.

Besides, employing various means of censorship, the most significant accomplishment of the regime is that it has managed to build and promote state legitimacy through economy, nationalism, ideology, culture, and governance to ensure that the citizens will comply with the system of control that the CCP has created. In its evolution through the last two decades, the Chinese Internet has witnessed the growth of authoritarianism and also the development of grassroots activism fuelled by contention and participation. The co-evolution of online activism and authoritarianism is a constant battle or best described as a "cat and mouse" game. China's regime has proved that the diffusion of the Internet is not an insurmountable threat and has so far managed to promote the Internet as a tool for economic development while simultaneously minimizing the negative political impact. Overall, despite limited political freedoms, people's rights in other domains have expanded. So, the current situation is complex and dynamic, which makes it difficult to pronounce immediate winners or losers (DeLisle et al., 2006).

13.5.3.2 The Internet Control in China

The evolution of the Internet control regime in China can be broken down into three stages. The first stage is chronologically placed between 1994 and 1999. During this stage, the main focus was to establish the general framework of how the internet would work in the country, so the CCP focused on the regulation of network security, internet service provision and required institutional restructuring. The most significant act of institutional restructuring was the merging of the Ministry of Post and Telecommunications and the Ministry of Electronics Industry, which happened in 1998 as the merging led to the creation of the Ministry of Information, which became the primary regulatory agency of the information industry.

The second stage can be identified from 2000 to 2002 and can be summarized as the stage where Internet control expanded and refined. The main focus of this stage was strengthening content regulations that targeted not only Internet content providers but individual consumers as well. In addition, during this time, filtering technologies were first introduced and the CCP created lists of forbidden terms that were distributed to website owners for the first time to censor speech.

The third stage began in 2003 and marked the expansion of Internet regulation and control, and the introduction of new principles for Internet control. These new principles led to creating implementing a new framework through some new initiatives. The Chinese government launched campaigns to promote corporate social responsibility, professional codes of conduct, and self-discipline regarding Internet use. Moreover, a strong emphasis emerged on forging positive public opinion regarding the Internet. This meant that t the state tried to incorporate the Internet into the mass media to apply the same regulations. Yang (2009) stated that "treating the Internet as new media, or the mediatization of the Internet, allows the state to extend its framework of mass-media control to the Internet".

The government in China mostly uses three types of censorship: *the Great Firewall*, *the Golden Shield* and the *Keyword Blocking*. They all end with little or no access to foreign websites, and the blocking of

forbidden keywords and phrases to search or send to someone. It affects e-mails, blogs, websites, and even search engines. They track the IP addresses by monitoring Internet service providers, and, in many cases, ends with the "offender" (Monggilo, 2016). Here is a demo example of Keyword Blocking: In December 2010, Nick Kristof of *The New York Times* opened an account on *Sina Weibo, a Chinese social networking platform (presented later),* to test its level of censorship; his first posts were "Can we talk about Falun Gong?" and the second one was "Delete my weibos if you dare! My dad is Li Gang!". The post on Tiananmen Square was deleted within twenty minutes; after attracting the broader attention of the media, his entire account was shut down as well. He had the account for less than an hour, in total.

Three systems, or stages, were created after establishing the telecommunications legislature in 2000. The first one demands a license for a site to be registered, then it needs to be pre-approved and then fully approved for the function of specific sites. These all aim to prevent by prohibiting whomsoever from producing or reproducing news and information which contain the following: disagreement with the constitutional principles, danger to national state security, hostility towards the state's interests, tendency to hatred and racism, information which can cause social disorder, offensive stuff, or violence.

The CCP has also set a series of laws requiring companies operating in China to store user data on local servers. The authorities can access these data if it is deemed necessary. The list continues with Real-name registration, an army of human content moderators that survey and police online content, and to cap it all off, the government does not hesitate to threaten or harass citizens who speak against the CCP (Huang, 2019). The government has employed a multi-layered strategy to control online content and activities. Authorities of all levels utilize strict regulations, surveillance, imprisonment, propaganda, and the blockade of many international websites with the use of the "*Great Firewall*" of China. The authorities' tactics include all methods presented in the previous paragraphs. Keyword filtering is a prime example. A list of more than a thousand words is automatically banned in China's online forums, including dictatorship, truth, and riot police (Xiao, 2011). Some techniques are oriented on the psychology of the surfer, slowing the source, sabotaging its accessibility, or misdirecting its data. Among other methods used are flooding, domain name system (DNS) poisoning, and fear. The former overwhelms the source's output with false information, so the online visitor may not distinguish real from fake. The poisoning drags the speed of the source to an almost unusable state, driving the user to an alternative domestic service.

The "*Great Firewall*" constitutes the most well-known tool that the CCP uses to block internet users from accessing foreign websites with which Chinese authorities restrict the information exchange between citizens living within it. Moreover, it shapes and directs public opinion and influences how information that contradicts the regime-provided information is perceived. As a result, it becomes clear that information is not only censored but tailored to promote the view that the CCP wants regarding Chinese history and foreign countries to promote nationalist sentiments (Maags, 2019).

Up to recent years, the *Great Firewall* continues to receive upgrades with more complex algorithms, tackling external and internal threats to the national communist interest. It consists of crucial applications, one of which was in 2015, when the "Great Cannon" service was launched, aiming at foreign news, translated in Chinese, from providers like *The New York Times* or *The Washington Post*, that were taken down. Chronically parallel began an extensive strike on virtual private networks (VPNs), resulting in the deepening of the struggle regarding the private sector, which depended on bypassing the *Great Firewall* trying to contact foreign markets and investors. Although many companies decreased their activities, there were some, that through cooperation with the central regulatory bodies, even benefited from the cut. That is at least the case for the founder of Baidu Robin Li, and Xiaomi's founder and CEO Lei Jun, who were both offered the honor to run their own political offices.

Finally, during this last stage of evolution, a new propaganda mechanism emerged, hiring "Internet commentators" either as volunteers or as paid staff. Their job was to intervene in online discussions and guide the debates in a direction aligned with the party's propaganda. As a result, these commentators have earned a bad reputation that christened them with the name "fifty-cent party" because according to the story, the authorities pay them 50 cents per post (Yang, 2009).

13.5.3.3 Social Media in China: The Rise of Weibo and WeChat

YouTube, Instagram, Facebook, and X have been banned in China. Everything started on January 27th, 2008, when a bunch of sexual content photographs of Edison Chen and Gillian Chung were released at a Hong Kong forum. Soon, many other celebrities' photos were released until the police found the culprit and put him in jail. He was an IT technician named Sze Ho-chun. Subsequently, a chain of events regarding internet censorship started, with a Websites Correction Campaign taking the initiative later in 2008 to eliminate all undesirable content. This is when all the worldwide famous social platforms were banned in China. In the beginning, many Chinese people, mainly parents and school teachers, supported the government's actions since they believed that this would lead to an internet clean-up and a better online environment for their children. Little did they realize that for the government, the whole incident was a very suitable excuse, and it became the instrument of taking advantage of and promoting all these restricted policies in order to create a more manipulated society (Wang, 2011).

With the internet's core almost totally driven through the Western trendsetter and its corporations, Chinese technology services parallel to governmental rule started a commonly beneficial policy, the "*Block and Clone*" initiative. The plan relied on the action of the Great Firewall, tracking an external popularly visited source and applying pressure using one of the previously mentioned methods. Then tech providers, pouncing on the market void of displeased demand, produced similar Chinese sources that play by the one-party's rulebook. These two resulted in the creation of an enclosed environment of copied services. In China, for instance, YouTube, is replaced with its Chinese duplicate, Youku. Similarly, for Google, there is Baidu, for X, there is Sina Weibo, and the list continues. The "*Block and Clone*" benefits the domestic investment sector of economic growth, as users opt for local options, while the surveillance operation collects more fluent data.

As has already been made clear, Facebook is blocked by the "great firewall of China" although people can still access it via Virtual Private Networks (VPV). However, Facebook has reported that its market share in China is "almost zero." There are several other websites like Facebook, such as:

- **Douban**, a more specialized social networking site that attracts art students and those passionate about books, cinema, culture, and music. Users connect according to their interests and often hold offline activities such as trips.
- **Kaixin001**, a platform designed for a more mature audience of young professionals. Users do not upload personal content but instead share information they find, often relating to health, relationships, and professional advancement.
- **RenRen**: A platform similar to Facebook that attracts university students who use it to connect and interact with classmates. Originally called Xiaonei (which means campus), it started in 2005 and tended to be used by teens. It had around 178 million users in 2012 but started to lose customers because there was no efficient mobile version. In late 2013, RenRen launched a mobile app targeting people born in the 90s, and it has increased its registered users to approximately 219 million, reaching 54 million active monthly users.

X is also one of the social networks blocked in China, but it is said to have around 50,000 users in China who access it via VPNs. Microblogs or Weibos are very popular communication platforms in China.

YouTube is blocked as well, but there are several local versions. The most popular Chinese site for watching videos was YouKu, which had 100 million visitor views in January 2013, rising to 400 million by

August. Baidu is the "red" version of Google. Generally, Google blockage includes the Google search engine, translators, Gmail, and all other Google suite products. In addition, the block covers Google Hong Kong and all other country-specific versions, e.g., Google France.

In August 2009, *Sina Weibo* appeared, and until now, it is one of the most influential and popular social media platforms. It is a micro blogging site; like the Chinese version of X, since it has a 140-word post limit. *Weibo* users are also able to arrange and classify the accounts they follow to avoid the accumulation of information. People can participate in open public discussion even though some issues of sensitive areas are still blocked and deleted. Those with a large number of followers, or the "*Big Vs"* as they are called, are subject to stricter control and censorship since they influence public opinion more easily (DeLisle et al., 2016). A big advantage of Weibo is that its system associates the posts with each user's interests, which works well for the commercial field.

Tencent is Sina Weibo's main competitor, the third most popular social network in the country, with more than 230m active users. It has a user base of 507 million users, thanks to Tencent's instant messaging service called QQ.

Therefore, the isolationism and actions of the Chinese regime have led to some interesting technological innovations. A strong example is *WeChat*, the so-called by Western counterparts super-app. It was introduced in January 2011. Its original range of functions expands from social media to payment organizing, from taxi to dating services and clothing or food deliveries. Raising the bar even higher, it offers home service orders, like a private cleaning assistant, a hospital and doctor appointment system, and a traffic heat map of your route to a designated destination. Needless to add, all these data are under the jurisdiction of the central surveillance body, feeding it constantly with private user information related to the whereabouts of an individual's locations, their annual income, and their favorite restaurant.

Many users of Weibo have migrated to *WeChat* since it offers the opportunity to communicate among small private groups. In this way, the danger of political censorship was reduced, and people started to feel more free to discuss more "forbidden" issues there. It is a mobile-based application, and after its appearance, it soon became the most popular instant messenger in China. However, although it is a platform mainly created to make social interactions easier, it does not focus on generating public information. *WeChat* users are only allowed to post once per day with no limitation regarding the post's length, given that they have a public account. Another restriction comes to the organized groups of no more than 100 people. In that case, people must link their *WeChat* account to a Chinese bank card to join the group. That means the company behind *WeChat* knows these people's real identities (Stockmann & Luo, 2017). In a recent example of the company *Tencent* shutting down public accounts in 2014, almost forty public accounts were closed because they were thought provocative and they did not provide qualitative content to the users (Ruan et al., 2016).

Even though it seems that domestic social media platforms are quite "open" in China's online realm, there is also hidden—or not so hidden—censorship behind it. Keyword filtering and blocking is the method that is used for every *WeChat* user being registered with a mainland China phone number. The restrictions will still be the same, even if a person travels out of China. How does it work? The answer is on the server side. When someone wants to send a message via *WeChat*, the message is first sent to a remote server and checked for forbidden keywords. If it contains one or more, it will not be sent to the receiver.

According to Ruan et al., most keywords are generally censored and blocked in group chats and not so much in one-to-one chats. They are specially targeted because they have much more influence and can affect more people regarding a sensitive topic, especially the Chinese political scene. Furthermore, a URL filtering system implemented in *WeChat*'s integrated browser. Some websites will never appear on a user's screen connected in mainland China, and they are not only related to politics but also gambling websites, or of socially motivating content.

What is also worth mentioning is that when users try to send a message with blocked keywords, they are not informed that their message was not sent. The implementing censorship just rejects it, and no one knows why. There is not even a warning notification, and this is how it works for the Chinese national-level filtering system, the so-called Great Firewall of China. Blocked and censored websites do not indicate that they will not appear. Instead, a network timeout error appears on the screen, which, in any other case, could mean a very "busy" network or a functional problem.

At the beginning of 2015, the Great Firewall of China blocked many private networks, trying to avoid and bypass the consequences of the filtering system. Later that year, the government released the *Great Cannon*. Its main difference with the Great Firewall was that instead of blocking content, it would modify and replace the undesirable content.

13.5.3.4 The Impact Outside PRC: The Case of Hong Kong

In the case of Hong Kong and the agreement of "one country, two systems," things are quite contradictory regarding the applied censorship deriving from the "mainland." People in Hong Kong live outside China's Great Firewall, meaning they can use Facebook, YouTube, or X freely. Having in mind the movement going on in Hong Kong regarding people's human rights and their abuse by the Chinese government, it is quite obvious that the more international interest they attract, the more they try to conceal the situation and not let the world see the real consequences. TikTok's example and its sudden huge appearance in the world market during March-April 2020 with the COVID-19 pandemic can be indicative. It is said and believed that the Chinese application has limited and localized the restrictions and the censors to its Chinese audience. However, when TikTok's general guidelines were leaked, they explicitly forbid content related to criticism of the Chinese authoritarian regime. News agencies all over the world have noticed that, indeed, there was a lack of information and news related to Hong Kong protests and the situation going on in the country. This can prove that even if an application has billions of users worldwide, censorship can be implemented if the creator of the application wishes to keep international attention away (O'Brien, 2019).

13.5.3.5 Domestic and Multinational Tech Companies

Domestic companies in the field of technology in China are an interesting topic. In most cases, the country's most prominent entrepreneurs are active government members, mainly in executive posts (Economy, 2018). In the marketing and multi-national companies' field things are quite complicated. Take the example of Google in 2010 when they ignored China's regulation system for filtering the content and redirected the users to the—free of censorship—Hong Kong site. The result was that the Chinese government blocked Google. According to Andrea Durkin and the Information Technologies and Innovation Foundation (ITIF), a Washington DC-based think tank, Google lost approximately $32.5 billion from2013 to 2019 because of the restricted Chinese market. That is why they started to develop Dragonfly, a Google search engine equivalent for the Chinese audience. More than that, some of the world's biggest tech companies have bowed to the Chinese government by submitting to their will. Companies like Apple, NBA, Blizzard-Activision, and many more have had to make decisions that favor the Chinese government. Some other big companies like Google and Facebook have had a more neutral stance that favored neither many times, but they acted according to the company's rules. The 2019 Hong Kong protests, known as the Anti-Extradition Law Amendment Bill (Anti-ELAB), have demonstrated the issue:

Apple

With the 2019 Hong Kong Protests going on, Apple initially allowed a Hong Kong location map app that tracks protest activities to go on its App Store, reversing an earlier decision to reject the submission. The app's name is *HKmap.live*, and it is an app that crowdsources the police's locations. Apple initially approved the app's

availability for Anti-government protesters in Hong Kong. The app has attracted positive and negative reviews, with one user calling it "lifesaving technology" while another said it supported law-breaking and put "citizens in danger." One day after, a commentary in China's state-owned *People's Daily* questioned whether Apple was "thinking clearly" for letting the App Store host an app that tracks the police's movements in Hong Kong. The California tech giant then reacted and took the app down. After removing the app, the Apple team responsible for the App store said in its final statement: "We created the App Store to be a safe and trusted place to discover apps. We have learned that your app has been used in ways that endanger law enforcement and residents in Hong Kong."

Google

The search giant said it disabled 210 YouTube channels that "behaved in a coordinated manner" while uploading videos related to the Hong Kong protests, and its discovery was "consistent with recent observations and actions related to China" by X and Facebook.

X

X had already uncovered more than 900 accounts originating from the PRC that were "deliberately and specifically attempting to show political discord in Hong Kong," the company said, along with an additional network of 200,000 accounts that were part of a broader spam campaign. That prompted X to announce that it would not accept advertising fees from state-controlled news media entities. The policy would not apply to taxpayer-funded entities and independent public.

Facebook

Facebook subsequently said it found seven pages, three groups, and five accounts it believed were involved in "coordinated inauthentic behavior" out of China, focusing on Hong Kong. Over 15,000 accounts followed at least one of the pages, and about 2,200 joined one of the groups. Facebook's discovery was based on a tip from X. Facebook told BuzzFeed News it would not make the same move but will take a "close look at ads that have been raised to us to determine if they violate our policies".

The biggest problem for companies outside of mainland China, regardless of size, is that they are in the dark. Most of the time, they are unaware of the exact guidelines the Chinese government implies or the standards which they need to fulfill not to be blocked or censored. This leads to ambiguity and not the most suitable conditions for a foreign investor to attempt commercial activity in China. Nevertheless, the Chinese market is probably the biggest in the world by population. The Chinese economy is very powerful and necessary for the whole global economy. The challenge for foreign companies is always there, and the possibility for things to loosen remains unknown.

13.5.4 The Case of Turkey

In the 2002 national elections, the AKP (Justice and Development Party) rose to power, and its leader, Recep Tayyip Erdoğan, became the Prime Minister. This tenure officially launched in 2003 and lasted until 2014. The 2014 elections were the first time the president was elected directly, rather than by the parliament. Erdoğan won easily in the first round of voting and took office on August 28, 2014.

Following the failure of AKP to reach a parliamentary majority in June 2015, the following year, Turkey's President experienced a violent and bloody coup attempt. On the night of July 15, a limited number of military personnel invaded Ankara and Istanbul and took possession of facilities, including television stations and bridges. Some coup plotters accused Erdoğan and the AKP of undermining democracy as well as tearing apart the rule of law. However, loyal military units and civilians soon overpowered the coup plotters, and the government quickly regained control. The number of losses during the coup, was nearly 300 people, mostly

civilians. Notwithstanding the critical reverberations on the army, judiciary, law enforcement, and civil society, the abortive coup set in motion a massive purge of civil servants, closure of media outlets, arrests of journalists, and blocking of websites and social media accounts.

13.5.4.1 Internet Policy

The first case of website blocking took place in 2002 when a military court ordered a website to shut down due to the publication of documents concerning claimed corruption within the Turkish Air Force (Akgül & Kırlıdoğ, 2015). The first mass website blocking took place in 2005-2006 when the courts blocked more than ten websites with the excuse of copyright infringement because they provided hyperlinks to downloadable audio files or software to acquire such files. A huge step was taken a few years later when Turkey chose to purge the internet of undesirable and inappropriate content, which resulted in the censorship of websites. The censored sites ranged from child and adult pornography websites to commonly used platforms such as YouTube, Blogger, or Alibaba.com (Akgül & Kırlıdoğ, 2015).

That year, Turkey enacted its first internet-specific legislation, “Law No. 5651, Regulation of Publications on the Internet and Suppression of Crimes Committed by Means of Such Publications.” It was formed for fear of moral issues such as teen sexuality, pornography, drug use, video games and violence. It was, therefore, introduced to protect users from illegal and harmful content.

According to “Internet Law,” the Presidency of Telecommunications and Communication (TIB) was assigned to carry through with administrative duties such as monitoring content and mandating hosting and access providers to combat categorical crimes (Yurtsever, 2019). The Information and Communication Technologies Authority (BTK) was established as the “regulatory authority for the telecom sector”, and it was responsible for the enforcement of the legal framework provided by the Law (Yurtsever, 2019).

The law introduced seven categories of crime (provocation to suicide, facilitation of the use of narcotics, child pornography, obscenity, prostitution, facilitation of gambling, and defamation of the legacy of Ataturk). It specified that a website could be blocked by a court order or an administrative order issued by the TIB if it was found to be committing one of these crimes. It also forced hosting and access providers to keep track of online content transmitted through their infrastructure and required them to ban access to illegal content once they were served with a court order or a TIB-issued notice.

Various types of Turkish online restrictions range from throttling to prosecution of users. These are throttling, internet shutdowns and cloud/VPN restrictions, internet sovereignty and data localization initiatives, the prosecution of social media users, and the institutionalization of “snitching.” Throttling is a way of limiting specific types of online content. Both social media platforms and private messaging applications are throttled to restrict online communications in the aftermath of terrorist attacks, security, and military-related incidents (Yaguez, 2017). Internet sovereignty and data localization initiatives refer to cases where Turkey creates digital borders and launches country-specific social media platforms. This venture aims to monitor and control the flow of information from outside Turkey. In conjunction with enhanced surveillance of online communications, Turkey attempts to store user data within Turkey’s borders and ensure that communications can be thoroughly analyzed domestically.

13.5.4.2 Cases of Social Media Blocking

In December 2010 in Tunisia, it was Mohammed Bouazizi’s exertion of working as a street vendor that led to his self-immolation, a fact that unsettled the whole Tunisian society. His act was recorded by passers-by and was uploaded on YouTube. After that, video footage from massive protests following his funeral was also added. Later, on January 11, protests got into the capital city, Tunis, causing President Zine al-Abidine to release a night-time curfew. Sfax, Tunisia's second city, was to follow the next day. On January 14, 2011, Bed

Ali fled the country. Tunisia's government had been ousted by its people, with France, being the powerful country to sway Tunisia, supporting the conduction of the election.

Ben Ali's regime banned YouTube in Tunisia during the month of commotion. However, cyber activists still posted texts and contexts about protests on social networking sites. Facebook got an 8% increase in Tunisia, getting from 16% to 24% of the country's population.

In Egypt, political unrest existed long before Tunisia against the long-time Prime Minister Hosni Mubarak. The US State Department began publishing critics about the fundamental rights of expression and congregation, aiming to stimulate action to reform Egyptian politics.

Meanwhile, an unfortunate incident caused Egyptian people to create a Facebook page named '*We Are All Khaled Said*' with over 500,000 members. An Egyptian businessman, Khaled Said, died after being beaten by the police because he had videotaped police officers taking confiscated marijuana. Hoping to draw attention to police corruption, he copied that video and posted it to YouTube.

After this incident and all those years of political dissatisfaction, the Egyptian protestors inundated Cairo's Tahrir Square under the watchful eye of a military that was loath to turn on citizens. In order to impugn the protestors, the government imposed a night-time curfew and sought to block access to Facebook and X. This strategy failed as numerous supporters all over the world managed to subvert the censorship. When the Mubarak regime realized social media's power, effectiveness and extraordinary capacity for mobilization and coordination among activists, it cut off Internet and cellular phone communication across Egypt on January 28.

On March 28, 2014, Turkey blocked YouTube, provoking an eventful restriction to more than 10 million Turkish users (Sezer, 2016). The crackdown happened just a few days before the nationwide municipal elections and days after the TIB order to block access to X.

The Turkish government reported that its YouTube ban came as a response to the leak of voice recordings, which included conversations between top government officials, the Turkish intelligence chief Hakan Fidan, Foreign Minister Ahmet Davutoglu, undersecretary of the Foreign Ministry Feridun Sinirlioglu and deputy chief of the general staff, Yasar Gürel, who were allegedly discussing the possibility of going to war with Syria. Erdogan rejected the allegations as lies and means of blackmail, accusing the opposition of attempting to undermine and slander his Justice and Development Party success (AKP) ahead of critical local elections (Letsch & Rushe, 2014).

On April 29, 2017, Turkey blocked access to the online encyclopedia *Wikipedia* to all its language editions throughout the country, referring to the law ("Law No. 5651") by which the government can ban a specific number of websites with the excuse of the protection of the public. Users trying to access *Wikipedia* online via Turkish internet providers received a "connection timed out" error message. Precisely, this restriction happened due to the publication of an English article that depicted Turkey as a proponent country for ISIS and Al-Qaeda. Indeed, the service in charge (Wikimedia Foundation) refused to remove the articles that accused Turkey's government of cooperating with the well-known Islamic State (IS) group and al-Qaeda in Syria. Since then, the Turkish president has suspended 120,000 police officers, civil service employees, and judiciary workers. He decided to close dozens of media organizations and arrested more than 40,000 people who were reported to be associated with terrorist groups (Phippen, 2017). However, after almost three years of restriction (April, 29, 2017-January 15, 2020), the Turkish Constitutional Court ordered that the ban violated one of the fundamental human rights, the right to freedom of expression and, thus, it was decided, in to lift the block and gradually restore the access.

A watchdog website called "*Engelliweb,*" which monitors the blocked websites in Turkey, reported that since May 2015, approximately 80,000 websites have been blocked. However, the real number is far beyond these numbers, as *Engelliweb* only announces the blocked websites signaled by internet users. About 93% of

the sites registered in *Engelliweb* are blocked by a decision of the TIB, which means they are blocked without a court order. Most of the blocked sites include pornographic content. The other group contains the websites of opposing political groups and Kurdish insurgent movements. Almost all of the pornographic websites are international and do not specifically target Turkish audiences. On the contrary, the banned political websites target the audience in Turkey and can only be accessed by VPN.

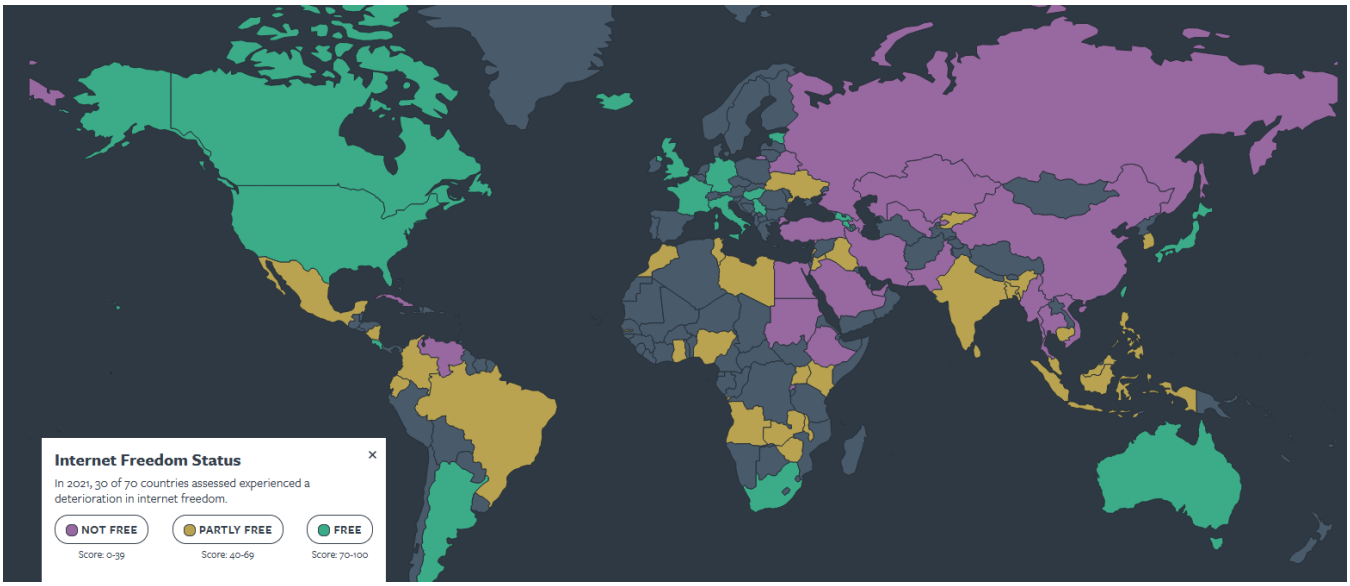


Figure 13.6 *Internet freedom status globally for 2021 (Source: https://freedomhouse.org).*

13.5.5 A Global Assessment

"*Freedom on the Net*" is an American report issued by the *Freedom House.* It is founded on the core conviction that freedom flourishes in democratic nations where governments are accountable to their people. The report measures the "level" of internet and digital media freedom around the globe. Each country receives a numerical score from 0 to 100 (the least free), which serves as the basis for the status of free (0-30 points), partly free (31-60), and not free (61-100 points) (**Figure 13.6**). Ratings are determined by examining three categories: obstacles to access, limits on content, and violation of user rights.

Table 13.3 *Top-10 countries according to Internet Freedom scores for 2021 (Source: https://freedomhouse.org/)*

	Country	Total Score and Status	Obstacles to Access	Limits on Content	Violations of User Rights
1	China	10 Not Free	8	2	0
2	Iran	16 Not Free	8	5	3
3	Myanmar	17 Not Free	4	7	6
4	Cuba	21 Not Free	5	9	7
5	Vietnam	22 Not Free	12	6	4
6	Saudi Arabia	24 Not Free	12	8	4
7	Pakistan	25 Not Free	5	13	7
8	Egypt	26 Not Free	12	10	4

9	Ethiopia	27 Not Free	4	12	11
10	United Arab Emirates	27 Not Free	12	9	6

In the 2021 report, China was ranked first (**Table 13.3**), scoring 10/100, being the worst among restrictive countries worldwide, with a side score of 8/25 in the *Obstacle to Access*, 2/35 regarding *Limits on Content,* and 0/40 on what has to do with *Violations of User Rights*. Freedom of House reported that "*conditions for internet users in China remained profoundly oppressive and confirmed the country's status as the world's worst abuser of internet freedom for the seventh consecutive year*" (Freedom House, 2021).

Regarding Turkey, for the same year it was reported that "Internet freedom continued to decline for a third year in a row in Turkey. Hundreds of websites were blocked, during the coverage period, sometimes under a new social media law." Turkey scored 15/25 in *Obstacle to Access, 10/35 in Limits on Content, 9/40 in Violations of User Rights, and a total score of 34/100.* (Freedom House, 2021).

It should be noted that the report does not include countries where no data is available, such as North Korea, where people are not allowed to use the internet.

13.6 Conclusion

The confidentiality of personal data is threatened daily by many factors. It is often insufficiently protected and immediately needs attention to maintain online privacy and avoid risks. Digital security and privacy protection have become public policy priorities and critical challenges for governments, businesses, and individuals that aim to reduce risks and increase trust without inhibiting the opportunities offered by the digital economy. Protecting personal information is essential for building trust in e-business, e-government, and other online activities, mainly nowadays in an increasingly digital and data-dependent economy and society. Cybersecurity measures became mandatory for these issues.

This is why cybersecurity is a part of the national security strategy in most countries. In the name of this and after historical incidents such as the 9/11 attack, governments have adopted digital surveillance tactics. These practices enhance citizens' safety on the one hand, but on the other, they seem to threaten fundamental human rights and invade privacy, being, at the end of the day, incompatible with democratic values.

Surveillance is a prerequisite for online censorship to be applied, which is a practice deployed in many countries' authoritarian regimes across the globe, mainly for political reasons. Digital liberties are suppressed there, and the race between ways to circumvent these practices and new methods to monitor and control them can be endless.

The assessment of the situation is a dynamic process and, at the same time, a difficult task, as the issues involved are multifaceted and sometimes controversial. It should, however, be done, having as the primary axis in this process the indisputable importance of fundamental human rights and liberties.

References

Ackerman S., and Roberts D., 2019. "Obama presents NSA reforms with plan to end government storage of call data." [online] *The Guardian*. Available at: https://www.theguardian.com/world/2014/jan/17/obama-nsa-reforms-end-storage-americans-call-data [Accessed 5 January 2020].

Adkinson W. F., Eisenach J. A., and Lenard T. M., 2002. "Privacy online: A report on the information practices and policies of commercial websites." The Progress & Freedom Foundation. Available at: http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf [Accessed 5 April 2019].

Akgül M., and Kırlıdoğ M., 2015. "Internet censorship in Turkey." *Internet Policy Review*, 4(2).

Allam H., 2014. "Fans say Snowden is vindicated, deserves amnesty for leaks." [online] Available at: https://www.mcclatchydc.com/news/nation-world/national/national-security/article24761908.html [Accessed 5 January 2020].

American Progress.org, 2013. "What the Snowden Affair Says About US-Russian Relations." Available at: https://www.americanprogress.org/article/what-the-snowden-affair-says-about-u-s-russian-relations/ [Accessed 6 December 2019].

Anon (n.d.). "Security vulnerabilities and threats existing in the e-Governance." [online] Available at: http://ictpost.com/security-vulnerabilities-and-threats-existing-in-the-e-governance/ [Accessed 20 May 2020].

Avira Operations GmbH, 2016. "Avira phantom VPN secures your connection, anonymizes your activities, and frees up the whole web." [online] Available at: https://www.avira.com/en/avira-phantom-vpn?navsrc=store [Accessed 19 November 2016].

Bakir V., Cable J., Dencik L., Hintz A., and McStay A., 2015. "Public feeling on privacy, security and surveillance: a report by DATA- PSST and DCSS." Cardiff University and Bangor University. Available at: https://eprints.glos.ac.uk/5433/1/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf

Bartunek R. J., 2018. "Facebook loses Belgian privacy case, faces fine of up to $125 million." Reuters, February 16. Available at: https://www.reuters.com/article/us-facebook-belgium/facebook-loses-belgian-privacy-case-faces-fine-of-up-to-125-million-idUSKCN1G01LG [Accessed 15 February 2019].

BBC News, 2019. "Germany wants Snowden spying details." [online], https://www.bbc.com/news/world-europe-24770430 [Accessed 2 February 2020].

BBC.com, 2014. "Edward Snowden: Leaks that exposed US spy programme." Available at: https://www.bbc.com/news/world-us-canada-23123964 [Accessed 6 December 2019].

Belanger F., and Crossier R., 2011. "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems." *MIS Quaterly,* Vol.35 No.4 pp. 1019–1035. Available at: https://www.researchgate.net/publication/220259962_Privacy_in_the_Digital_Age_A_Review_of_Information_Privacy_Research_in_Information_Systems[Accessed 23 March 2019].

Bendrath R., 2009. "Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection." Paper presented at the International Studies Annual Convention, New York City, 15–18 February 2009 (PDF). *International Studies Association*. Retrieved 2010-01-08.

Bennett J. C., 1999. *Visions of Privacy: Policy Choices for the Digital Age*. Studies in Comparative Political Economy and Public Policy, Toronto: University of Toronto Press, Scholarly Publishing Division.

Berkman F., 2014. "AT&T's First Transparency Report Reveals 300,000 Requests for Data." *Mashable*. Available at: https://mashable.com/archive/att-transparency-report [Accessed 5 January 2020].

Blankenship J., 2013. "Cybersecurity or Cyber anything usage." [online] *Solutionary.com*. Available at: https://www.solutionary.com/resource-center/blog/2013/10/cybersecurity-usage/ [Accessed 7 November 2016].

Bowen B., Devarajan R., and Stolfo S., 2011. "Measuring the Human Factor of Cyber Security." Available at: https://doi.com/10.1109/THS.2011.6107876

Brathwaite S., 2021. "What are the 3 principles of Information Security?" Security made simple [online]. Available at: https://www.securitymadesimple.org/cybersecurity-blog/what-are-the-3-principles-of-information-security

Breslow J. M., 2015. "How AT&T Helped the NSA Spy on Millions." [Online] Available at: https://www.pbs.org/wgbh/frontline/article/how-att-helped-the-nsa-spy-on-millions/

Bryant N., 2013. "The Snowden effect on US diplomacy." *BBC.com*. Available at: https://www.bbc.com/news/world-us-canada-24664045 [Accessed 6 December 2019].

Butler I., 2017. "Security through Human Rights." Published online, pp. 10–32. Available at: https://www.researchgate.net/publication/329752069_Security_Through_Human_Rights [Accessed 15 November 2019].

Chertoff M., and Simon T., 2015. "The Impact of the Dark Web on Internet Governance and Cyber Security." PAPER, [online]. Available at: https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf [Accessed 20 May 2020].

Cohen E. D., 2010. *Mass Surveillance and State Control. The Total Information Awareness Project*. New York: PALGRAVE MACMILLAN.

Dan Tynan D., 2018. "Facebook says 14m accounts had personal data stolen in recent breach," *The Guardian*, Available at: https://www.theguardian.com/technology/2018/oct/12/facebook-data-breach-personal-information-hackers [Accessed 3 May 2019].

Davies H., 2015. "Ted Cruz using firm that harvested data on millions of unwitting Facebook users." *The Guardian.* Available at: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data [Accessed 3 May 2019].

DeLisle G., and Yang J.A.G., 2016. "The Coevolution of the Internet, (Un)Civil Society, and Authoritarianism in China," in Jiang, M. (ed.) *The Internet, Social Media, and a Changing China*. University of Pennsylvania Press. Project MUSE. pp. 29–31. Available at: https://muse.jhu.edu/book/44996 [Accessed 10 March 2019].

DeLisle J., Goldstein A., and Yang G., 2016. "The internet, social media, and a changing China." University of Pennsylvania Press, Philadelphia. Available at: https://books.google.gr/books?hl=en&lr=&id=KdiaCwAAQBAJ&oi=fnd&pg=PA1&ots=qwumXUToUe&sig=FoWiwI5BIwInxUIVBKAVBLceuhM&redir_esc=y#v=onepage&q&f=false [Accessed: 14 June 2020].

Economy E. C., 2018. "The great firewall of China: Xi Jinping's internet shutdown." *The Guardian*. Available at: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown [Accessed: 14 June 2020].

ENISA, 2016. NATIONAL CYBER SECURITY STRATEGY (version 2.0), ENISA, EUROPEAN UNION AGENCY FOR CYBERSECURITY. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/GRNCSS_EN.pdf [Accessed 2 February 2019].

Epstein E., 2017. "How Edward Snowden changed history." *The Economist*. Available at: https://www.economist.com/books-and-arts/2017/01/14/how-edward-snowden-changed-history [Accessed 15 December 2019].

Feldstein S., 2019. "The Global Expansion of AI Surveillance." Carnegie Endowment for International Peace.

Freedom House, 2019."Expanding freedom and democracy." Available at: https://freedomhouse.org/ [Accessed: 14 June 2020].

Fuchs C., and Trottier D., 2017. "Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden." *Journal of Information, Communication and Ethics in Society*, 15 (4), pp. 412-444. Emerald Publishing Limited. Available at: https://doi.org/10.1108/JICES-01-2016-0004

Gallagher R., 2016. "U.K. PARLIAMENT APPROVES UNPRECEDENTED NEW HACKING AND SURVEILLANCE POWERS." *The Intercept*. Available at: https://theintercept.com/2016/11/22/ipbill-uk-surveillance-snowden-parliament-approved/ [Accessed 6 December 2019].

Geere D., 2012. "How deep packet inspection works." *Wired*. Available at: https://www.wired.co.uk/article/how-deep-packet-inspection-works

Gellman B., 2013. "Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished." *The Washington Post.* Available at: www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html [Accessed 2 February 2020].

Gibb J., 2006. *Ποιος μας παρακολουθεί*. Αθήνα: Εκδοτικός Οργανισμός Λιβάνη.

Gibbs S., 2018. "Facebook ordered to stop collecting user data by Belgian court," *The Guardian*, February 16, 2018. Available at: https://www.theguardian.com/technology/2018/feb/16/facebook-ordered-stop-collecting-user-data-fines-belgian-court [Accessed 15 February 2019].

Gilbert F., 2008. "Beacons, Bugs, and Pixel Tags: Do You Comply with the FTC Behavioral Marketing Principles and Foreign Law Requirements?" *Journal of Internet Law*.

Granick J., 2017. "Reining In Warrantless Wiretapping of Americans." [Online] Available at: https://tcf.org/content/report/reining-warrantless-wiretapping-americans/ [Accessed 6 December 2019].

Granville K., 2018. "Facebook and Cambridge Analytica: What you need to know as fallout widens." *The New York Times.* Available at: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [Accessed 20 February 2019].

Greenwald G., 2013a. "NSA collecting phone records of millions of Verizon customers daily." *The Guardian*. Available at: https://www.theguardian.com/world/2013/jun/06/nsa-phonerecords-verizon-court-order [Accessed 18 December 2019].

Greenwald G., 2013b. "Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy." *The Guardian*, 29 July 2013. Available at: https://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew [Accessed 2 February 2020].

Guess A., Nyhan B., and Reifler J., 2020. "Exposure to untrustworthy websites in the 2016 US election." *Nature Human Behaviour*. 4. https://10.1038/s41562-020-0833-x

Hamelink J. C., 2000. *The Ethics of Cyberspace*, California: SAGE Publications Ltd.

Harkous H., 2016. "How Chatbots Will Redefine the Future of App Privacy." [online] Medium. Available at: https://chatbotsmagazine.com/how-chatbots-will-redefine-the-future-of-app-privacy-eb68a7b5a329 [Accessed 5 April 2021].

Haunss S., 2015. "Privacy Activism after Snowden: Advocacy Networks or Protest?" Heidelberg: Universitätsverlag Winter. Available at: https://www.researchgate.net/publication/292630367_Privacy_Activism_after_Snowden_Advocacy_Networks_or_Protest [Accessed 21 October 2019].

Hoofnagle C. J., Soltani A., Good N., and Wambach D.J., 2012. “Behavioral Advertising: The Offer You Can't Refuse." 6 Harv. L. & Pol'y Rev. 273. Available at: http://scholarship.law.berkeley.edu/facpubs/2086 [Accessed 5 April 2019].

Huang Z., 2019. “8 ways China controls the internet.” [online] Available at: https://www.inkstonenews.com/tech/what-china-can-teach-world-about-controlling-internet/article/3006687 [Accessed: 15 June 2020].

InternetLiveStats, 2014. "Number of internet users." [online] Available at: http://www.internetlivestats.com/internet-users/ [Accessed 18 November 2016].

Isaac M., and Frenkel S., 2018. “Facebook security breach exposes accounts of 50 million users.” *The New York Times.* Available at: https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html [Accessed 22 February 2019].

Isaak J., and Hanna M.J., 2018. “User Data Privacy: Facebook, Cambridge Analytica and Privacy Protection.” IEEE Computer Society 51, No. 8, pp. 56–59. Available at: https://ieeexplore-ieee-org.ezproxy.is.cuni.cz/stamp/stamp.jsp?tp=&arnumber=8436400 [Accessed 25 February 2019].

Juerveton S., 2014. "EU Asylum For Snowden? Our Reaction." World Wide Web Foundation. Available at: https://webfoundation.org/2015/10/eu-asylum-for-snowden-ourreaction/ [Accessed 18 November 2019].

Kelley M., 2019. "He Is Priceless: Here's Why Edward Snowden Is Screwed." [online] *Business Insider Australia*. Available at: https://www.businessinsider.com.au/why-edward-snowden-is-stuck-2014-4 [Accessed 2 February 2020].

Kelly H., 2013. Report: NSA mined US e-mail data. [online] CNN. Available at: https://edition.cnn.com/2013/07/04/tech/web/restore-nsa-protests [Accessed 21 February 2020].

Kerry C.F., Ann R., and Tisch A.H., 2020. "Protecting privacy in an AI-driven world." *Brookings*. Available at: https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/ [Accessed 31 January 2021].

Kharpal A., 2017. "Edward Snowden: US government ‘reckless beyond words’ after WikiLeaks docs show CIA hacking tools." CNBC. Available at: https://www.cnbc.com/2017/03/08/edward-snowden-wikileaks-cia-hacking-us-government-reckless-beyond-words.html [Accessed 6 December 2019].

Kouroupis K., Vagianos D., and Totka A., 2022. “Artificial Intelligence and Customer Relationship Management: The Case of Chatbots and their Legality Framework.” Accepted for publication in the 2021 issue of the *East European Yearbook on Human Rights* (https://eeyhr.eu).

Kojouharov S., 2018. "Chatbots, AI & The Future of Privacy." [online] *Medium*. Available at: https://chatbotslife.com/chatbots-ai-the-future-of-privacy-174edfc2eb98 [Accessed 5 April 2021].

Koty A. C., 2019. "China’s Corporate Social Credit System: What Businesses Need to Know." China Briefing. Available at: https://www.china-briefing.com/news/chinas-corporate-social-credit-system-how-it-works/ [Accessed 6 December 2019].

Kristol D. M., 2001. “HTTP Cookies: Standards, privacy, and politics.” *ACM Transactions on Internet Technology*, Vol. 1, No. 2, November 2001, pp. 151–198. Available at: http://www-cs.ccny.cuny.edu/~fazio/S13-csc48000/Kristol01.pdf [Accessed 5 April 2019].

Kuchler H., 2018. “Zuckerberg failed to fix Facebook users´ privacy concerns.” *Financial Times.* Available at: https://www.ft.com/content/171cc986-41b5-11e8-803a-295c97e6fd0b [Accessed 20 February 2019].

Kumari L., and Kumar R., 2015. "Impact of Cyber Security in different application of e-Governance: Case Study." [online] p. 365. Available at: http://tmu.ac.in/college-of-computing-sciences-and-it/wp-content/uploads/sites/17/2016/10/CCSIT322.pdf [Accessed 5 May 2020].

Leenes R., Van Brakel R., and Gutwirth S., 2017. *Data Protection and Privacy: (In)visibilities and Infrastructures*. Brussels: Springer.

Letsch C., and Rushe D., 2014. "Turkey Blocks Youtube Amid 'National Security' Concerns." [online] *The Guardian*. Available at: https://www.theguardian.com/world/2014/mar/27/google-youtube-ban-turkey-erdogan [Accessed 19 May 2020].

Longitude research, 2013. "Cyberrisk in banking." [online] Available at: http://www.instituteofat.org/whitepapers/cyberrisk-in-banking-106605.pdf [Accessed 18/11/16].

Lupton D., 2014. "The politics of privacy in the digital age." Available at: https://simplysociology.wordpress.com/2014/10/27/the-politics-of-privacy-in-the-digital-age/ [Accessed 5 April 2019].

Maags C., 2019. "The limitations of the Great Firewall of China." [online] Available at: https://www.fairobserver.com/region/asia_pacific/great-firewall-china-censorship-chinese-news-today-vpn-china-38018/ [Accessed: 14 June 2020].

Madhani A., and Jackson D., 2013. "Obama: I don't see Snowden as a patriot." [online] Eu.usatoday.com Available at: https://eu.usatoday.com/story/news/politics/2013/08/09/obama-news-conference/2636191/ [Accessed 21 February 2020].

Mann J., and Reitbauer A., 2017. "Beacon." W3C Candidate Recommendation, W3C.

Meserve A. S., Pemstein D., 2018. "Google Politics: The political Determinants of Internet Censorship in Democracies." Published online, pp. 4-14. Available at: https://www.researchgate.net/publication/313592681_Google_Politics_The_Political_Determinants_of_Internet_Censorship_in_Democracies [Accessed 15 November 2019].

Milojevic S. J., 2015. "BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT." Published online, pp. 4-7. Available at: https://www.researchgate.net/publication/326016248_BLOCKING_FILTERING_AND_TAKE-DOWN_OF_ILLEGAL_INTERNET_CONTENT [Accessed 15 November 2019].

Monggilo Z. M., 2016. "Internet freedom in Asia: Case of internet censorship in China, Jurnal Studi Pemerintahan." 7(1), pp. 153–179. Available at: https://journal.umy.ac.id/index.php/jsp/article/viewFile/1174/pdf_6 [Accessed: 14 June 2020].

Morrison, S., 2020. "Alexa Records You More Often Than You Think." [online] *Vox*. Available at: https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording [Accessed 5 April 2021].

Naarttijärvi M., 2013. "För din och andras säkerhet: Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel." Uppsala: Iustus förlag. Available at: https://www.researchgate.net/publication/316361343_For_din_och_andras_sakerhet_Konstitutionella_proportionalitetskrav_och_Sakerhetspolisens_preventiva_tvangsmedel [Accessed 21 October 2019].

Newcomb A., 2018. "A timeline of Facebook´s privacy issues – and its responses." *NBC News*. Available at: https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651 [Accessed 3 May 2019].

Nippert E., and Christena E., 2010. *Islands of Privacy*. Chicago: University of Chicago Press.

Norton, 2016. "2016 Norton Cyber Security Insights Report." [online] Available at: https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf [Accessed 18 November 2016].

O´Flaherty K., 2018. “Facebook data Breach – what to do next.” Forbes. Available at: https://www.forbes.com/sites/kateoflahertyuk/2018/09/29/facebook-data-breach-what-to-do-next/#3d5c0b6f2de3 [Accessed 20 February 2019].

O’ Brien D., 2019. "China’s Global Reach: Surveillance and Censorship Beyond the Great Firewall." *Electronic Frontier Foundation*. Available at: https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall [Accessed 10 March 2020].

OECD, 2013a. “Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value.” *OECD Digital Economy Papers*. Available at: https://econpapers.repec.org/paper/oecstiaab/220-en.htm [Accessed 5 April 2019].

OECD, 2013b. “The OECD Privacy Framework.” Available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [Accessed 5 April 2019].

Olsen S., 2002. "Nearly undetectable tracking device raises concern." *CNET News*.

Osborn A., and Powell S., 2017. "Putin says Snowden was wrong to leak secrets, but is no traitor." *Reuters*. Available at: https://www.researchgate.net/publication/316361343_For_din_och_andras_sakerhet_Konstitutionella_proportionalitetskrav_och_Sakerhetspolisens_preventiva_tvangsmedel [Accessed 18 December 2019].

Panchanatham N., (n.d.). “A case study on Cyber Security in E-Governance.” [online] *International Research Journal of Engineering and Technology* (IRJET) e-ISSN, pp.2395–0056. Available at: https://www.irjet.net/archives/V2/i8/IRJET-V2I846.pdf [Accessed 25 May 2020].

Papademas D., 2011. *Human Rights and Media, Studies in Communications*. (Book 6), UK: Emerald Group Publishing Limited.

Pearson J., 2012. “Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability.” *Digiworld Economic Journal*.

Phippen J., 2017. "Why Turkey Blocked Access To Wikipedia." [online] *The Atlantic*. Available at: https://www.theatlantic.com/news/archive/2017/04/turkey-blocks-wikipedia/524859/ [Accessed 19 May 2020].

Rainie L., Kiesler S., Kang R., and Madden M., 2013. "Anonymity, Privacy, and Security Online." Pew Research Center’s Internet & American Life Project.

Reitman R., 2013. “Under CISPA, Who Can Get Your Data?” Electronic Frontier Foundation, 20 Mar. 2013. Available at: www.eff.org/deeplinks/2013/03/under-cispa-who-can-get-your-data [Accessed 21 February 2020].

Reitman R., 2015. "EFF's Game Plan for Ending Global Mass Surveillance." EFF. Available at: https://www.eff.org/deeplinks/2015/01/effs-game-plan-ending-global-mass-surveillance [Accessed 1 December 2019].

Resolution of April 6th, 2001. “Seventh Revisionary Parliament” (Government Gazette A΄ 85 / 18.4.2001).

Rodriguez S., 2018. "Facebook security breach details." CNBC. Available at: https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html [Accessed 3 May 2019].

Romansky R., 2014. "Social Media and Personal Data Protection." International Journal on Information Technologies & Security No.4. Available at: https://www.researchgate.net/publication/307570419_SOCIAL_MEDIA_AND_PERSONAL_DATA_PROTECTION [Accessed 5 March 2019].

Rotenberg M., Scott J., and Horwitz J., 2015. "Privacy in the Modern Age: The Search for Solutions." Available at: https://books.google.gr/books?id-3TozBQAAQBAJ&printsec=frontcover&hl=el#v=onepage&q&f=false [Accessed 5 April 2019].

Ruan L., Knockel J. J. Q., and Crete-Nishihata M., 2016. "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally." Citizen Lab Research Report (84), University of Toronto. Available at: https://tspace.library.utoronto.ca/bitstream/1807/96729/1/Report%2384--oneapp-twosystems.pdf [Accessed: 14 June 2020].

Sanger D., 2013. "N.S.A. Leaks Make Plan for Cyberdefense Unlikely." *The New York Times*. Available at: www.nytimes.com/2013/08/13/us/nsa-leaks-make-plan-for-cyberdefense-unlikely.html?pagewanted=all&_r=1& [Accessed 21 February 2020].

Schofield J., 2015. "How can I make my PC completely secure?" [online] *The Guardian*. Available at: https://www.theguardian.com/technology/askjack/2015/jan/15/how-can-i-make-my-pc-completely-secure [Accessed 19 November 2016].

Schulze, M. 2015. "Patterns of Surveillance Legitimization: The German Discourse on the NSA Scandal." *Surveillance & Society* 13(2): pp. 197-217.

Security Scorecard, 2017. " 2017 Financial Industry Cybersecurity Research Report." [online] Available at: https://securityscorecard.com/resources/2016-financial-industry-cybersecurity-research-report [Accessed 18 November 2016].

Sezer C., 2016. "Turkey Blocks Access To Twitter, Whatsapp: Internet Monitoring Group." [online] *REUTERS*. Available at: https://www.reuters.com/article/us-turkey-security-internet/turkey-blocks-access-to-twitter-whatsapp-internet-monitoring-group-idUSKBN12Z0H4 [Accessed 20 May 2020].

Shailendra S., 2011. "E-Governance: Information Security Issues." [online] *International Conference on Computer Science and Information Technology*. Available at: https://www.researchgate.net/publication/266770761_E-Governance_Information_Security_Issues [Accessed 23 May 2020].

Skandali G., 2018. "Cambridge Analytica: How will it Play out for Chatbots?" online] *Medium*. Available at: https://medium.com/yellow-hammock/cambridge-analytica-how-will-it-play-out-for-chatbots-5c1d44f4fe29 [Accessed 5 April 2021].

Solms S., and Heerden R., 2015. "The Consequences of Edward Snowden NSA Related Information Disclosures." Research Gate. Available at: https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures [Accessed 18 November 2019].

Solove D. J., 2004. *The Digital Person, Technology and Privacy in the Digital Age*. New York University Press.

Stalder F., 2006. *Manuel Castells: the theory of the network society*. Cambridge: Polity.

Talmadge E., 2014. *North Korea: Where the Internet has just 5,500 sites*. Toronto Star. Associated Press. [Accessed 15 July 2019].

Timberg C., 2014. "Tech Companies to Government: Stop Secret Searches." *The Washington Post.* Available at: www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html [Accessed 21 February 2020].

Tréguer F., 2016. "After Snowden: Rethinking the Impact of Surveillance". Available at: https://www.researchgate.net/publication/275019554_The_Consequences_of_Edward_Snowden_NSA_Related_Information_Disclosures [Accessed 21 October 2019].

Tucker C., 2010. “The Economic Value of Online Customer Data.” OECD, Paris. Available at: https://www.oecd.org/sti/ieconomy/46944475.pdf [Accessed 5 April 2019].

UN Human Rights Committee (HRC), (n.d.). "CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation."

Wang D., and Mark G., 2015. "Internet censorship in China: Examining user awareness and attitudes." ACM Transactions on Computer-Human Interaction (TOCHI), 22(6), pp. 1–22. Available at: https://escholarship.org/content/qt48x7k7j2/qt48x7k7j2.pdf [Accessed: 14 June 2020].

Warf B., 2013. “Global Internet Censorship” Published online." pp. 8–16. Available at: https://www.researchgate.net/publication/303131145_Global_Internet_Censorship [Accessed 15 November 2019].

Watt N., 2019. "David Cameron makes veiled threat to media over NSA and GCHQ leaks". [online] *The Guardian*. Available at: https://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden [Accessed 21 February 2020].

Weinstein M., 2016. "13 ways your online privacy was violated in 2016 - and what you can do about it." *The Mirror*. Available at: https://www.mirror.co.uk/tech/13-ways-your-privacy-violated-9479084 [Accessed 5 April 2019].

Williams M., 2017. "All That Glitters Is Not Gold: A Closer Look at North Korea's Ullim Tablet." 38 North. US-Korea Institute, Johns Hopkins University School of Advanced International Studies. [Accessed 15 July 2019].

Winkler S., and Sherali Zeadally S., 2016. “Privacy Policy Analysis of Popular Web Platforms.” IEEE Technology and Society Magazine 35, No. 2: 75-85. Available at: https://ieeexplore-ieee-org.ezproxy.is.cuni.cz/document/7484849/ [Accessed 25 February 2019].

Wong C. J., 2018. "Facebook says nearly 50m users compromised in huge security breach." *The Guardian.* Available at: https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach [Accessed 3 May 2019].

Xiao Q., 2011. “Liberation Technology: The Battle for the Chinese Internet.” *Journal of Democracy*, vol. 22 no. 2, pp. 47–61. Project MUSE [online]. Available at: https://muse.jhu.edu/article/427160 [Accessed: 17 June 2020].

Yaguez B., 2017. "How Throttling Internet Has Become A Way Of Censorship In Turkey." [online] https://magazine.journalismfestival.com/ Available at: https://magazine.journalismfestival.com/how-throttling-internet-has-become-a-way-of-censorship-in-turkey/ [Accessed 21 May 2020].

Yang G., 2009. *The Power of the Internet in China*. Columbia University Press.

Yurtsever A., 2019. "INTERNET BANS IN TURKEY" [online] *ASY LEGAL*. Available at: https://www.asylegal.com/internet-bans-in-turkey/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration [Accessed 20 May 2020].

Zhe Jin G., 2018. "Artificial Intelligence and Consumer Privacy." Working Paper 24253. Available at: https://www.nber.org/papers/w24253.pdf [Accessed 5 March 2019].

Zheng Y., 2008. *Technological Empowerment: The Internet, State, and Society in China*. Stanford University Press [Accessed 10 March 2019].

Ziccardi G., 2012. *Resistance, Liberation Technology and Human Rights in the Digital Age*., Berlin: Springer.

Γέροντας Α., 2002. *Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων.* Αθήνα: Σάκκουλας.

Μάνεσης Α., 1981. *Συνταγματικά δικαιώματα, Ατομικές ελευθερίες*. Αθήνα: Σάκκουλας.

Μανωλεδάκης Ι., 2002. *Ασφάλεια και ελευθερία*. Αθήνα: Εκδόσεις Αντ. Ν. Σάκκουλα.

Παπαθεοδώρου Θ., 2009. *Επιτηρούμενη δημοκρατία*. Αθήνα: Βιβλιόραμα.

Σωτηρόπουλος Β., 2005. *Η πρόσβαση στη δημόσια πληροφορία και η προστασία προσωπικών δεδομένων.* Digesta.

Χοχλιούρος Ι., 2006. *Θέματα ασφάλειας ηλεκτρονικών υποδομών και εφαρμογών : διασφάλιση του απορρήτου και νόμιμη παρακολούθηση των επικοινωνιών*. Αθήνα: Εκδόσεις Αντ Ν. Σάκκουλα.

Chapter 14 Impact of Digital Media on Education and the New Generation

Abstract

This chapter analyzes the impact of technology and digital media in today's educational system. From the early use of computers in the school environment to the broad use of distance learning systems, social media, smart mobile devices, and cloud computing of the present, the benefits and drawbacks of technological advancements in education are discussed, and examples of the digital media applications in school across the globe are presented. The second part of this chapter presents the general implications of the use of digital media by the New Generation. The opportunities that children are given are described, including their potential for socialization, mostly through the formation of social media or online gaming communities. Finally, the threats, mainly including children's online victimization, isolation, internet addiction, narcissism, and cyberbullying, are highlighted.

14.1 The Impact of Digital Media on Education

14.1.1 The Need to Transform Education

In human history, education is in a continuously evolving state. Teaching methods and supporting tools are changing throughout this long evolution in order to serve the values that each society wants to promote. Education always aims to prepare the new generations to serve roles leading to society's further development. These roles differ from place to place and from time to time. Over the years, technology has become a very important tool in the hands of educators throughout the world, giving enormous power to teachers and making the teaching process more interesting and appealing to students. At the same time, it helped disseminate information and knowledge, solving and creating problems.

There is a worldwide concern that contemporary educational systems are outdated and fail to give children the necessary skills to prepare them for future challenges adequately. The previous generations' motivation to study was mainly based on the sense of duty. Younger generations have different motivational profiles, interests, emotions, and engagement, which are much more vital. The emerging social practices of the new generation are constantly evolving and so is Information and Communication Technology (ICT).

It is widely known that ICTs have brought changes to education. Over the last decades, it has been clear that educators, parents, and community leaders are accountable for providing educational opportunities to children by developing innovative learning methods.

The challenge is to respond to the technology and its extraordinary pace of change to provide a better learning outcome by adopting new approaches that include values such as creativity, innovation, critical thinking, problem solving, decision making, lifelong learning, collaboration and communication, ICT literacy, consciousness of being a local and global citizen, and personal and social responsibility.

It is a new challenge to enable the broader educational community to meet these requirements. Moreover, teachers need the capacity to plan and implement new learning methods and should be supported in the development of innovative teaching practices underpinned by digital technology.

The coming together of several historical factors highlights the essential need to engage in a step-change education by systematically developing new paradigms for learning and supporting these.

The first and most widely known such factor is the one related to changes occurring in the world, including:

- the shift from industrial to information-based knowledge economies,
- the globalization of products, markets, and companies,
- the changing patterns of life, including greater life expectancy,
- the significant advances in technologies requiring new kinds of literacy.

A second factor is the changing nature of work. The shift towards technology-rich workplace environments requires multidisciplinary teamwork, greater innovation and creativity. Manual labor and routine skills are increasingly being automated and, therefore, there is a need for a future workforce with digital competencies at a global level as well as with a spirit of creativity.

New and emerging technologies, such as cloud services, quantum technologies, augmented reality, and a semantic web leading to artificial intelligence, are inadequate to lead a successful transition to a bright future. We are currently entering a new and demanding epoch characterized by rapid technological advancements, wherein the outcomes of education will be shaped by the methods and support employed for teaching and learning.

14.1.2 The New Face of K-12 Education with the Use of Digital Media

K-12 education, which includes primary and secondary levels of education, has been among the slowest sectors of society to integrate digital media fully. Outside schools, only a few conduct research, analyze data, carry out a scientific experiment or write an in-depth paper without using an Internet-connected computer or digital device. In school, students can be taught to perform such tasks much better if they have the right tools to do so. Moreover, change is on the way. With the advent of low-cost netbooks and tablets, open access and cloud-based resources, and the growing digitalization of educational content and assessments, the question will move to how soon we will replace textbooks and paper with digital media.

The accelerating availability of digital media in schools, including devices, software, and content, introduces exciting possibilities. A child can use a wireless laptop, netbook, or tablet to access interactive and individualized instructional content; collect and analyze data for research projects, write, revise, and publish papers, communicate, and collaborate across the school or globe and use or create multimedia games, simulations, and computer programs.

However, digital devices cannot generate learning simply by being at the disposal of a child. It takes more than giving a child a netbook or iPad to transform education. Such transformation requires clear goals about what digital media in schools can accomplish, the appropriate curricula, pedagogy, and assessment to reach these goals, and the proper social and technical infrastructure to support this endeavor.

Still, in contemporary education, achieving effective learning using digital media is a major concern. Today's technologies relate to education in many ways instead of the historical pedagogies of a one-way discussion as an educational procedure. Today, individuals employ digital media and the Internet in naturally occurring ways, and education in this form is contemplated in the context of social change, which, in turn, is fully integrated with digital media.

Part of our lives is the daily use of all forms of digital media; and therefore, it has become a key component of education. Truly effective contemporary education must consider these elements—the changes they bring about in our social and cultural environment—and apply them today. Educators need to consider and act toward integrating digital media nowadays and in the future. Historically, educators have reviewed digital media in education, thinking of it in various roles, including tutor, supplier, communications, facilitator, motivator, stimulator of a specific activity or thought, and more, as digital media can serve this and beyond.

Today's society is considered a digital society. People enjoy using digital media and have many of its elements integral to their daily lives. Educational reform is crucial, though, the most critical point for any tool within the pedagogy framework is to assist educational reform to comprehend the best techniques and environment of students' lives as they take up new ideas in learning.

For educators to attain the levels of advancement in interest, capability, and stimulation within the grasp their students' attention, careful consideration must be given to the process of digital media. The emphasis is on what kind of content, skills, and attitudes enhance individuals, and on the ability to adapt to technology within education and society. This implies that the essence lies in how to learn instead of what to learn.

With the change from the "lecture and learn" model to fully interactive learning available through digital media, students acquire greater responsibility for their education and view it as a process of lifelong learning; they learn the consequences of enhanced thinking ability and problem-solving skills connected to the many tools around them. It is essential to describe digital media as a means for creating new approaches to learning. When using these technologies in education, the target is not just to prepare students for their careers but also to nurture a new generation of creative thinkers fluent in using digital media.

Selecting the right tools is one side of developing and sustaining a thriving educational environment with digital media. All these different tools for digital classrooms, platforms, apps, and devices can enhance education. Some of the most common tools that are used in the new digital era of education are the ones below:

One-to-One (1:1)

One-to-one environments, where all students have access to their own computer or digital device, are the best for enabling content access, community building, construction, and composition and, if implemented well, can also provide the most seamless technological solution.

Interactive Whiteboards

Interactive whiteboards are here to replace the old-fashioned blackboards. They can do everything that a computer can do—play videos, flash animations, presentations, etc. Apart from all the new stuff, they can still be written on with either a special marker or a finger—because they are touchscreens. This way, you can turn your classroom into a playground, where students can play games on the board, watch YouTube videos, and show the homework that they have previously submitted.

Student Response Systems

Teachers have access to wireless electronic student response systems. These devices can be used in the classroom to collect data from each student. Students feel more engaged, and teachers can assess students' learning immediately—with real data—to decide on how to proceed through a lesson. This approach is also more dynamic and inclusive of everyone in the room.

Digital Textbooks

Digital textbooks often accompany online materials to assist instruction, such as individualized diagnosis and intervention systems.

Mobile technology

Increasingly, laptops, tablets, and smartphones have entered K-12 classrooms, supplementing—and sometimes, replacing—traditional learning tools like blackboards and textbooks. At this point, almost all US schools use some non-desktop device to aid the learning process. Generally, educators agree that mobile devices in classrooms introduce new challenges and offer unique educational opportunities. According to a 2014 survey, 77 percent of teachers believe that mobile devices increase student engagement in learning. Mobile technology offers more accessible and faster search, total or partial processing and playback, and, of course, the ability to have audio-visual material in a project. Even more important is that most students believe mobile devices are important for learning and should be used the classroom regularly.

Internet is Transforming Standardized Testing

Schools have also begun to use the internet to transform standardized testing, replacing traditional paper and pencils. Across the US, schools are using online software like Pearson’s TestNav test delivery system to administer and manage testing on laptops, Chromebooks, and other mobile devices. Across the country, schools are embedding the internet into the learning process and seeing results.

Online Aid Tools and Applications

Teachers, parents, and students can use online aid tools and applications to do their research, and work in teams. It also allows for individualized learning and encourages students to seek out the content they like. Some examples are the following: Learn Boost, Moodle, Class Dojo, Cacoo, Pixton, Trello, and ReadWriteThink.

Document Cameras

Document cameras are designed to quickly display an object or document on a screen in the classroom using an LCD projector. The advantage of using document cameras instead of traditional overhead projectors is that a teacher can easily show the students important instructional images (maps, books, or art prints) without taking the time to make a transparency. Teachers can also show students three-dimensional objects such as coins, jewelry, or rocks.

Gamification

Over the last decade, video games designed to teach academic content have continuously increased. Students can learn about Newtonian physics from a game or prep for entry into the army. However, an emphasis on the instructional approach to gaming has overshadowed the constructionist approach, in which students learn by designing their games. Some research suggests that gamification can improve attendance, enhance understanding of content, encourage engagement, and improve academic performance if properly applied.

Audio Amplification Systems

Audio enhancement provides an optimal learning environment for all students, not just the hearing impaired. There is consistent research that supports the fact that this technology solution has a positive impact on student achievement.

New Form of HW

The homework nowadays is not just repeating what was done in class but actively acquiring new knowledge by researching the internet. Apart from the research, homework can have different submission procedures because not all homework must be brought into the class. On the other hand, homework can be e-mailed or uploaded to a cloud server.

Blended Learning

It is a term increasingly used to describe how e-learning combines with traditional classroom methods, creating a new hybrid teaching methodology. It represents a much greater change in basic technique than simply adding computers to classrooms; in many cases, it represents a fundamental change in how teachers and students approach the learning experience. It has already produced an offshoot—the flipped classroom—that has quickly become a distinct approach.

There is a consensus among education innovators that blended learning has three primary components:

- In-person classroom activities facilitated by a trained educator,
- Online learning materials, often including pre-recorded lectures given by the same instructor,
- Structured independent study time guided by the lecture material and skills developed during the classroom experience.

A course created in a blended learning model uses the classroom time for activities that require direct interaction. In a blended learning model, lectures can be videotaped ahead of time so students can watch on their own time.

Blended learning is redefining teaching roles. In some situations, the move to blended learning has inspired educators to redefine traditional roles. The word "*facilitator*" has emerged as an alternative to *"teacher",* bringing a slightly different focus. The facilitator emphasizes on empowering students with the skills and knowledge required to make the most out of the online content and individual study time, guiding students toward the most meaningful experience possible.

Cloud

The future of education is about the coordinated effort of accessing knowledge in any place and anytime. Educational institutions are expected to eliminate boundaries and accept online students who live across the world. Things are now beginning to move along these lines with the emergence of distance learning systems and *Massive Open Online Courses* (MOOCs). Mobile devices, like smartphones, and tablets, already in use, will also be an important part of the courses in the future. Several schools and universities use all these tools, but the number of educational institutions embracing digital media and online systems will increase. Nevertheless, the future does not revolve around a single device but rather centers on the cloud, which was predicted to have a significant influence on education at an early stage (Britland, 2013). For that reason, infrastructure is of great significance, with a fast Internet connection being among the prerequisites (Britland, 2013). If the system is moderate and systems are not working appropriately, students and academics will not have the motivation and desire to utilize the available devices. Educators may use the cloud to set, gather, and grade students' work on the web. Students can have access to evaluations and feedback through their mobile devices. The educational landscape has the potential to change as the classrooms and other aspects of the educational system are digitized (Britland, 2013). Furthermore, the focus will be on individual learning using shared information and several affordable (Mertzanos, 2013) cloud applications. It is also expected that over the years, the content transaction between students and teachers will become digital using cloud services to reduce paper abuse by adopting an eco-friendly policy.

Mobile Augmented Reality

Mobile Augmented Reality (AR) will probably be used in education. In some instances, the virtual world can replace the real world. Elements of the real world will be augmented through technological functions and interaction where this is feasible (Ahmad, 2015). This method could be used to implement virtual lectures for students.

3D Learning Tools

Although 3D technology has emerged since the early 90s, during the last two years, 3D technology has been greatly developed. 3D learning tools aim to change the passive activity of multi-faceted technology (GMI, 2014). As technology develops, education progressively emphasizes integrating soft skills, like creativity into students' abilities. Thus, 3D learning tools seem to be a popular solution. These tools focus on formal and informal learning in a unique manner for all levels of education. 3D learning is a particular technique because it shows how people view the real world. It is really beneficial especially for children (GMI, 2014). Visual learning enhances students' understanding because this realistic form of learning makes complicated theories more easily understood. Students can use 3D learning tools in a variety of ways. For example, in scientific and historical lessons, students can access 3D printing tools and interact with fossils and artifacts that would only be seen in museums. Also, chemistry students who study molecular chemistry can print out models of complex proteins and molecules, as seen in 3D Molecular Design's Model Gallery (GMI, 2014).

Internet of Things (IoT)

The Internet of Things (IoT) describes the network of physical objects— "things"— embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. Education is not yet among the most common IoT applications. However, as the Internet of Things platforms become more widespread and cheaper to adopt, campuses, schools, and other institutions are leveraging the technology's potential. From improving campus attendance to ensuring in-class productivity, IoT has dozens of promising applications in education, such as school management, real-time data collection, resource management, distance learning, AR-equipped systems, safety on premises, special education (for students with disabilities) and student health monitoring in the post-covid19 era.

14.1.3 Educational Software

Educational software can be used in learning processes. The teacher, knowing the learning theory that each software supports, will greatly facilitate both the choice of the most appropriate educational software and the most effective way of using it in class. The educational software used and proposed in the modern educational environment can be categorized, for instance, according to the role that the teacher, student, and software are invited to have during the teaching, according to the interface of each software with the student or according to how it is distributed (open source or not). More specifically, closed-type software can be practice and drill systems, guided teaching systems, multimedia thematic encyclopedias, guided teaching systems for preschool and first school age, presentation software, general-purpose applications, or educational games where the software code is not available for further development by the programmers' community. On the other hand, open-source software's code is set at the disposal of the programmers' community for further interventions. It can support hypermedia applications and programming, expression systems and Development of creativity for early ages, conceptual mapping systems and visualization or simulation and modeling environments. Based on the learning theory underlying the design of each digital tool, they are distinguished, initially in guided teaching (tutorials) and drill and practice software. Guided teaching substitutes the teacher's role, aiming to transfer knowledge to the student. The level of cognitive skills they serve is low (Grabowski, 2009). Practice and drill software allows the student to practice knowledge that has been acquired during teaching. Software for guided discovery and investigation support activities aims to cultivate high-level pupils' skills and allows students to engage in activities that favor student self-action, solving problematic situations, making decisions and cultivating critical thinking. The expression, communication, and creativity software can be freely modified by teachers and are created in the context of sociocultural theories and constructivism (Κόμης, 2004). Their use cultivates expression, linguistic communication, and students' creativity.

14.1.4 Applications of Artificial Intelligence in Education

One of the greatest steps technology has taken during the past few years is the development of *Artificial Intelligence* (AI). AI is the ability of computers to do tasks that humans commonly handle. AI is expected to reform the educational system completely as the years go by. The future of education is based on technological development and the benefits that intelligent machines will provide to humanity (Popenici & Kerr, 2017). According to Ron Sclmelzer (2019), the applications of AI that already serve the educational domain are:

- **Hyperpersonalization**: Intelligent machines enable students to tailor their educational profiles according to their needs and preferences to improve their performance in class and facilitate the educational process.
- **Voice assistants**: With voice assistants such as Amazon Alexa, Apple Siri, Google Home, etc., students gain access to additional educational material in a more interactive way that can transfer the "classroom experience" at home.
- **Assisting educators**: These machines aim to help teachers with tasks not associated with the educational process, such as evaluations, grading or extra tasks that schools assign.

All of the above have upgraded the educational process, solving daily issues that teachers had to deal with and helping students improve their skills with a more appealing way to learn. Teachers' challenge is incorporating AI technologies in their classes and schools (Strommen & Lincoln, 1992). Schools again need to be equipped with the essential tools to enable teachers to fully incorporate AI technology in class and make the educational experience easier and more interactive.

According to Sebastian Miller (2019), AI in educational systems can embody virtual reality, allowing students to use virtual reality and broadening teaching horizons. A great example of that is the virtual science lab. With its use, students can perform chemical experiments without the risk of using flammable materials in a screen's "safe" environment, offering an enjoyable experience for students.

It is also important to highlight the use of robots in the educational process since intelligent machines can assist the teacher's work and are, therefore, expected to introduce new applications of AI in schools. Robots can be ideal for kids with disabilities as well. The Nao robot has been designed mainly for this reason to help kids with autism get socially engaged improving their lives tremendously. Nonetheless, it is important to consider AI technology and its products as assisting tools for educators' jobs cannot replace them (Bigiti, 2018).

14.1.5 Examples of Digital Media Projects in Schools

14.1.5.1 Education Gamification Example – Mr Pai's Class: The Digitally Assisted Class

Sometimes, the best gamification examples are those that combine a multitude of fun technologies and solutions. Third-grade teacher Ananth Pai at the Parkview/Centerpoint Elementary School in White Bear Lake, MN, believes in the promise of games within education where students can learn more and learn faster at their learning level. He advocates interactive learning games that can be played individually, with other students in the class, or even students located in other cities, states, and nations. In Mr. Pai's class, several devices and media channels are used. Not just computers with local programs and game-based apps but also web-based and console-based (such as Nintendo) games. He has taken traditional education methods and provided a technological twist to create new, digitally assisted learning opportunities. As a result, this digitally assisted learning has produced increased class interest, improved math and reading scores, overall enthusiasm, and class engagement. The programs and games are often multi-subject based, such as the game Flower Power, which introduces basic concepts in economics and business as the students increase their math skills. Multiple goals, achievements, rewards, and positive feedback from fellow students are some of Mr. Pai's characteristics that make the class so engaging and fun. Enthusiastic responses from students, their parents, other teachers, and supportive companies and organizations have led to a school policy (school law) to enhance all classes with digitally assisted learning.

14.1.5.2 Australia

Some schools are breaking traditional boundaries by using smart devices to reinvent the classroom for students and teachers. Portable and multifunctional smart devices that students own for personal use are increasingly important learning tools in Australian classrooms in a *bring your own device* (BYOD) environment. For example, the 10th-year history students studying the Vietnam War at a school in Hobart collaborated on a project that included video interviews with veterans. They used their devices to record interviews and then created video clips, using mobile video applications. These were incorporated into a joint presentation that included still images from the period drawing on primary source documents. To consolidate and share their learning, their teacher arranged a web conference with a historian from the Australian War Memorial. The teacher recorded the web conference and made it available for students away from school on the day, to review from home.

Few argue that change and innovation, supported by enabling technologies, are the foundations of next-generation schools. Innovation has been imposed on schools for too long, often resulting in inertia and resistance. In a dynamic Web 2.0 world, innovation is driven by the experiences gained from learning and teaching.

14.1.5.3 The School of the Future in Philadelphia

The School of the Future in Philadelphia is unique as it is the first urban high school built in a working partnership with a leading software company, Microsoft. The school opened in September 2006 and serves approximately 750 students in a state-of-the-art, high-tech, and "green" facility. Microsoft's Partners in Learning initiative played an integral part in the design and conceptualization of the school, not through a monetary donation (The School of the Future is funded by the School District of Philadelphia) but through the development of new technologies for teaching and administrative purposes. Among the most innovative and controversial technologies is a smart card that allows access to digital lockers and tracks calories consumed during school meals (breakfast and dinner are also served before and after school). Class 50 Appendix schedules and locations change daily (the goal is to break down our culture's dependence on time and place), and all rooms are designed with flexible floor plans to foster teamwork and project-based learning. Instead of a library and textbooks, all students are given a laptop with wireless access to the Interactive Learning Center, the school's hub for interactive educational material. These laptops are networked and linked to SMART Boards in every classroom so that assignments and notes can be accessed from home. The building itself is also unique in its holistic approach. Rainwater is caught and repurposed for use in toilets, the roof is covered with vegetation to shield it from ultraviolet rays, panels embedded within the windows capture light and transform it into energy while room settings auto-adjust based on natural lighting. In short, the School of the Future incorporates many innovations but has high-tech interactivity that borders on extreme surveillance, making it a questionable model for future participatory learning initiatives.

14.2 The Impact of Social Media on Education

Social Media Technology (SMT) permits social interaction and lies on web-based or mobile applications that help people absorb and spread information through multiway communication. Traditionally, SMT entails virtual social spaces supporting interaction, highlighting the transition from face-to-face to platform engagement. These include Facebook, YouTube, or Blogger and does not include any educational learning or content management. They are solely developed and used for user-generated content and sharing of exchanges and interactions, not particular learning purposes. Thereby, there is a difference between social media and educational learning platforms like Blackboard or WebCT (Davis et al., 2015). However, the increasing use of social media has a vital influence on the educational sector, where students use social media for several purposes. In general, SMT makes young people more peer based. They interact with friends, strangers, and idols and receive feedback from others about their posts. As a result, they are more inclined to learn from their peers than their teachers or parents. Therefore, social media can be seen as open and bottom-up. Every day, almost all students spend some time on social networking sites. Mostly, they use technology up to eight hours a day. No matter if they use it for study or entertainment purposes, social media has been shown to have positive and negative impacts on the educational level of students (Raut & Patil, 2016). Overall, the positive impacts of SMT are comprehending human behavior and enhancing social intelligence through communication. Global adverse effects of SMT are the addiction to being online and in contact, as well as the distraction most people have from real life. However, the problem does not only come from social media platforms, but rather from people's lack of understanding and analysis of their online actions and how they impact their personal lives and society in general. With this, both personal development and destruction come with social media (Klient Solutech, 2019). Many studies have tried to analyze the effect of the upsides and downsides of social media, especially for Students in the Educational System, and have come up with multiple conclusions.

Social media is on the rise in incorporating higher classroom learning with educational apps to enhance communication and learning. Studies have found that compared to traditional learning, using social media provides some control for learning in the students' hands. This independence, as well as the purpose of

collaborative study and social interaction, is more attractive to students and has been found to increase their learning process (Al-Deen & Hendricks, 2011). The use of social media has shown the ability to increase happiness, self-esteem and success via the possibilities of communication among peers and students. Someone can be integrated into the school system through social media and talk about sophisticated themes if needed, as well as find a closer feeling of belonging and identity, which affects the overall ability to feel included in the school (Davis et al., 2015). Also, studies have found multiple other positive impacts of social media on students, for example, the speed and ease of access to information, as platforms like Facebook or X provide news on politics, science, and many more. Further, the possibility of building technical skills is increased by establishing blogs or profiles on any social media platform with easy instructions. In conclusion, social media platforms have made it easier for talented individuals to gain recognition through sharing and liking, while also providing students with feedback from their peers that can lead to opportunities for success (Raut & Paril, 2016). In education, the use of social media has the potential to facilitate communication, collaboration, knowledge gathering, and have positive effects on cognitive, emotional, and social well-being.

Nevertheless, the negative impacts of social media have been seen as profound by most researchers, and all conclude the downside SMT brings to the educational system. In their eyes, social media presents a massive distraction to students, leading to poor performance and academic decline (Raut & Patil, 2016). First of all, the attention span decreases with multitasking in class. Most students use social media like Facebook and focus on their laptops or their smartphones instead of attending the class. Students believe they can listen to the class and check the newest posts on Facebook at the same time, which is impossible. Studies have shown that one must focus on one source of information. This results in poor performance which includes slower content comprehension and a delay in reaction, as the focus is on the information provided by the social media platform rather than the class. Ultimately, this may have a negative effect on learning results (Al-Deen & Hendricks, 2011). Other problems include that students mostly use several SMTs at once but potentially miss out on critical social media platforms like LinkedIn, where potential employers and future success lie. Further, it was found to be difficult for students to draw a line between their professional and private lives in their social media files. They repeatedly post comments or pictures that employers might see as inappropriate. This behavior suggests that students do not seem to know the range of people viewing their profiles, especially employers. Research has proved that students are aware of the accessibility of their profiles to employers and that they feel uncomfortable about it.

However, it appears that individuals lack awareness regarding the potential repercussions of undergoing employment screening and fail to recognize its significance. Additionally, they exhibit a sense of ambiguity regarding the appropriate information to disclose to specific individuals. Much personal information is shared that could be held against people when in the wrong hands. Studies have determined that either a lack of awareness regarding making profiles private prevails or individuals do not even consider it. Insufficient educational resources are also evident, as students typically must depend on their personal experiences or the knowledge of their peers to gain understanding in this area (Al-Deen & Hendricks, 2011). Further, studies have shown that students are more driven to learn from their peers than they are to learn from their teachers or parents. Hence, teachers and parents are not the only ones with wisdom, and social media is seen as more trustworthy and exciting (Raut &Patil, 2016). Moreover, knowledge and action are mostly not in line for students in terms of social media. Almost everyone knows how to switch their profiles to private, but many students are willing to accept random people on their friend lists or do not privatize their profiles (for example Instagram). With this, students may easily allow the wrong people to follow (Al-Deen & Hendricks, 2011). Finally, Junco, Heibergert, and Loken (2010) have found that only specific behavior on SMT is causing the decrease in grades and level of college engagement. For example, sharing and collecting information, instead of socializing, predicts a high-grade point average (GPA). Further, a high amount of time spent on Facebook negatively forecasts the *grade point average* (GPA) but does not correlate with the amount of time spent

studying; it rather proposes that other behaviors may predict high Facebook use and low GPA (Davis et al., 2015; Junco et al., 2010). With this finding, Kuh (2009) challenged the view that SMT threatens students' engagement in school and academic performance. Instead, he urges understanding how online and offline activities can reinforce school performance, so that social media and studying can coexist (Kuh, 2009).

Many researchers have analyzed SMT's impact on education, but few solutions have been provided. The research of Greenhow and Lewin (2016) has concluded that there has always been a debate about the challenges and benefits of SMT, where the necessity of a model might theorize social media in terms of formal and informal learning. With this concept, they try to conceptualize the ambiguity of using social media and search for a solution for the educational system. Grennhow and Lewin believe that technology, in general, can disarray the boundaries between those two sites where learning takes place. They have worked on two theoretical models to assemble strategic possibilities and proven remarkable results. First, they implemented *Innovative Technologies for an Engaging Classroom* (iTEC) in about 20 schools. Teachers were mediators and were supposed to help their students (ages 7-14) implement learning via social media. The program incorporated blogs and wikis, search engines, social bookmarking tools, other collaborative tools or apps, and video-sharing websites, like YouTube, into their curriculum. The results have shown that social media was used for sharing ideas, communicating with peers and teachers, managing group work, and posting assessments and evaluations of peers and teachers. Reflection through social media has taught students the skills of metacognition and self-evaluation, and the likelihood of sharing knowledge and ideas has increased steadily. With their mediation, teachers have noticed that social media has enabled better teacher-student communication with possibilities of tutoring and feedback. This program showed the options of formal learning, where the teachers used social media as a tool for communication and education, and where they improved the impact of SMT for students by teaching them how to use the platforms. Nevertheless, teachers had to authorize the learning and have a firm hand over what to do and how to learn via social media. When provided with increased independence, students began to create and structure their own educational tasks, which encompassed both individually determined and collectively influenced activities within the entire class. Also, some students continued using platforms like Facebook for non-school activities, even during the courses when given the freedom to use SMT. This behavior also continued outside school, where students kept using the program, as intentional, educational, and purely social. In the end, the importance of authority and guidance of the teacher was highlighted, as they led the students into the possibilities of formal learning with SMT (Greenhow & Lewin, 2016). Secondly, the Facebook application Hot Dish was tested as a form of informal learning for students (age 16-25) outside school. The app is about the sharing and engagement of environmental science issues, like climate change. Students share stories or articles of their interest with the community and vote and comment on others' posts. With this, Hot Dish combined the possibility of social networking and spreading knowledge. Here, young people were inclined to collaborate with like-minded people, where the form of learning was self-directed and unintentional. They chose what to read and how long they wanted to use the app. Further, their knowledge was also spread to other peers or followers, and the likelihood of "speaking" and "persuading" others to join has led to a possibility for a greater community. In the end, the site' team provided feedback and rewarded people for their work of commenting and sharing, to ensure the attractiveness and realness of the system. Therefore, Hot Dish promoted learning without the constraint of formal learning.

The two studies show two different opportunities for student social media use. The researchers conclude that the level of control and surveillance are essential for social media use in students. Students need self-determination and control over features like direction, audience, and assessment to learn. Nevertheless, it may be necessary for schools to possess some form of authority in order to effectively navigate the realm of SMT. As a result, the distinction between formal and informal learning becomes increasingly indistinct (Greenhow & Lewin, 2016).

As seen above, social media causes several social, emotional, and cognitive results regarding education. Concluding, studies have shown the positive and negative sides of social media in Education and tried to develop solutions for educational purposes. Both the upsides and downsides of SMT have to be included in the theme of student education. Social media is a great place for communication and spreading knowledge, but the right way to use it seems lacking for most students. Missing expertise or the desire to implement that knowledge into their education is what brings social media into the negative side of technology. Only a few studies were able to come up with solutions or implementation for this negative impact of social media on students' education. Recently, Greenhow and Lewin tried to integrate formal and informal learning into the effects of SMT on education. Their argument for the need for a theoretical model leads to novel ideas and investments into the issues of social media, where they state two possible solutions. iTEC and Hot Dish learning devices have shown excellent results and highlighted the importance of formal and informal learning in the educational system. Here, the importance of a mediator for students in terms of learning about social media and studying, as well as the importance of self-directed and exploratory learning with social media are irreplaceable in the subject. This is also in line with other studies that approve the need for older peers to show how to act on social media while exploring on their own. Klient Solutech also concluded that it does not matter whether it is social media, the internet, or artificial intelligence, as the only thing that matters is the knowledge that must be adequately used with all devices. Therefore, education and regulation for the content are needed to ensure the correct use of any technology, especially social media. In the end, SMT has exclusive and impressive features providing a participatory commitment to ineffective, multimodal learning communities. Much more research is therefore needed to ensure more sustainability and focus on the work of more theoretical models that highlight the need for learning communities.

14.3 Smart Phone Implications

14.3.1 Children/Adolescents and Cell Phones

Owning a smartphone is often considered a cause of social and educational problems for children and adolescents (Wright, 2018). It is attributed to a set of behavioral and cognitive disorders. The smartphone itself is not considered to be an addictive product like tobacco, alcohol, cannabis, etc. Indeed, neither OFDT (French Organization about Drug and Addiction) nor WHO (World Health Organization) have included smartphones in their list of addictive products. Reports define the dependence on a substance as "a set of cognitive, behavioral and physiological symptoms, indicating that the subject continues to use the substance despite its significant problems." The biological circuits activated by smartphone use seem not to be the same as those activated by a substance in terms of pleasure. Using a smartphone tends to satisfy needs such as being constantly online and part of a group or social network that allows for connection with friends integrating the user into a system of virtual relationships. The pleasure associated with smartphones mainly derives from this role, with content consumption being the second most pleasing process. For these processes, the new generation prefers smartphones more and more than desktop computers because of their easy, quick, and portable usage (**Figure 14.1**).

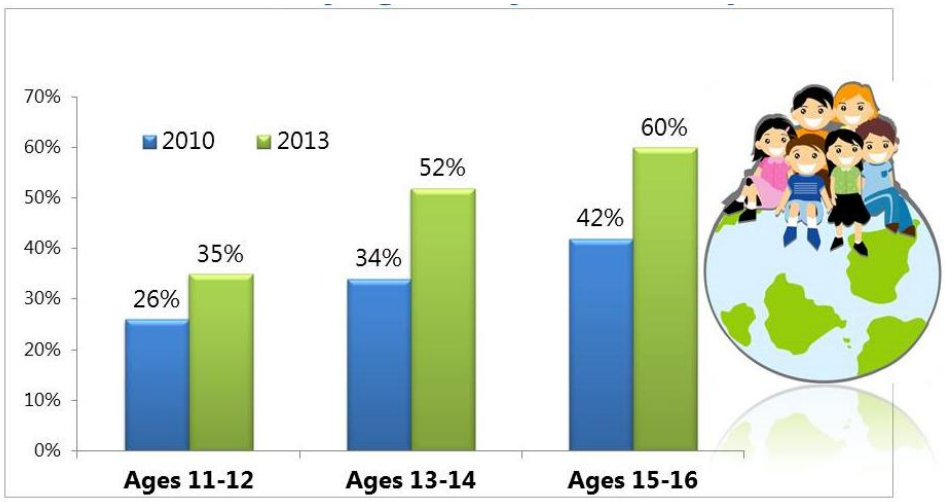


Figure 14.1 *Percentage of those who use cell phones to surf the internet by age and year in Europe (Stald, 2014).*

Some decades ago, parents had to face and control how much time children spent in front of TV screens and what they attended. This problem has now evolved into setting limits on how children use smartphones. Moreover, the age at which children start using mobile devices is decreasing. According to research by the University of Sheffield (2015), one third of children under five own tablets. According to a report from Common Sense Media, 53% of US kids own their own cell phones by the age of 11.

Parents worry about the appropriate age for kids to obtain a cell phone. There is no right answer to this question. Many opinions and surveys try to answer, but a clear answer is yet to be given. Ongoing surveys consistently challenge previous findings. Certain studies advocate for children having a cell phone once they reach an age where they are left unsupervised or venture out alone, as it can enhance their safety. Conversely, others argue that children should be introduced to smartphones at an early stage to develop proficiency in internet usage, applications, and conveniently access educational materials. Less enthusiasts think that smartphones provoke health problems, so it is better for kids to obtain one as late as possible.

A report that was published in 2016 at Frontiers Psychiatry suggested a set of criteria that show if a young person is addicted to a cell phone, among which are:

- Young people anxiety,
- reduction of sleeping time,
- need to reply immediately to messages,
- being connected on social media all the time,
- argue a lot with family and friends,
- becoming aggressive and alienated.

Some health consequences related to the use of cell phones that are affecting even young users, are presented below.

Hearing Issues

The auditory system consists of sensory cells that can be destroyed due to intense noise exposure. Passive or permanent whistling and buzzing in the ear, called tinnitus, are becoming more and more frequent due to overexposure to high levels of music sounds (above 80 dB). Hyperacusis can also be associated with intense content consumption using earphones connected to a smartphone. These hearing disorders are, in many cases, irreversible.

Carpal Tunnel Syndrome

Trauma specialist Antonio Galvan, a specialist in hand microsurgery working in Quiron hospitals in Tenerife, Spain, argued that using a smartphone too often makes the base of the thumb ignite while it is also common for the median nerve of the wrist to compress, causing carpal tunnel syndrome.

Sleep Disorders

Smartphones have proved to have the power to invade the personal sphere by disrupting life habits and particularly sleep. Indeed, this is the statement by the National Institute of Sleep and Vigilance (INVS) made in its 2016 study. The use of new technologies and screens in the evening is usual. 8 out of 10 adolescents use their tablet or smartphone in the evening after dinner, and almost 4 in 10 use them in bed. In addition, 40% of young people sleep with a phone on standby. Half of them are regularly awakened by a message in the middle of the night. In more than 90% of cases, teens consult their messages, and 79% answer them on the spot. More than half of people who use their tablet or Smartphone at night in their bed are between 18 and 34 years old.

Whether natural or artificial, light plays a vital role in the biological clock and synchronizes vital human functions. For example, body temperature, blood pressure, alertness, cognitive performance, etc., are at their maximum during the day. On the contrary, muscle relaxation, sleep pressure, and the secretion of melatonin (a sleep hormone) are at their highest level in the evening. However, if the sleeper is unconsciously waiting for communication, the slightest light signal the screen delivers will disturb him. "*Bright flashes a few milliseconds at night can delay the biological clock and the system is so sensitive that the light acts even if you sleep, eyes closed!*", says Dr. Claude Gronfier, neurobiologist. Indeed, even at low light intensity, the circadian system is impacted. The LED screen's blue light is the most active on the circadian system.

The "Text Neck" Syndrome

The number of addicted to texting continues to increase. According to the IRBMS (Regional Institute for the Well-being of Medicine and Health Sport in Nord Pas de Calais, France), "*more than 20% of mobile phone users report spending 2 to 4 hours a day sending messages.*" This trend is not without consequences for the health of young people. The "*text neck,*" an expression from Great Britain, is the proof.

The "*Text-neck syndrome*" is neck pain due to wrong head positions when using smartphones and texting. Its definition has since been extended to cervical pain related to the use of digital tablets and other computer screens. In fact, most of the time, the screen used is not positioned at eye level. This results in lowering the head towards the screen with the chin facing the chest and the neck flexing.

In the long run, the wrong neck position can cause tension or muscle contractures and cervical vertebral movements. The head of a human, weighs on average, between 4.5 and 5.5 kg; neither the neck nor the shoulders are adapted to support this weight for long periods. However, wrong neck positioning is not the only cause of the "Text Neck" syndrome. The positioning of the arms, elbows, hands, and fingers also counts.

When writing a text message or checking emails, the face is tense and the eyes are crisp. The muscles of the face and eyeballs are connected directly to the vault of the skull and the cervical. Therefore, facial contractions repeated several times a day can cause headaches, feelings of compression in the skull, chronic migraines, sleep disorders, vertigo, or even eye disorders in some cases.

14.3.2 Effects of Cell Phones' Use in Classrooms

The average college student uses a cell phone for 8-10 hours per day. The reason for this use is for texting, connecting on social media, browsing the web, taking photos, listening to music, watching movies, shopping

online, and generally accessing everything a young person wants. The problem is that these activities now happen in a class as more than 95% use their device during lessons.

According to a recent survey, around 94% of students would like to use their cell phones during class for academic purposes. Many of them support the idea that using cell phones helps them update their skills in learning and retaining information (Wesolowski, 2018). They use them to take pictures of the slides, to access textbooks, search on the web and answer to questions held in the classroom. The majority would prefer more digital material in classes as they believe this makes learning more interesting and easier. For example, they prefer digital interactive material, videos, and interactive texts as academic content to obsolete methods already used for years. As stated earlier in this chapter, an increasing number of schools around the world accept the use of cell phones in classes, and many of them find ways to adapt them in the educational procedure. Students can use their devices to download helpful applications such as dictionaries or access school platforms to compete through educational trivia. According to some surveys, in circumstances where active learning took place, students improved during exams by around 6%, and students who attend traditional lectures were 1.5% more likely to fail exams than those with a significant active learning procedure. A professor of Chemistry at Duke University decided to run an experiment and combine both active learning and traditional lectures to determine what the impact of this new method. Of course, the results can be measured not only by exam scores but also by the possible new skills that students may develop if they are more active in the classroom. In Finland, schools have using handwriting in lessons in 2016 and followed the US plan to teach students to touch type as they believe this skill is more useful in the modern world. Moreover, in the Netherlands, in the so-called Steve Jobs schools, books, blackboards, and notebooks have been replaced with iPads, and students get into workshops in different subjects through these devices. Students could join the workshop whenever they wanted and not only during school, so they had immediate access to knowledge the whole day. Additionally, every student has his learning plan, designed by the teacher and parents and of course by the student. In this way, every child can develop skills and obtain knowledge in various fields depending on their personality, interests, and talents. Students are often more interested in learning through these portable devices.

On the other hand, using cell phones can sometimes be harmful. Isolated or unhappy children can easily play games or use attractive applications without trying to improve their social skills or communicate with others. This can easily occur during breaks. Another important problem that has been stated above is cyberbullying, which is born in the school environment and can be supported by smartphones inside or outside schools. In 2017, 1 out of 5 young people declared that they had experienced cyberbullying (Culpepper, 2017). According to research from the American Academy of Pediatrics, children that own a cell phone are more possible to be cyberbullied in the academic environment. Sexual harassment also takes place through these devices during school time. The American Academy of Paediatrics, found that 20% of students who own a cell phone have encountered *sexting,* which is sexually explicit messages.

Finally, distraction is also important. According to research published by the London School of Economics (LSE), students at schools where cell phones were banned had higher exam scores. According to another research published by the University of Chicago, students may have low learning and test performance when cell phones are in the classroom and not in use. It is well-known that there are rules at schools, but this does not mean that they do not get broken by students. Teachers cannot always find out if students use their phones during class or if they use them in a way other than the one, they have been instructed. Students can easily play a game on their cell phones or text each other and socialize in classrooms, which is usually inappropriate.

14.4 Online Gaming

Nowadays, online games constitute a great amount of the total free time young people or even adults devote to themselves in their everyday lives. Although online games have existed since 1972, living in the 21st century of technology and information, online games, especially multiplayer ones are rising, and their resonance is constantly growing, regardless of gender or age.

14.4.1 History of Online Games: From Plato to the 21st Century

Before we went "online," many video or computer games existed. Among them were *NIMROD* (1951), *OXO* (1952), and, of course *Spacewar!* (1962), games that demanded one computer only to operate for one or two users simultaneously. Later, in 1970, the *PLATO* time-sharing system, created by the University of Illinois and Control Data Corporation, allowed users to connect at different locations and do online lessons, which, of course, gave them the idea to create multiplayer online games such *as Empire*, *Spasim,* and *Airflight*. Later, computer networking systems like ARPANET and JANET allowed computers to be connected and attached to one "head" computer (known as host or terminal). Users could use programs on other computers and play games in several locations. The development of systems like these continued to grow bigger with the examples of *TYMNET* (1971), *CYCLADES* (1973), *TELENET* (1974), and *USENET* (1980). Online games started to go global in 1991, with the passing of the World Wide Web (www). From that year on, but mostly in the late 1990s, online gaming and especially MMORPGs (Massively Multiplayer Online Role-Playing Games), on which I will mostly rely and focus, were met with an explosive rise and resonance having as representatives *Lineage* (1998), *EverQuest* (1999) and *Ultima Online* (1997). As reaching modern gaming history with the introduction of consoles (Playstation, Xbox, etc.) and the rapid development of online gaming, gamers started being somehow attached to the play itself and have shown signs of bonding with other users or even their game character (e.g., avatar). The paragraphs below will be presented how bonds are created within the communities, the effect they have on the gamer, and how gamers react in and out of the game after being influenced by their "in-game" life.

14.4.2 Gamers' Behavior and Social Interaction In and Out of MMORPGs

Massively Multiplayer Online Role-Playing Games (MMORPGs) are highly developed universes in which gamers create their character, displayed in high-definition visuals, figures, and audio. In these universes, users can create their individualistic character and voluntarily immerse themselves in a graphical virtual environment and interact with each other daily (Yee, 2007). Environments are physically, socially and psychologically healthy, so the real concern lies in the gamers and how they feel about their avatar or react after some game outcomes, maybe winning or losing.

Starting upon this topic and to further and in depth understand the ways of interaction among gamers, it would be really helpful to look at the motives that push them to choose an MMORPG or any of its subgroups. While examining online gameplay, Bekhtina subsequently identified four basic motivations for playing:

- curiosity, astonishment, and interest,
- cognitive stimulation,
- enjoyment of a different lifestyle in virtual environments,
- recreational refreshment.

Yee (2007) identified three broad motivations for online play: achievement, social, and immersion (**Table 14.1**). Each broad motivation is subdivided into specific subcomponents shown in the table below:

Table 14.1 *Primary motivations for play in MMORPG environments and their subcomponents as identified by Yee (2007).*

Achievement	Social	Immersion
Advancement Progress, Power, Accumulation, Status	**Socializing** Casual Chat, Helping Others, Making Friends	**Discovery** Exploration, Lore, Finding Hidden Things
Mechanics Numbers, Optimization, Templating, Analysis	**Relationship** Personal, Self-Disclosure, Finding and Giving Support	**Role-Playing** Story-Line, Character History, Roles, Fantasy
Competition Challenging Others, Provocation, Domination	**Teamwork** Collaboration, Groups, Group Achievements	**Customization** Appearances, Accessories, Style, Color Schemes
		Escapism Relax, Escape from offline world, Avoid offline problems

As Rachel Kowert states in "*Video Games and Social Competence,*" "there are two ways which OVG (Online Video Games) play may be associated with social competence. The first is that engaging in OVG play offsets social development because players spend less time socially interacting in offline contexts than non-players. This is known as the social displacement hypothesis, which assumes that online and offline social interactions are zero-sum. That is, there is a substantial trade-off between online and offline friendships, relationships, and interactions, and that offline interactions are more "socially valuable" than online ones in terms of promoting the development and maintenance of social skills (Cole & Griffiths, 2007; Hussain & Griffiths, 2009; Lo et al., 2005; Morahan-Martin & Schumacher, 2003; Shen & Williams, 2010). From this perspective, online gaming does not directly cause social deficits, but rather, social deficits are an indirect consequence of play caused by the displacement of offline social interaction. In this sense, the potential negative social impact of OVG play would be no different from the effects of other activities that "displace" offline interactions, such as online gambling or offline gaming. However, a sub-type of the displacement hypothesis argues that gaming does directly affect social competence by influencing cognitive development. For example, Sigman (2009) has hypothesized that a task of "real" social networking (i.e., socialization that involves face-to-face interaction) may alter the way genes work and negatively influence mental performance. However, the research in this area remains largely exploratory.

Approaching the second way it is referred: "*The other way OVG may be associated with social competence is if people with lower levels of social resources (e.g. poor social skills, greater social anxiety, lower quality or quantity of offline friendship circles, etc.) are drawn to this activity. This is referred to as the social compensation hypothesis. From this perspective, online gaming spaces hold particular qualities (e.g. visual anonymity, few non-verbal cues, etc.) attractive to individuals lacking in social competence or social opportunity.*" Now, trying to clarify and end up to a point she summarizes: "*Again, there is no sense in which playing games is directly detrimental to social competence. While displacement effects could exacerbate the pre-existing disposition (e.g., lead to increased loneliness, depression, and social anxiety), a certain degree of social inadequacy is believed to pre-exist among those who are motivated to engage within online gaming spaces.*"

14.4.3 Negative Outcomes

As analyzed above, online gaming itself cannot alone create negative behavior in the community. However, it depends on the individual player's predisposition, and may can create negative results on a character's pre-existing features, boosting them up. Some incidents which occupied the news report and maybe got gamers stereotyped from then on. Rachel Kowert refers to incidents such as "*Addicted: Suicide over EverQuest*" (Kohn, 2002), "*Chinese man drops dead after 3-day gaming binge*" (Associated Press, 2007) or "*Chinese gamer sentenced to life*" (BBC News, 2005). Upon the dangers and the rising social concerns, the author of *Video Games and Social Competence* states: "*Current empirical evidence confirms that online gamers are perceived as incompetent and undesirable, with a stereotype centering the themes of unpopularity, unattractiveness, idleness and social incompetence. Online games are perceived as being competitive, addicted loners who are obsessive, socially inept, isolated, immature, and young. The image of an individual playing alone and for long periods of time seems to be at the heart of this representation, as multiple traits refer to the idea of being engrossed in the activity (addicted, obsessive) and doing so without the company of others (loner, isolated). The addition of the quality of social ineptness hints at the inability of online gamers to interact with others, even if desired. These representations are also largely limited to online players, as individuals who engage in offline gaming environments are perceived differently. In a recent study investigating the stereotypical perceptions of various gaming groups (e.g., online, arcade, MMORPG, console), console gamers were perceived as skillful and fun loving, emerging with a significantly less negative stereotypical profile than online gamers and their subgroups.*" However, online gaming universes and communities constitute a shelter for more insecure personalities with signs of offline social incompetence, which can lead to social alienation.

Although they may develop in-game socializing skills, they lack yet real, face-to-face interaction development. When examining the relationship between online game addiction and a variety of psychological characteristics, Kim et al. (2008) uncovered a significant negative correlation between online game addiction scores and offline social relationship scores, suggesting that more involved online video game players experience social difficulties and stress in offline interpersonal relationships. Addiction to online gaming can lead to psychosocial dispositions, loneliness, depression, social anxiety, and even a lack of social skills.

14.4.4 Positive Effects

Online video games, however, have some positive social effects among players, regardless of their pre-existing social competence. Patricia Marks Greenfield argues that habitual playing of this type of game results in the development of new cognitive abilities that translate into key skills (Facer, 2003):

- The ability to process information very quickly,
- The ability to determine what is and is not of relevance to them,
- The ability to process information in parallel, at the same time, and from a range of different sources,
- Familiarity with exploring information in a non-linear fashion,
- A tendency to access information in the first instance through imagery and then use text to clarify, expand, and explore,
- Familiarity with non-geographically bounded networks of communication,
- A relaxed approach to "play"—the capacity to experiment with one's surroundings as a form of problem solving.

Rachel Kowert states in her book: "*Like other computer-mediated social spaces, such as chat rooms, online video games are social environments where friendships often develop. One's co-players can be more than just individuals who help achieve in-game instrumental goals; they can be close, trusted friends, and valued sources*

of offline advice" (Pena & Hancock, 2006; Williams, 2006; Yee, 2006). Cole and Griffiths (2007) found that up to 75% of online game players report making "good friends" within their gaming communities, and, of these, between 40% (Cole & Griffiths, 2007) and 70% (Williams, Ducheneaut, Xiong, Yee & Nickell, 2006) report regularly discussing "offline" issues online, including concerns that they have not discussed with pre-existing, offline social contacts. In this sense, online video games converge with other Internet-based social outlets, such as chat rooms or newsgroups, where the development of acquaintances, friendships, and romantic relationships as a result of involvement has been well-documented (Katz & Aspden, 1998; Parks & Floyd, 1996; Peris et al., 2004; Ridings & Gefen, 2004). However, unlike these spaces, online video games are also environments characterized by play. She also points out that "*in some ways, all video games are similar as they are playful, interactive mediums that require the user to actively engage in order to progress through the content. Online video games share the additional feature that they incorporate multi-player play over a networked Internet connection*". From this point of view, online game environments provide gamers with the ability to have fun and be entertained at the same time while enjoying the comfort of anonymity and freedom from stereotypes. However, some researchers consider that the absence of social cues found online may be beneficial by providing a level of social accommodation not found in traditional interpersonal interactions. For instance, the lack of non-verbal cues can promote dissociative anonymity and invisibility. Together, this generates a unique combination of trust and anonymity, often referred to as the Online Disinhibition Effect (Suler, 2004), which can stimulate open and intimate conversations as it removes the fear of any social repercussions (Morahan-Martin & Schumacher, 2003; Suler, 2004; Walther, 1996). Consequently, individuals become inclined to self-disclose at a quicker rate than is found in non-visually anonymous relationships (Joinson, 2001; McKenna & Bargh, 2000; Parks & Floyd, 1996; Parks & Roberts, 1998; Suler, 2004) and to be more honest and open" (Whitty & Gavin, 2001).

In conclusion, we can see that even though online gaming can be addictive and may isolate gamers from offline socialization, it can help different personality types (e.g., introverts, with insecurity issues) socialize through the game through a process of having fun and play.

14.4.5 South Korea's Example

As the online gaming industry has risen and developed in the past 20 years, South Korea has rapidly grown and dominated the global market. Although the country came late to the revolution of Internet and broadband services, South Koreans soon realized the significance of online gaming and its development, leading to the top of the list. Competing with the West, South Korea developed impressive progress in online gaming software and soon became the head of the sector, pointing to a 56% increase in the sales of domestic online games through the years 2007 to 2009 from $2.24 billion to $3.49. In 2006, the global online game market was valued at $4.98 billion, with Korea being the largest and most viable market in the world (PricewaterhouseCoopers, 2007), which continues to the present.

Regarding the social part of this internet gaming revolution, Dal Yong Jin states in his book that "*Playing online games involves active socializing and intertwined relationships; this is why the current generation is called the game generation*" and makes a reference to Ryu (2008) reporting that "Gaming has moved beyond being merely a leisure activity—it is a social and cultural phenomenon." At this point, and trying to see the whole picture, South Koreans not only developed the game industry but also accepted the gaming habit so much that gaming, especially online passed to the level of creating a whole new culture. South Koreans no longer focus on the play but also on the general development of the game itself and its other features.

14.4.6 Gaming for Society

14.4.6.1 PewDiePie

The most prominent YouTube personality with 33,000 subscribers was once Felix Arvid Ulf Kjellberg, better known by his pseudonym "*PewDiePie.*" PewDiePie is a Swedish gaming commentator on YouTube and has organized four charity campaigns in the last three years. He has expressed in interviews that he is really into using his popularity to be involved in fundraising drives.

In February 2012, PewDiePie, while only having 200.000 subscribers, took part in an online contest named "*King of the Web*" but lost the overall title. However, he won the title "*Gaming King of the Web*". He donated all his winnings to the World Wildlife Fund (WWF), an international non-governmental organization that works on issues regarding environmental conservation, research, and restoration. It is the largest conservation organization in the world.

Some months later, in August 2012, being at 1,600,000 subscribers, PewDiePie ran a second charity campaign, this time for St. Jude Children's Research Hospital, which is a hospital with the mission of advancing cures, and means of prevention, for pediatric catastrophic diseases through research and treatment.

In July 2013, PewDiePie organized his third charity campaign, a "water campaign" charity, where his subscribers and fans could donate to *Charity:Water,* an organization that brings clean drinking water to people in developing countries. What needs to be highlighted is that his starting goal was 250,000 dollars but eventually 462,466 dollars was achieved. He also donated 10,000 dollars himself.

His last and most recent charity fundraiser was towards *Save The Children* in June 2014, which ended up with 630,000 dollars, stomping his initial goal of 250,000 dollars. This time, PewDiePie donated 25.000 dollars due to hitting 25.000.000 subscribers on YouTube, which was why this campaign was started.

Overall, Felix Arvid Ulf Kjellberg—PewDiePie has funded over 1,000,000 dollars for charity and is a very important personality in the charity area. The important thing about PewDiePie is that his charity actions show that this world needs more people who use their fame towards a good cause rather than using it only to promote their image and increase their bank balance.

14.4.6.2 The AbleGamers

The *AbleGamers* Foundation is a nonprofit charity organization that empowers children, adults, and veterans with disabilities through the power of video games. AbleGamers is the largest community for gamers with disabilities found anywhere in the world. It was founded in 2004 by Mark Barlet and Stephanie Walker to help people with disabilities to keep playing games for rehabilitation. AbleGamers became an IRS recognized charity in 2009.

There are 33,000.000 million people with disabilities around the world who play video games. The AbleGamers' goal is to make video games more accessible to such people, enabling them to break the perception barrier about their physical challenges. They have been fundraising since day one and continue to do so. They raised over 240,000 dollars in 2014. They basically try to provide a greater quality of life for people with disabilities through video games. They run the "*Grant Program,*" which purchases assistive technology for people with disabilities when their families cannot afford it, and insurance companies refuse to help.

Gaming is becoming a part of everyday lives and can be used as a means to crush social discrimination in all its forms. The AbleGamers aim to bring people together to surpass any physical disability obstacle that exists. And this is the social message they are trying to convey: that all people are equal and should not be discriminated against for being disabled and that there should be no barrier to fun.

14.4.6.3 Humble Bundle

The *Humble Bundles*, previously known as *Humble Indie Bundles,* are a series of bundles of video games and digital creations that are distributed online and sold at a price determined by the purchaser. It was formed in 2010 in San Francisco, California, and its motto is "pay what you want." Early bundles featured independently developed multiplatform games with no digital rights management. Recent bundles feature games from established developers and bundles consisting of big titles from major publishers. The bundle sales are split between the developers/creators of the games, the Humble Bundle operators, and many charities, including *Child's Play*, the *Electronic Frontier Foundation*, *Charity: Water,* and The *Red American Cross*.

Several of the bundles have brought in more than 1,000,000 dollars. As of August 2013, the bundles had earned over 50 million dollars, 20 million of which went to charity. By the end of 2014, the total amount funded for charities was over 50 million dollars going out to more than 50 charity organizations, while participating developers grossed more than 100 million dollars.

The Humble Bundle is also supporting another charity group by the name of *GamesDoneQuick*. GDQ is a bi-annual charity gaming marathon. Volunteers play games at incredible speed, also known as "speedrunning." The games are streamed online non-stop, and all donations go directly to charity. GamesDoneQuick hosts various charity events, one of the latest being for *Prevent Cancer Foundation,* a nonprofit organization formed in 1985 that has invested millions of dollars in cancer prevention research, education, and advocacy. GDQ has raised 227 thousand dollars for the *Prevent Cancer Foundation* and continues going on *twitch.tv/GamesDoneQuick*.

14.5 Social Media and the Challenges for the New Generation

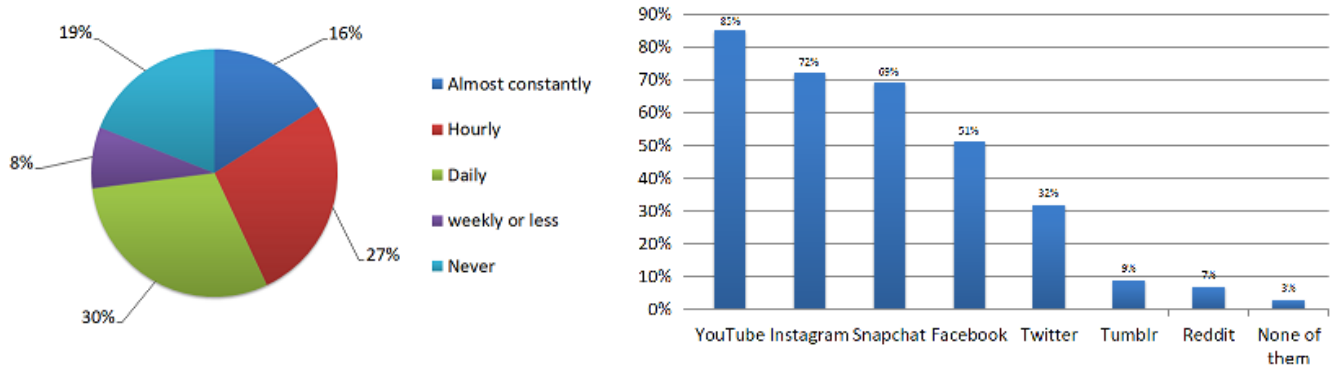
14.5.1 Generation Z and the Effects of Social Media on Their Life

From 1997 until today a new group called Generation Z, the generation following the Millennials has been formed. This new generation has been taking over the Internet, among others. Many changes have been made from the Boomer generation until today's Generation Z. Topics like body positivity, gender identification, racial oppression, and climate change have a very important meaning. With social media, younger people can participate in movements easily and gain information quickly. It was never easier before to express opinions online due to the strong protection of freedom of speech. Changes in social media through Generation Z include increasing support for the LGBTQ community (Davis, 2018). The movement for equal rights and greater acceptance of gender identification is rising daily. Furthermore, platforms like Instagram, Facebook, and X have been portraying the wrong images of real life to younger impressionable children and teenagers. It has become a trend to move against idols that try to show a fake perfect life and instead encourage a better and healthier image. Moreover, young adults have been more active in the oppression of different races, which still has an immense impact on the world. The movement *Fridays for Future* which is for preserving our planet, was formed by Greta Thunberg in 2018 (Kühne, 2019) in response to climate change. However, not only positive changes have occurred with Generation Z. Negative points such as increased depression, anxiety, and cyberbullying have developed as well. The youth must overcome great psychological stress in high schools, universities, jobs, and personal life. Today's rapid technological changes have allowed young adults to move their problems to social media (**Figure 14.2**). In many such cases, challenges are not handled correctly (Toscos & Coupe, 2019).

Results of research conducted by EU, NET, and ADB show that social networking facilitates meeting new people with children and teenagers. It concerns people they have never met and people they know only by sight, for example, in a school corridor or friends of friends.

Young people admit that writing a message to someone on a social networking site is easier than establishing relationships beyond the Internet. For instance, Facebook helps to break the ice with those people with whom previously there was no chance to talk face to face. The motivation for establishing a contact may be a common interest or getting advice on a forthcoming test. Thanks to special groups created on social networking, it is easier to communicate with colleagues regarding schoolwork related issues. Social networking is often the source of all kinds of information for young people. It may be related to current activities, interests, or current events.

In various conducted surveys, participants emphasized that social networking platforms facilitate the formation of opinions concerning individuals they have not yet encountered. Additionally, adolescents contend that Facebook enables them to observe the behaviors, interests, and idiosyncrasies of specific individuals. Social networking also allows teenagers to participate in social life by monitoring information about current social and cultural events, such as upcoming concerts, parties or birthdays of friends or colleagues or any planned meetings.



(a) **(b)**

Figure 14.2 (a) *How frequently do United States' teenagers use Social Media, April 2018 (Statista, 2021),* **(b)** *Most used social media by United States' teenagers, 2018 (Pew Research Center).*

Moreover, young people can follow all issues concerning society online. Thanks to social networking, they can learn how to argue, take a stand on something, and polemize. However, they can also participate in discussions using social networking tools like blogs or discussion forums. The modern teacher can also augment class communication using applications like blogs to establish two-way communication channels with students beyond school hours. In these environments, students like to exchange opinions and observations with other people and present their viewpoints. Thematic portals, forums, and social networking sites support the work and creativity of young people and demonstrate the need to share their experiences with others. Young people are also interested in tips given by their peers on the Internet.

Most students of Facebook create groups with their peers and log in daily to exchange information about their common classes, activities, notes, and to discuss about a not completed course. Particularly, Facebook has become a natural environment for them that offers many tools supporting education in a parallel way.

14.5.2 Social Media Platforms' Different Policy Regulations

Every single social network has its policy regulations. Especially for children, various restrictions and observances differ from network to network.

On Facebook, registration is possible at the age of 13 years. Because 13-year-old children are not mature enough, several other guidelines exist to protect them. It is prohibited to upload any illegal or malicious codes

or posts that tyrannize, daunt, or victimize others. On top of that, every pornographic, threatening, or discriminatory post leads to an exclusion from Facebook. Also, it is not allowed to create any application which does not comply with the age limitation. From time to time, Facebook updates its policy regulations. The latest release in 2015 came along with simplifications in limiting content sharing to increase the user's privacy.

Instagram has almost the same policy regulations as Facebook does. It is also possible to register at 13 years of age, and people may not post violent, nude, partially nude, discriminatory, unlawful, infringing, hateful, pornographic, or sexually suggestive photos or other content via the Service.

YouTube's policy differs a bit from the other platforms. You must be 18 years old to enroll, or 13 years old and need the parents' agreement. or any other guardian's consent. On top of that, it is declared that somebody needs to talk to their parents about what sites are appropriate. There are age limitations for specific videos. A person who would like to enroll must indicate their age and can only see videos that accompany this information. Moreover, there are limitations prohibiting pornographic, racist, or violent material.

Supporting the guidelines of Facebook and Instagram, Snapchat cannot be used by children under 13. For children between 13 and 17 years, parents must review and agree to the terms. There is also control over the so-called "snaps" (pictures only visible to the receiver for a few seconds). If they feature any forbidden content, they are deleted immediately, and the same applies to similar text messages.

Regarding X, the Terms of Services pose no limitations for age. Concerning Google, age limits differ from country to country. In Spain and South Korea, for instance, being 14 years old is the prerequisite, but in the Netherlands, it is 16 years. In all other countries, it is 13 years, which holds for most social networks.

14.5.3 Opportunities

There has been a lot of media attention to the negative aspects of social networking; however, research has shown that social networking can also have a positive impact on children (Firth, 2015). Aspects of this impact can be:

- It can reduce social isolation and loneliness by making it possible to connect to friends and family, even when there is a long distance between them, allowing, e.g., for sharing pictures and videos.
- It makes it possible to find people with the same interests online. This can even result in close friendships.
- It might help in developing one's identity.
- It allows for enrolling in a community and participating in petitions or discussions.
- Project participation is made feasible by having support from corresponding virtual communities. It makes it possible to easily ask for help online without the need to meet up with others.
- Feedback on these projects is a matter of seconds.
- It makes it possible to find information concerning health online and support by networks of persons suffering from similar diseases.

Next to these aspects, research by psychologist Larry D. Rosen (2011) showed that:

- Children who spend much time on Facebook are more capable of showing "virtual empathy" to their online friends.
- Social networking can help children who face problems in their offline social lives learn how to socialize with other people online.

- Social networking can engage young students by providing tools for education in compelling ways.

According to research by the NSPCC (2014), "*young people tend to view social media as a positive influence in their lives, in particular, valuing the social benefits it can provide.*" The social benefits they pointed out were the possibility to talk with friends online, the possibility to be creative, and the possibility to express themselves online. According to them, "*social networks help them to hone their social skills and are a valuable source of advice and emotional support*."

In the article "*The Bad, the Ugly, and the Good of Children's Use of Social Media,*" Jim Taylor says that social media can also help those young people who experience shyness or social anxiety. Introverted young people can gain comfort and confidence in social interactions in several ways. Shy children can use social media to overcome their most difficult challenge, initiating new relationships in a low-risk environment. They can avoid awkwardness that is endemic to making friends by allowing them to gain familiarity with others and build friendships online. Introverted children can also practice social skills with the relative distance and safety social media offers.

Research by PISA (2015) concerning the well-being of children showed that when 15-year-old students were asked if it was very beneficial to have social networks on the internet, 82.1% of boys and 86.5% of girls agreed, or even strongly agreed with this statement.

As stated in the previous paragraphs, social media can also have educational benefits for children. They are learning practical skills necessary for success in today's wired world. Specifically, children are learning to use and become proficient with technology, developing their creative abilities, appreciating new and different perspectives, and enhancing their communication skills.

Technology may even help children better cope with stress in their lives. Technology can potentially mitigate stress is in several ways. First, technology provides children with more outlets to express their feelings of stress, thus allowing a cathartic effect. Second, social media can provide children with social support, acting as a buffer against stressors. Technology, including Facebook postings and instant messaging, enables children to receive more immediate and diverse support from a broader range of people. Third, technology can allow children to find useful information that may help them reduce their stress. Technology may also act as a distraction and a means of distancing children from stressors, providing a respite from the stress and giving them the time and perspective to deal with the stress more effectively.

Social media could also be great for young artists on the internet, as they can share their work with friends and strangers to receive feedback from the audience. Lauren May considers that for young people who like to write or create graphics and digital designs, social media is an ideal place to share their work and get encouragement and feedback from others. Teens and children can come up with innovative ideas and get instant feedback. In this way, social media can be a tool for creative teens. Today, teens and children are used to engaging with their peers daily through social media. They likely check their accounts every few hours, if not sooner, to see what they have missed and what has been shared and discussed among their friends. While it is not face-to-face interaction, social sites and apps can help them improve their social skills, encouraging them to communicate with others they may not have been likely to talk to otherwise. This can help teenagers make new connections, meet new friends, and expand their community. Their social circle can grow, and for introverted individuals, these apps can make meeting and connecting with people a much more pleasant experience. A healthy balance of online and in person interactions is good for, teens and adults alike.

14.5.4 Threats of the Excessive Use of Social Networking Sites by Children and Young People

Social networking is correlated with many threats, especially for children and adolescents. Some of them are shown in the chart below (**Figure 14.3**). In the following paragraphs, some of them are presented in more detail: cyberbullying, cyber grooming, cyberstalking, pornography and harmful content and sharing.

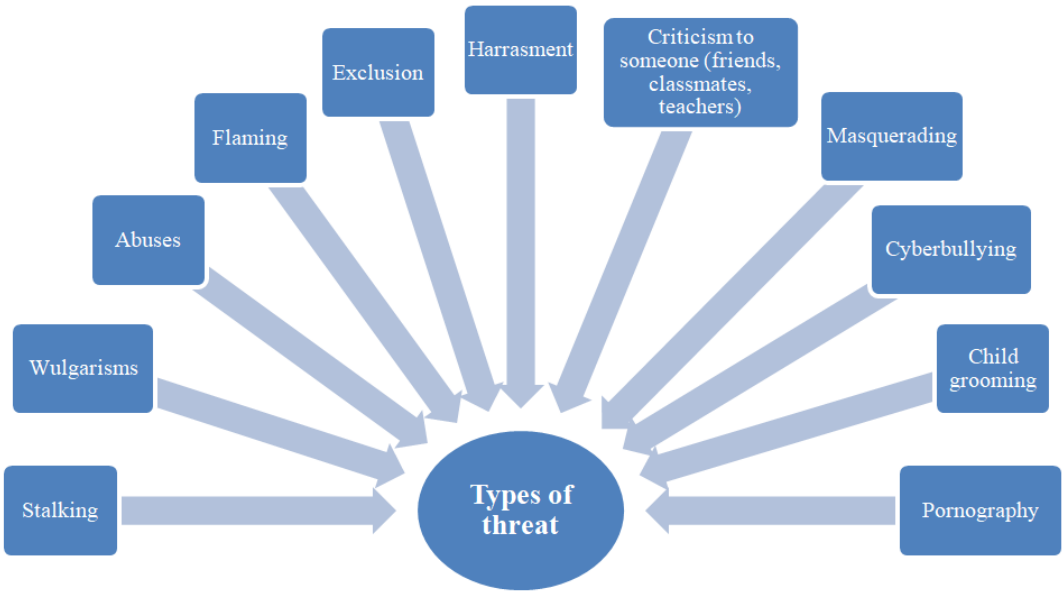


Figure 14.3 *Own elaboration based on Kozak S., "Pathologies of communication on the Internet. Risks and consequences for children and young people" (2011).*

14.5.4.1 Cyberbullying

Cyberbullying is defined as an aggressive, intentional act carried out by a group or individual using electronic forms of contact, repeatedly or over time, against a victim who cannot easily defend himself (Hinduja, 2019). With the increasing use of Internet services and mobile technologies, cyberbullying has become frequent, especially among teens. It may occur on personal websites, or it may be conducted via e-mail, social networking sites, chat rooms, message boards, instant messaging, or cell phones. Cyberbullying is based on sending messages containing slanderous expressions, harmful to victims or verbally bullying others within an online community.

Cyberbullying differs from traditional bullying in several aspects. The most obvious is that it requires some degree of technical expertise. Cyberbullying also provides anonymity to the bully which is not possible to attain with traditional bullying. Because of this, bullies cannot see the reactions of their victims and studies have shown that they feel less remorse. In addition, cyber bullying can be more pervasive than traditional bullying. While traditional bullying is generally limited to school, victims of cyber bullying can be reached anywhere, anytime, and the potential audience is huge. This is compounded by the fact that there is a lack of supervision. Most cyber bullying cases fall into one or more of the following categories:

- **Flaming:** Online fights using electronic messages with angry and vulgar language,
- **Harassment and stalking:** Repeatedly sending cruel, vicious, and/or threatening messages,
- **Denigration:** Sending or posting gossip or rumors about a person to damage his or her reputation or friendships,
- **Impersonation:** Breaking into someone's e-mail account (or social media account) and using it to send vicious or embarrassing material to others,

- **Outing and trickery:** Engaging someone in instant messaging, tricking them into revealing sensitive information, and forwarding that information to others, and
- **Exclusion:** Intentionally excluding someone from an online group.

A cyber bully can be a stranger on the Internet or someone familiar to the victim. In many cases, a cyberbully can also bully in face-to-face encounters. Bullying over the Internet may be a natural extension of their behavior. Most victims of cyberbullies are children, but many adults are cyberbullying victims. Generally, cyberbullies seem to know their victims, but occasionally, they will pick victims they do not know. In this situation, the cyberbully is picking on someone based on a type of bias or prejudice. They may pick on people based on religion, race, gender, sexual orientation, or people who are deemed "not cool."

Cyberbullying cases have a great impact on every individual in the short or long term. However, the issue of this effect not only affects the minds of the victims but also affects the predators. According to Beale (2001) and Roberts and Coursel (1996), victims involved in bullying will suffer mental several effects such as increasing feelings of oppression, loneliness, feelings of self–esteem and feeling of a tendency towards suicide. There have been several cases that involve teenagers committing suicide because of being mistreated or humiliated over the internet. According to Hinduja and Patchin survey (2010), conducted among 2,000 middle-school youths, cyberbullying victims are 1.9 times more likely to attempt suicide than those who are not involved in cyberbullying.

One of the most typical cases of cyberbullying is the Megan Meier story which ended in suicide. Megan Taylor Meier was born on November 6, 1992, in O'Fallon, Missouri. Megan had been diagnosed with attention deficit disorder, depression, and self-esteem issues regarding her weight. Soon after opening an account on MySpace, Megan received a message supposedly from a 16-year-old boy, Josh Evans. Meier and Josh became online friends but never met in person or spoke.

On October 16, 2006, the tone of the messages changed. According to her father, Ron Meier, the last message sent by Josh read, "*Everybody in O'Fallon knows who you are. You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you.*" Some minutes after Megan told her parents about the trouble she had, Tina Meier, Megan's mother, found her daughter dead in her bedroom. Megan Meier had hanged herself with a belt in the bedroom closet.

Several weeks after her death, Megan's parents were told that Lori Drew, the mother of Sarah Drew, a former friend of Megan Meier, had created the "Josh Evans" account. Lori Drew admitted to creating the MySpace account. Sarah and Ashley Grills, Lori's 18-year-old employee aided her. Lori Drew characterized the hoax as a "joke." Initially, Drew denied knowing about the offensive messages sent to Megan. She told the police the account aimed to "gain Megan's confidence and find out what Megan felt about her daughter." However, witnesses testified that the women intended to use Megan's messages sent to "Josh" to get information about her and later humiliate her, in retribution for her allegedly spreading gossip about Drew's daughter. Although Lori Drew had at least contributed to Megan's suicide, the court acquitted Lori in cyberbullying case. St. Charles Prosecutor Jack Banas stated there was insufficient evidence to bring charges.

14.5.4.2 CyberStalking

The Internet has enabled people to socialize and exchange personal information online with a high degree of anonymity. Together with the lack of supervision, this has encouraged different forms of anti-social behavior against vulnerable individuals, including adolescents. Cyberstalking is considered one of the methods that online perpetrators use in order to harass their victims (Pittaro, 2007).

In the real world, stalking definition is an unwanted, obsessive attention to a specific person. Physical stalking can get forms of following, secretly watching, persistent calling and texting to manipulate, and finding other means to approach the victim unexpectedly. Cyberstalkers are driven by the same intention—to

embarrass, threaten, or harass their victims. The difference is that they rely on online technology to do it. Physical and cyberstalking interconnects in many cases, making it even more threatening. Cyberstalkers can use email, social networks, instant messaging, and personal data available online to make inappropriate contact with their victims. It involves nefarious intentions, ranging from false accusations and defamation to sexual harassment and even encouraging others to harass the victim.

Cyber stalkers might terrorize victims by sending unpleasant messages (or even emails) systematically or by sending negative comments on social media, perhaps even several times a day (Hinduja, 2019). It is also common that such messages come from different accounts managed by the same person. This type of online stalking is known as "*Catfishing.*" Catfishing occurs on social media sites, such as Facebook, when online stalkers create fake user profiles and approach their victims as "friends of a friend" or expressing romantic interest. To look more like a real person, cyber stalkers sometimes copy profiles of existing users, impersonating their identity. Another accustomed cyber stalking method is monitoring location check-ins on social media or geotags that some uploaded personal photos may contain. Individuals often add location check-ins to their online profiles. As a consequence, cyber stalkers can easily track individuals by simply scrolling through social media profiles and indicate their behavior patterns quite accurately.

Furthermore, hijacking a personal webcam constitutes one of the most severe cyberstalking methods. This method is usually achieved by tricking individuals into downloading and installing a malware-infected file, granting cyber stalkers access to the intended webcam. In the same manner, cyberstalkers often hack victims' electronic devices, like computers or cell phones, or even their online profiles, in order to intercept personal information (photos, videos, emails, text messages). This information can be used by cyberstalkers in order to harass or blackmail a victim. More often, cyber stalkers post online harmful, negative personal information about the victim, including the victim's name, address, phone number, email address, and other private information. Last but not least, they often take advantage of their access to a victim's online profile by pretending to be the latter in order to embarrass victims.

In 2016, the Data & Society Research Institute and the Center for Innovative Public Health Research published findings from a nationally representative study named *Online Harassment, Digital Abuse, and Cyberstalking in America.* Its findings are based on a nationally representative survey of 3,002 Americans aged 15 and older conducted from May 17 through July 31, 2016.

In order to examine the types of harassment and abuse that Americans have personally experienced, researchers asked internet users about 20 harassing behaviors throughout the survey. Almost half (47%) of Americans have personally experienced one of these harassing behaviors. According to the research, 36% of internet users have experienced direct harassment, such as being called offensive names, being threatened physically, or being stalked. Cyber stalking research has shown that 8% of American internet users have been cyberstalked to the point of feeling unsafe or afraid. Additionally, research revealed that 30% of internet users have experienced invasions of privacy, like hacking, having their personal information exposed online without their permission, being monitored, or being tracked online. Finally, research has shown that men and women are equally likely to face online harassment. However, women experience a wider variety of online abuse, including more serious violations, as noticed in research about young people and sexual minorities.

14.5.4.3 Cyber Grooming

Nowadays, cyber grooming constitutes one of the most serious dangers in cyberspace. Online groomers are sexual predators, usually pedophiles targeting unsuspecting children. They use online platforms to contact their victims and come to a personal meeting with them. The sexual abuse of the victim, physical violence, child prostitution, pornography abuse, or even child kidnapping might be the results of this personal meeting (Machimbarrena et al., 2018).

Online predators often use social networks, such as Facebook, X, or Instagram, dating chatrooms, like Tinder, or even email platforms to contact their victims. However, apart from these communication environments, they also use advertising portals, where they offer various opportunities for employment or careers to adolescents (e.g. in modeling).

Cyber grooming victims are children and young people, usually aged 13 to 17 years, more often girls than boys. It can be assumed that victims are mainly Internet users who spend much of their free time in online communication environments (chatrooms, social networks), where they establish virtual contacts with others (looking for friends and life partners). Children and young people are more susceptible to manipulation because they lack developed social skills and life experience. Among the most common victims are children with low self-esteem and a lack of self-confidence, as it is easier for predators to emotionally or physically isolate children with emotional problems (victims in need) and naive and excessively trusting children who are willing to engage in online conversations with strangers. It is more difficult for them to recognize the risks of online communication among adolescents.

The process of manipulating the victim goes through four basic phases (preparation of the contact, contact with the victim, preparation for a personal appointment, and personal meeting), during which the attacker uses many techniques and procedures.

In the first stage, the attacker prepares the ground for implementing the victim's manipulation. One of the most frequently observed cyber groomer practices is creating a false identity. The attacker provides false personal information about himself such as name, age, or facial picture. Attackers are usually much older than the chosen victims; for that reason, they adjust their age and photos as necessary to complete the matches. In some cases, attackers adjust their identity according to their needs, and therefore they may appear under different nicknames/avatars. They can intentionally adjust their hobbies and interests, or even sex and other personal information, to approach the chosen victim as effectively as possible. Attackers with dynamic identities often communicate with multiple victims at once. Sometimes attackers do not act as individuals but as companies' representatives (managers, directors), who are supposed to bring some benefit to chosen victims. In some cases, where the attacker pretended to be a business executive specializing in financially assisting socially disadvantaged children. On behalf of this company, he then relates to potential victims through Internet adverts.

In the second manipulation stage, the attacker establishes contact with the victim and works to build and sustain a virtual relationship. A characteristic feature of a cyber groomer's behavior is an effect called "mirroring." The predator copies the victim's behavior in an attempt to approach the victim (pretending to have the same age, hobbies, interests, or even problems). By mirroring the attacker creates feelings of trust to the victim, which helps the latter to overcome the fear of communicating with a stranger. Additionally, online groomers try to collect as much of the victim's personal information as possible, to create a complete profile of victim's life (address, phone number, school address).

Online groomers aim to progressively reduce barriers of victims around sexuality by gradually introducing sexual content to the conversation. That could be primarily achieved with a discussion of human sexuality. Attackers usually offer a variety of erotic or pornographic material to victims, to arouse their interest and reduce their shyness, as an attempt to get photographs or videos of naked victims (force the victim to show himself on the webcam or to send personal naked photos). More often, these highly sensitive materials are used by groomers to blackmail their victims.

In the third stage of manipulation, online groomers try to prepare their victims for a personal appointment. At a moment when the predator has enough information about the victim and sensitive materials, he can try to invite him to a personal meeting.

In some cases, predators initially provided false information about their identity. However, they often admit their real age to meet their victims. In order to overcome the age difference between them and their victims, predators try to emotionally blackmail their victims by expressing fake feelings of interest or fear of losing them. Some victims are willing to meet their predator despite the age difference, while others refuse to keep contact with them. If the victim refuses to arrive at the appointment, the attacker begins to blackmail him. More often, online groomers threaten their victims with the publication of compromising material on the Internet (victim's nude photos, personal messages). Most victims cannot resist these threats but rather attend the meeting rather than be subjected to humiliation by others.

14.5.4.4 Sharenting

The term "sharenting" is a neologism coined from the words "parent" and "sharing." It refers to parents posting content about their children on social networks. According to a study by McAffee, 24% of parents publish daily pictures of their children, leading to an average of 1,300 pictures of a child before age 13. Sharenting often starts before the child becomes active online, but also before one's birth: one fourth of the children have a virtual identity before birth (picture of the ultrasound). The most used platform is Facebook, but these photos are shared everywhere. It is done by the average parents—wanting to build one's positive image through one's children, to have social support or to share memories with relatives—and by more influential channels on social networks, such as YouTube or reality show celebrities. The most popular YouTube children's channel is "Swan The Voice Neo et Swan", which has 4.8 million subscribers. They started with toys unboxing but now some videos are more personal, for instance, one of them tells the hospitalization of one of the boys. Some reality show performers' children have Instagram accounts even before birth (for example: chelsea_gcl).

The risks are nevertheless plentiful. The pictures are often accompanied by personal information about children (such as their name, their birth date or their school's address), which makes them vulnerable to predators or identity theft. This information is also likely to be used for profiling and can harm a child's future regarding jobs or advertisements in an algorithm-driven world. In the near future, these images and their dissemination may also have an impact on children's self-esteem (analyzed in the next paragraph), social integration, or perception of privacy. The study mentioned above revealed that only 20% of the parents are concerned by their children's emotions regarding these pictures. At the same time, they are often released in a crucial period in controlling one's image when the peers' feedback is really important. Some contents can be very humiliating for children when exposed to millions of viewers; for example, the TV show *Bébé Ruby* depicts childbirth and parents changing the baby's diaper, exposing both her nudity and face.

While children are constantly told that they are not aware of the risks of the Internet, they feel that their parents do not always master the codes of what is and what is not acceptable on social networks. There is also an undeniable lack of mastery of the networks children and young people use: Snapchat yesterday, Tik Tok today, and undoubtedly a new platform in the near future. At the same time, parents of some famous children (especially Youtubers) are often criticized because they do not show themselves on the screen and do not reveal their real names which shows that they are well aware of the related risks but do not necessarily hesitate to expose their children to them.

14.5.5 Self-Esteem and Social Media

As defined by Smith and Mackie (2007), the concept of self-esteem is the positive or negative evaluations of the self, as in how we feel about it. It is a basic human need. Abraham Maslow placed self-esteem at the top of his hierarchy of human needs. He described two different forms of "esteem":

- the need for respect from others in the form of recognition, success, admiration,
- the need for self-respect in the form of self-love, self-confidence, skill, or aptitude.

According to Maslow, without fulfilling the self-esteem need, individuals will be driven to seek it and unable to grow and obtain self-actualization. Parallel to this line of thought, it can be expected that individuals will strive for positive self-presentations in both online and offline social settings, so online communities offer a gateway for identity construction and self-presentation. It is also likely that people with low self-esteem will be even more eager to engage in online activities that may raise their self-esteem.

The relationship between the use of Social Networking Sites, or the use of the Internet in general, and people's well-being was examined by many researchers. Eric J. Mood reported that high levels of Internet use were associated with low levels of social loneliness and higher levels of emotional loneliness, suggesting that online interactions fail to satisfy one's need for emotional connections in social interactions. However, another research reported that loneliness and depression predicted problematic use of the Internet. If someone creates a Facebook profile just to be present there and it becomes a non-communicative use, it would negatively influence his self-concept or self-esteem because it reduces social integration. If the use of Facebook is related to bridging, bonding, and maintaining social capital, which has been accumulated in society, then it will increase a person's self-esteem.

Personality traits influence the ability to use SNS to build social connections. For example, Sheldon Caplan (2007) found that socially anxious individuals tended to spend more time on Facebook but reported fewer Facebook friends. In contrast, extroverted individuals had more Facebook friends and initiated more online relationships than introverted participants. The same is true with self-esteem. People with low self-esteem tend to have few friends on Facebook, or would rarely post on Instagram, so their self- esteem will decrease. In contrast, people with high self-esteem have many followers on Instagram and post frequently, so they maintain the social capital they gain in society. Social Networking Sites are instruments by which people reflect their self-esteem, but they can also influence them to decrease or increase their belief in themselves.

Striving for an unrealistic aim like, for example, building the perfect shape or even observing thin persons receiving positive feedback for their bodies may negatively influence one's self-image. A study by Irving (1990) stated that being confronted with thin models increased the risk of lower self-esteem and decreased satisfaction with personal weight. Moreover, this reduction of self-esteem is often accompanied by stress, depression, guilt, shame, and insecurity (Stice et al., 1994). These illnesses likely occur because of the unrealistic body-dimension goals set by supporting the internalization of this ideal-body stereotype (Stice et al., 1994). The pressure to achieve this shape increases because this aimed thinness has likely become an indicator of self-control and success (Garfinkel & Garner, 1982). In conclusion, people who often look at pictures with ultra-thin models are at higher risk of decreasing their self-esteem, and therefore, they are more prone to self-esteem-related diseases like eating disorders. For instance, anorexia nervosa, as a kind of eating disorder, is a psychiatric problem which is seen mostly in teenage girls and young women. This serious mental disorder is defined by an intense fear of gaining weight, the rejection of eating enough to reach a certain threshold of body weight, which states a minimal norm for height and age, as well as body image disturbances, and ultimately, amenorrhea (Harrison & Cantor, 1997). Generally, eating disorders like anorexia nervosa occur more often in young females. Accordingly, research from the American Psychiatric Association found that 90% of eating-disordered individuals are women and that the highest rates of anorexic behavior is reported by females in colleges (Widiger & Samuel, 2005).

14.5.6 Narcissism and the Selfie Syndrome

The word narcissist derives from the name Narcissus. Narcissus was an ancient Greek mythological person from Biotia, son of the nymph Liriope and of river Kifissos. According to the myth, Narcissus fell in love with

his own image reflected in a pool of water (Anon, 1998). Due to his addiction to looking at himself in the pool, he died from exhaustion, and at the place where he sat grew a flower named narcissus, which symbolizes his decay (Μπαμπινιώτης, 2008). As a result, a narcissist is a person who has an excessive interest in or admiration of themselves. A narcissist is an extremely self-centered person who has an exaggerated sense of self-importance (Anon, 2018). It is very common to hear from him that he loves himself and that he knows that everybody, with no exception, admires him and loves him unconditionally. Moreover, a narcissist feels that they have few equals in the whole world and that most people do not measure up to them (Navarro, 2017). Because narcissists perceive themselves much better than the average person, they try to present a false mask of self-esteem because they do not want to show that they are vulnerable, too (Paramboukis, 2016).

Instagram is the best place for a narcissist. It is like paradise for them because they can upload pictures of themselves all day, and at the same time, they can enjoy and take pleasure from their followers' likes. They feel fulfilled that way and their self-esteem and their confidence build up constantly. Most narcissists are follower seekers, and for this reason, they follow strangers and hope that they will be followed back. After they are followed back, they unfollow the other person, and with that action, they increase their followers and become more and more famous. There is a kind of narcissist who is called "vulnerable," who is just pleading with other users to follow them. They commonly post a photo with the hashtag "followforfollow," or just comment under celebrity pictures "please follow my account." Fame and publicity are everything for them.

Moreover, something that a narcissist does is delete the less popular and liked photos from their account. This is a common strategy of a narcissist, and for this reason, all of us have someone in our minds who has deleted some photos from his account because the photo did not get enough likes. Additionally, another favorite way of self- promoting for narcissists is hash tagging. If someone wants to find out how to use Instagram to become famous, with just a google search, they will find thousands of sites that promise you the ultimate guides providing success and fame on Instagram. Another thing that narcissists do is that they follow other narcissists because they identify with them (Pettit, 2018).

Narcissists on Instagram because they act in some specific way. To begin with, a typical narcissist posts photos that emphasize their body and their physical appearance. Usually, they take photos in the gym while working out or on the beach in their swimsuits (Lebowitz, 2018). They spend hours trying to find the best picture out of hundreds they took to convince others that they are cool and have the perfect life. A video that was uploaded on YouTube and became viral, named "*Are You Living an Insta Lie? Social Media Vs. Reality,*" shows how users create a fake because t that they want other people to be jealous and they want them to feel inferior and less happy (DitchtheLabelORG, 2017). Instagram's perfect life is a real catch-22 situation for most users.

Furthermore, some other things distinguish a simple user from a narcissist. A narcissist spends more time on the platform every day. Narcissists prefer online communities that consist of shallow relationships so that they have complete control over their self-presentation, which means that they can present themselves in an indefinite number of ways (Sheldon, 2016). When they upload a photo, the photo is edited. Some of them spend many hours trying to edit their photos and do not stop until they have the perfect picture to upload. Another habit that differentiates narcissists from common users is that they frequently change their profile image and choose to put a photo they look perfect in. Finally, they tend to upload selfies more often (Elsevier, 2016, pp. 22–25).

Some scientists of LendEDU researched the topic of social media and narcissism. A survey of 10,000 millennials found that 64 percent believe Instagram is the most narcissistic social media platform—with more votes than Facebook, X, and Snapchat combined (Tamplin, 2017).

A selfie is a very common thing in our everyday lives. It is a picture that captures some part of our bodies, most commonly with a smartphone, or with a webcam and later the photo is uploaded to one or more social media accounts. Especially for young people, it is not absurd to share their bodies with others online, some of them completely strangers. However, what will happen if we lose control? What happens when someone is obsessed with taking photos of his face and his body? The practice of uploading selfies is often viewed as a narcissistic behavior seeking self-glorification and affirmation (Reed, 2015). Resent research found that millennials are more narcissists than previous generations because of social media platforms (Twenge, n.d.). Nowadays, it is very common, especially young women, to have plastic surgery because they want to look perfect when they upload their selfies on their social media account. According to Eduard Farrior, president of the American Academy of Facial Plastic and Reconstructive Surgery (AAFPRS), "Social platforms like Instagram that are based only on images force the patients to hold a microscope onto their own images and look more critically than before their faces." The patients want to share a better image of themselves on their social media accounts because they are searching for friends, possible love interests or even employers (Finol, 2014).

According to some researchers, a typical person will take 25,000 selfies throughout their lifetime. For this reason, scientists have made a new unit to accurately measure narcissism, which measures the number of selfies that we take per hour. Google announced that, in 2016, users uploaded more than 24 billion selfies to their servers using their social media accounts. This is why many psychologists introduce the term *self-obsession* (Gray, 2016).

14.5.7 Internet Addiction Disorder (IAD)

Dr. Kimberly Young identifies five types of addiction associated with computers: cyber-sexual, cyber-relationship addiction, net compulsions, computer addiction, and information overload. Internet Addiction Disorder is a kind of disturbed behavior connected with the use of the Internet with the psychical and behavioral characteristics of addiction. According to Patricia Wallace, "*some psychological elements of the Internet can be so attractive and absorbing that can lead people to intensive use of the Internet and even to compulsive abuse.*" This problem can occur when using the Internet and being online becomes one of the most important human activities.

Internet Addiction Disorder can be recognized by the substantial decline in interest in any other activity rather than activities connected with a computer. People who have problems with Internet addiction do not participate in social life. They also have long-term depressed moods, and they are isolated and sad. This is also directly connected with bad academic performance (children and young people spend time on social networking sites instead of studying and concentrating on school). Unfortunately, the following symptoms of IAD are health problems (pain in the spine, the overall feeling of being unwell, eye pain, headache, stomachache, etc.).

The effects of Internet addiction are a disorder of interpersonal relationships (the resignation of direct contact with others), sometimes financial problems, forgetting about meals, disturbances in the sphere of feelings and emotions, etc.).

Parents and teachers should pay attention to children when they spend too much time using the Internet. Children may have a problem limiting time spent on the Internet. The next issue is irritation caused by an interruption of the Internet and mainly social networking sites. Lack of control over time spent could also be a symptom. Eventually, people addicted to Internet usually argue frequently with other family members.

14.6 Conclusion

Information and Communication Technology (ICT) has become an integral part of the 21st century, encompassing technological, social, cultural, and economic aspects. Its presence necessitates the establishment of conducive circumstances and the execution of suitable tactics to achieve educational objectives within an integrated, pedagogical, social, and cultural framework. This, in turn, will facilitate the utilization of ICT as a catalyst for broader educational reform and societal reorganization.

Education, though, is a complex undertaking, from the intricate cognitive processes of the human mind to the systemic complexities of human capital development in the 21st century. With society, technology, and schools constantly evolving, ICTs must be accepted and used properly. The more technology evolves, the more humanity should respond to it. It is vital to use the tools that ICT provides to develop a new way of education. There is no doubt that we are in the early stages of what will be a very long process. However, the dynamics of the Covid-19 pandemic have enormously accelerated the diffusion of distance learning platforms, synchronous or asynchronous in all educational levels, proving that technology was mature enough to support these methods and that it was all a matter of prevailing circumstances and social receptiveness to move to this level. Its results provided fertile terrain for further investigation and evaluation in the years to come. Not to neglect is that this unprecedented situation highlighted issues of uneven development between developed and developing countries as well as sensitive issues of private data disclosure that also need careful consideration.

On the other hand, multiplayer online games have indeed proven to be highly complex social spaces that offer and clearly promote social interaction and cooperation. The same applies to direct social learning opportunities in the sense that players can learn and practice socialization strategies by socializing with fellow players online. Since online gaming inherently offers a framework for observing other players' social interaction, it also comes with the indirect social learning opportunity to learn inappropriate behavior through others.

In conclusion, social media has positive and negative aspects that can affect the lives of children and teens in different ways. Social media could be great for learning and sharing photos or videos with friends and strangers, they could be used to meet and exchange ideas with people with the same interests. Also, young artists and writers could benefit from social media to share their work with the world and receive feedback. Social media could also have negative effects that can affect children very severely, as many of them become victims of cyber-bulling, suffer from social depression, tend to share too much personal information, and are exposed to unappropriated advertising; all this can also affect their mental health. Social media is part of our lives, and it is very hard to hide from it; the children should be often checked by their parents, and if there are problems with cyberbullies or strangers, they should talk to their parents and the website admins about the persons that cause them harm. Social media is neither bad nor good; it mostly depends on who is using it and in what circumstances.

Restricting access to social networking may reduce the risks children experience online on the one hand, and, on the other, it will also restrain the possibilities for children to develop certain "digital skills" and to improve their social lives. Research suggests that children should be made aware of the possible negative consequences and that there should be a clear public policy on improving the safety of children's "digital life."

References

Ahmad T., 2015. "Preparing for the future of higher education." *On the Horizon*, 23(4), pp. 323–330.

Akinwale O., "THE EFFECT OF MOBILE PHONES ON STUDENTS' ACADEMIC PERFORMANCE" [Online]. Available at: https://www.academia.edu/29026191/THE_EFFECT_OF_MOBILE_PHONES_ON_STUDENTS_ACADEMIC_PERFORMANCE?email_work_card=interaction_paper [Accessed on 12 December 2019].

Akrivopoulou C., and Garipidis N., 2012. "Human rights and risks in the digital era. Hershey," PA: Information Science Reference.

Al-Deen H. S. N., and Hendricks J. A., 2011. *Social media: usage and impact*. Lexington books.

Allmer T., 2015. *Critical Theory and Social Media*. Routledge, Taylor and Francis Group, London and New York.

Smith, E. R., and Mackie D. M., (2007). *Social Psychology* (Third ed.). Hove: Psychology Press.

American Academy of Pediatrics, 2014. "Sexting and Sexual Behavior Among Middle School Students" [Online]. Available at: https://pediatrics.aappublications.org/content/134/1/e21 [Accessed 8 December 2019].

American Academy of Pediatrics, 2016. "Cell Phone Radiation & Children's Health: What Parents Need to Know" [Online]. Available at: https://www.healthychildren.org/English/safety-prevention/all-around/Pages/Cell-Phone-Radiation-Childrens-Health.aspx [Accessed on May 2019].

American Academy of Pediatrics, 2017. "Grade School Students Who Own Cell Phones are More Likely to be Cyberbullied" [Online]. Available at: https://www.aappublications.org/news/2017/09/15/NCECellPhone091817 [Accessed 8 December 2019].

Anderson M., 2018. "A Majority of Teens Have Experienced Some Form of Cyberbullying." Pew Research Center. *Internet, Science & Tech*.

Anon, 1998. "The Chambers Dictionary. "The Authority of English Today. [Online] Available at: https://www.merriam-webster.com/dictionary/narcissism [Accessed 18 November 2018].

Antoniadou N., and Kokkinos M., 2013. "A review of research on cyber-bullying in Greece." *International Journal of Adolescence and Youth*. Vol 20, No 2 20, pp. 185–201. https://doi.org/10.1080/02673843.2013.778207

Anyangwe E., 2012. "20 ways if thinking about digital literacy in higher education" [Online]. Available at: http://www.theguardian.com/higher-education-network/blog/2012/may/15/digital-literacy-in-universities [Accessed 2 January 2016].

Avraam E., 2002. "Εξ αποστάσεως εκπαίδευση, διάδραση ανθρώπου και τεχνολογίας" [distance learning, interaction between human and technology]. Available at: https://dspace.lib.uom.gr/bitstream/2159/1007/3/AvraamEuangelia_Msc2002.pdf

Axelrod E., 2009. *Violence goes to the internet.* Springfield, Ill., Thomas.

Barnwell P., 2016. "Do Smartphones Have a Place in the Classroom?" [Online]. Available at: https://www.theatlantic.com/education/archive/2016/04/do-smartphones-have-a-place-in-the-classroom/480231/ [Accessed 12 December 2018].

Beland L. P, and Murphy R., 2015. "Communication: Technology, Distraction & Student Performance" [Online]. Available at: http://cep.lse.ac.uk/pubs/download/dp1350.pdf [Accessed 9 December 2019].

Bentley H., Burrows A., Hafizi M., Kumari P., Mussen N., O' Hagan O., and Peppiate J., 2019. "How safe are our children?" An overview of data on child abuse online. NSPCC.

Bigiti E.-M., 2018. "Artificial Intelligence (AI)" [Online]. Available at: https://www.academia.edu/36674977/%CE%A4%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE_%CE%9D%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7_%CE%A4%CE%9D_-_Artificial_Intelligence_AI_?fbclid=IwAR3X71SFBPAPGPv9DZdsV9ya1PUXREX0xcoT9oSyRWy74UKMcTxJnxnS1k4 [Accessed 19 January 2020].

Blair D., 2015. "Finland to teach typing rather than handwriting in schools." *The Telegraph* [Online]. Available at: https://www.telegraph.co.uk/news/worldnews/europe/finland/11391999/Finland-to-teach-typing-rather-than-handwriting-in-schools.html [Accessed 6 December 2019].

Bloom B. S., 1956. "Taxonomy of educational objectives – The classification of educational goals." *Handbook 1: Cognitive domain*. London: Longmans, Green & Co. Ltd.

Bos M. W., Duke K., Gneezy A., and Ward A. F., 2017. "Brain Drain: The Mere Presence of One's Own Smartphone Reduces Available Cognitive Capacity" [Online]. Available at: https://www.journals.uchicago.edu/doi/full/10.1086/691462 [Accessed 12 December 2019].

Brightman J., 2014. "Humble Bundle has raised over $50 million." *GamesIndustry.biz*.

Britland, M., 2013. "What is the future of technology in education" [Online]. Available from:http://www.theguardian.com/teacher-network/teacher-blog/2013/jun/19/technology-future-education-cloud-social-learning [Accessed 22 December 2015].

Buckingham D., 2006. *Digital Generations: Children, Young People and New Media*. London: Routledge.

Buckingham D., 2007. "Digital Media Literacies: rethinking media education in the age of the Internet." *Research in Comparative and International Education*, 2(1), pp. 43–45.

Caplan S., 2007. "Relations among loneliness, social anxiety, and problematic Internet use." *CyberPsychology & Behavior* 2007.

Chien J., 2012. "How Digital Media And Internet Transforming Education." University of Denverd E-learning conference [Online]. Available at: https://www.researchgate.net/publication/235901330_How_digital_media_and_Internet_transforming_education [Accessed 23 August 2019].

Cohen, J., 2013. "Top YouTuber PewDiePie Raising $250,000 For Charity: Water." Available at: https://www.tubefilter.com/2013/07/14/pewdiepie-charity-water/

Conway M., 2011. "Exploring the implications, challenges and potential of new media and learning." *On the Horizon*, 19(4), pp. 245–252.

Culpepper D., 2017. "Students' Perception of Cell Phones in the Classroom." *International Journal of Humanities Social Sciences and Education* (IJHSSE), 4(11) [Online]. Available at: https://www.researchgate.net/publication/331715927_Students'_Perception_of_Cell_Phones_in_the_Classroom#39;_Perception_of_Cell_Phones_in_the_Classroom [Accessed 4 December 2019].

Cybercivilrights.org, 2019. "Cyber Civil Rights Initiative" [online]. Available at: https://www.cybercivilrights.org/ [Accessed 16 December 2020].

Davis C.H., Deil-Amen R., Rios-Aguilar C., and González Canché M.S., 2015. "Social media, higher education, and community colleges: A research synthesis and implications for the study of two-year institutions." *Community College Journal of Research and Practice*, 39(5), pp. 409–422.

Davis N., 2019. "One in four children have problematic smartphone use." *The Guardian*, 29th November [Online]. Available at: https://www.theguardian.com/society/2019/nov/29/one-in-four-children-have-problematic-smartphone-use [Accessed 2/12/2019].

Davis S., 2018. "Objectification, Sexualization, and Misrepresentation", Social Media and the College Experience Social Media + Society. [Online]. Available at: https://doi.org/10.1177/2056305118786727 [Accessed 20 December 2019]

Dimock M., 2019. "Defining generations: Where Millennials end and Generation Z begins" [Online]. Available at: https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/ [Accessed 20 December 2019].

DitchtheLabelORG, 2017. "Are You Living an Insta Lie?" Social Media Vs. Reality. [Online] Available at: https://www.youtube.com/watch?v=0EFHbruKEmw [Accessed 14 December 2018].

Ellison N. B., Steinfield C., and Lampe C., 2007. "The Benefits of Facebook Friends: Social Capital and College Students Use of Online Social Network Sites." *Journal of Computer-Mediated Communication*, pp. 1143-1144.

Elsevier, 2016. "Personality and Individual Differences" [Online]. Available at: https://www.sciencedirect.com/science/article/pii/S0191886905002679 [Accessed 25 November 2018].

Englander E., Donnerstein E., Kowalski R., Lin C.A., and Parti K., 2017. "Defining Cyberbullying." *Paediatrics* 140, S148–S151. https://doi.org/10.1542/peds.2016-1758U

Faucher C., Jackson M., and Cassidy W., 2014. "Cyberbullying among University Students: Gendered Experiences, Impacts, and Perspectives" [WWW Document]. *Education Research International*. https://doi.org/10.1155/2014/698545

Federal Bureau of Investigation, 2019. "Welcome to FBI.gov." Federal Bureau of Investigation [Online]. Available at: https://www.fbi.gov/ [Accessed 25 January 2020].

Finol J. E., 2014. "Nuevos escenarios en la Corposfera: Fotografía, selfies y neo-narcisismo [Online]. Available at: http://www.revistalis.com.ar/index.php/lis/article/viewFile/158/156 [Accessed 12 December 2018].

Freeman S., Eddy S.L., McDonough M., Smith M.K., Okorafor N., Jordt H., and Wenderoth M.P., 2014. "Active learning increases student performance in science, engineering, and mathematics." *Proceedings of the National Academy of Sciences of the United States of America*. Vol. 111, no. 23.

Front Psychiatry 2016, "Symptomatology of problematic cell-phone use vs. DSM-5 criteria for compulsive gambling and substance use" [Online]. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5076301/table/T1/ [Accessed 3/12/2019].

Gold Mercury International (GMI), (2014). "The Future of E-Ducation: The Impact of Technology and Analytics on the Education Industry" [Online]. Available from: http://www.goldmercury.org/wp-content/uploads/2014/01/The-Future-of-E-Ducation-Report-2014-Gold-Mercury-International_Issuu.pdf [Accessed 20 December 2015].

Grabowski B., 2009. "ICT as an Enabler for Effective Learning Design: Its Evolving Promise." *International Journal for Educational Media and Technology*, 3, pp. 12-23.

Gray R., 2016. "What a vain bunch we really are! 24 billion selfies were uploaded to Google last year" [Online]. Available at: https://www.dailymail.co.uk/sciencetech/article-3619679/What-vain-bunch-really-24-billion-selfies-uploaded-Google-year.html [Accessed 12 November 2018].

Greenhow C., and Lewin C., 2016. "Social media and education: Reconceptualizing the boundaries of formal and informal learning." *Learning, media and technology*, 41(1), pp. 6–30.

Grinager H., 2006. "How education technology leads to improved student achievement" (USA). Denver. CO: Education Technology Partners: Technology in K-12. Education. Retrieved 12 January 12 2019.

Haddon L., and Livingstone S., 2009. *Kids Online: opportunities and risks for children*. Bristol, UK: Policy Press.

Hamid T., and Maple C., 2013. "Online Harassment and Digital Stalking." *International Journal of Computer Applications*.

Hemsley J., Jacobson J., Gruzd A., and Mai P., 2018. "Social Media for Social Good or Evil: An Introduction." *Social Media + Society*. [Online]. Available at: https://doi.org/10.1177/2056305118786719 [Accessed 20 December 2019].

Hennessy S., Harrison D, and Wamakote L., 2010. "Teacher Factors Influencing Classroom Use of ICT in Sub-Saharan Africa." Itupale On line, *Journal of African Studies*, 2:39-54.

Herodotou C., 2017. "Young children and tablets; A systematic review of effects on learning and development." *Journal of computer assisted learning*, 34 (1), pp. 1–9. https://doi.org/10.1111/jcal 12220

Hinduja S., and Patchin J., 2018. "Connecting Adolescent Suicide to the Severity of Bullying and Cyberbullying." *Journal of School Violence*.

Hinduja S., and Patchin J., 2015. "Measuring Cyberbullying: Implications for research." *AGGRESSION AND VIOLENT BEHAVIOR*.

Hinduja S., 2019. "Cyberstalking-Cyberbullying Research Center" [Online]. Cyberbullying Research Center. Available at: https://cyberbullying.org/cyberstalking

Instagram, 2018. "Tips for parents" [Online]. Available at: https://help.instagram.com/ [Accessed 10 November 2018].

Jabłońska M. R., 2017. "Modern Consumer in Cyberspace-Internet and Psychology Approach" [Online]. Available at: https://doi.org/10.1515/fman-2017-0009 [Accessed 20 December 2019].

Jamil D., and Khan M. N. A., 2011. "Is ethical hacking ethical?" I*nternational Journal of Engineering Science and Technology* (IJEST).

Javier Yanes, 2019. "Should the Time Children Spend in Front of Screens be Limited?" Open Mind BBVA, [Online]. Available at: https://www.bbvaopenmind.com/en/technology/digital-world/should-the-time-children-spend-in-front-of-screens-be-limited/ [Accessed 9 December 19].

Jennings B., and Mary Beth Oliver M. B., 2009. *Media Effects, Advances in Theory and Research*, 3rd edition, Routledge.

Jo Sales N., 2019. "The majority of 11-year-olds own smartphones. And experts are worried." *The Guardian*, 1st November [Online]. Available at: https://www.theguardian.com/commentisfree/2019/nov/01/smartphones-children-technology-mobile-phones [Accessed 01 December 2019].

Junco R., Heibergert G., & Loken E., 2010. "The effect of Twitter on college student engagement and grades." *Journal of Computer Assisted Learning*, 27(2), pp. 119–132.

Kiesbye S., 2010. *Does the internet increase crime?* Detroit: Greenhaven Press.

Kizza J., 2011. *Computer network security and cyber ethics*. Jefferson, N.C.: McFarland.

Korte W. B., and Hüsing T., 2006. "Benchmarking Access and Use of ICT in European Schools, Results from Head Teacher and A Classroom Teacher Surveys in 27 European Countries." empiricaGesellschaftfürKommunikations- und TechnologieforschungmbH 2006.

Kowalski K., 2016. "When smartphones go to school" [Online]. Available at: https://www.sciencenewsforstudents.org/article/when-smartphones-go-school [Accessed 12 December 2018].

Kowalski R. M., Limber S.P., and Agatston P.W., 2007. "Cyber Bullying: Bullying in the Digital Age." 1st edition. ed. Wiley-Blackwell, Malden, MA.

Kozak S., 2011. *Pathologies of communication on the Internet. Risks and consequences for children and young people*. Difin 2011.

Kraut R., Patterson M., and Lundmark V., 1998. "Internet paradox: A social technology that reduces social involvement and psychological well-being?" *American Psychologist* 1998.

Kuh G. D., 2009. "What student affairs professionals need to know about student engagement. *Journal of College Student Development*, 50, pp. 683–706.

Kühne R., 2019. "Climate Change: The Science Behind Greta Thunberg and Fridays for Future." [Online]. Available at: https://doi.org/10.31219/osf.io/2n6kj [Accessed 20 December 2019].

Leach J., Ahmed A., Makalima S., and Power T., 2005. "DEEP IMPACT: An investigation of the use of information and communication technologies for teacher education in the global south." London: DFID.

Lebowitz S., 2018. "Narcissists can hide in plain sight on Instagram — here are 7 signs you're following one" [Online]. Available at: https://www.businessinsider.com/narcissists-habits-instagram-2018-1 [Accessed 19 December 2020].

Lenhart A., Ybarra M., Zickuhr K., and Price-Feeney M., 2016. "Online harassment, digital abuse, and cyberstalking in America." *Data & Society Research Institute*.

Li C., and Lalani F., 2020. "The COVID-19 pandemic has changed education forever." [Online] *World Economic Forum*. Available at: https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning [Accessed 12 March 2020].

Li Q., and Ma X., 2010. "A Meta-analysis of the effects of computer. Technology on School Students' Mathematics Learning." *Educational Psychology Review*,22 (3), pp. 215–243. https//doi.org/10.007/s10648-010-9125-8

Lipschultz J., 2015. *Social media communication*. New York, NY: Routledge.

Livingstone S., and Haddon L., 2009. "Introduction: kids online: opportunities and risks for children." Livingstone S., Haddon, L. (Eds.), *Kids Online: Opportunities and Risks for Children*. The Policy Press, Bristol, UK, pp. 1–6.

Ma W., Adesope O.O., Nesbit J.C., and Liu Q., 2014. "Intelligent tutoring systems and learning outcomes: A Meta-analysis." *Journal of Educational Psychology*, 106(4), pp. 901–918. https://www.apa.org/pubs/journals/features/edu-a0037123.pdf

Machimbarrena J., Calvete E., Fernández-González L., Álvarez-Bardón A., Álvarez-Fernández L., and González-Cabrera J., 2018. "Internet Risks: An Overview of Victimization in Cyberbullying, Cyber Dating Abuse, Sexting, Online Grooming and Problematic Internet Use." *International Journal of Environmental Research and Public Health*.

Marsh S., 2014. "Inside Steve Jobs schools: swapping books for iPads." *The Guardian* [Online]. Available at: https://www.theguardian.com/teacher-network/teacher-blog/2014/oct/07/text-books-school-ipad-steve-jobs-classrooms [Accessed 6 December 2019].

Marsh S., Plowman L., Yamada-Rice D., Bishop J.C., Lahmar J., Scott F., Davenport A., Davis S., French K., Piras M., Thornhill S., Robinson P., and Winter P., 2015. "Exploring Play and Creativity in Pre-Schoolers' Use of Apps: Final Project Report." Available at: http://techandplay.org/tap-media-pack.pdf [Accessed 2 April 19].

Mascheroni G., and Cuman, A., 2014. "Net Children Go Mobile: Final report Deliverables." D 6.4 & D5.2 Milano: Educatt.

Maslow A. H., 1987. *Motivation and Personality* (Third ed.). New York: Harper & Row.

McCoy W., (n.d.). "Five positive effects of Technology on Education" [Online]. Available at: http://smallbusiness.chron.com/five-positive-effects-technology-education-31222.html [Accessed 19 December 2015].

McQuade S. C., Colt J. P., and Meyer N.B., 2009. *Cyber bullying: protecting kids and adults from online bullies*. Westport, Conn.: Praeger Publishers.

Mertzanos A., 2013. "Τι είναι το cloud computing. Ανάλυση με απλά λόγια."[Online]. Available at: http://webapptester.com/ti-einai-cloud-computing [Accessed 19 December 2017].

Metzger M., and Flanagin J., 2008. "Digital Media, Youth, And Credibility." Massachusetts Institute of Technology.

Miller S., 2019. "How will technology change education in the future" [Online]: Available at: https://www.itbriefcase.net/how-technology-will-change-education-in-the-future?fbclid=IwAR1d_E4Axu_TTWaWfDR8_8tI9aQCocIUHhtH8-WDjHQ4wmhwjmGtwWkJhck [Accessed 5 May 2020].

Moody E., 2001. "Internet use and its relationship to loneliness." *CyberPsychology & Behavior* 2001.

Natriello G., 2005. "Modest Changes, Revolutionary Possibilities: Distance Learning and the Future of Education" [Online]. Available at: https://cdn.tc-library.org/Rhizr/Files/sHzT6ngX98NEDhAP8/files/38_12099.pdf?fbclid=IwAR1GfxrMUo_DHvxfbBndCajxmd7NeKXAnd41lLocipWAb44ZAQZIozNSZyE [Accessed 3 March 2018].

Navarro J., 2017. "Inside the Mind of a Narcissist" [Online]. Available at: https://www.psychologytoday.com/us/blog/spycatcher/201709/inside-the-mind-narcissist [Accessed 10 December 2018].

Neier S., and Zayer L. T., 2015. "Students' perceptions and experiences of social media in higher education." *Journal of Marketing Education*, 37(3), pp. 133–143.

Nwachukwu S., Ugwu C., and Wogu J., 2021. "Digital Learning in Post COVID-19 Era: Policy Options and Prospects for Quality Education in Nigeria." *Library Philosophy and Practice* (e-journal) [Online]. Available at: https://digitalcommons.unl.edu/libphilprac/5122/

O'Bryan, L., 2012. "Six ways to use social media in education" [Online]. Available at: https://cit.duke.edu/blog/2012/04/six-ways-to-use-social-media-in-education/ [Accessed 4 January 2016].

OECD, 2017. "Pisa 2015 Results: Students' well-being." Volume III Available at: https://www.oecd.org/education/pisa-2015-results-volume-iii-9789264273856-en.htm

Ofcom, 2015. "Children and Parents: Media Use and Attitudes Report." Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-nov-15

Oliveto J., 2017. "The Effects of Digital Media Consumption on Education" [Online]. Available at: https://www.qaeducation.co.uk/content/effects-digital-media-consumption-education (Accessed: 12/12/2018).

Polglase M., 2018. The impact of the digital revolution on education [Online]. Available at: https://www.familyzone.com/schools/blog/the-impact-of-the-digital-revolution-on-education [Accessed 12 December 2018].

Ouvrein G., and Versjwijvel K., 2019. "Sharenting: Parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management." *Children and Youth Services Review* (vol 99).

Ouyang J.R., and Stanley N., 2014. "Theories and Research in Educational Technology and Distance Learning Instruction through Blackboard." *Universal Journal of Educational Research* 2(2): pp. 161-172, 2014. http://www.hrpub.org https://doi.org/10.13189/ujer.2014.020208 [Online]. Available at: https://files.eric.ed.gov/fulltext/EJ1053980.pdf?fbclid=IwAR2M0uMdH1p7GEpP4tPU1RkOvK0gkSs0iTWB6LdygA-e6Oas5tzI_kwinUE [Accessed 25 November 2020].

Paramboukis O., 2016. "An Exploratory Study of the Relationships between Narcissism, Self-Esteem and Instagram Use" [Online] Available at: https://www.scirp.org/journal/PaperInformation.aspx?paperID=66043 [Accessed 25 November 2018].

Pettit H., 2018. "Narcissists like fellow narcissists on Instagram: Users who take selfies are more likely to follow 'arrogant' and 'attention-seeking' people" [Online]. Available at: https://www.dailymail.co.uk/sciencetech/article-5249705/Narcissists-love-narcissists-Instagram.html [Accessed 03 December 2018].

PewDiePie, 2013. "Thank you! (We raised $450 000 for Charity Water).". *PewDiePie,* YouTube.

Pierson E., 2015. "Assessing the Impact of Digital Media on Learning and Teaching." *Education Development Center*.

Pilgrim K., and Bohnet-Joschko S., 2019. "Selling health and happiness how influencers communicate on Instagram about dieting and exercise: Mixed methods research" [Online]. Available at: https://doi.org/10.1186/s12889-019-7387-8 [Accessed 20 December 2019].

Pittaro M. L., 2007. "Cyber stalking: An Analysis of Online Harassment and Intimidation." *International Journal of Cyber Criminology*.

Polakovic G., 2018. "Smartphone Use Linked to Behavioral Problems in Kids" [Online]. Available at: https://news.usc.edu/146032/digital-media-use-linked-to-behavioral-problems-in-kid [Accessed 2 December 2019]

Popenici S., and Kerr S., 2017. "Exploring the impact of artificial intelligence on teaching and learning in higher education." *Research and Practice in Technology Enhanced Learning* (2017) 12:22. https://doi.org/10.1186/s41039-017-0062-8 [Online]. Available at: https://telrp.springeropen.com/track/pdf/10.1186/s41039-017-0062-8?fbclid=IwAR2hYI_CUImBLxGV6gOF7Owbo6z6XshPUR63RLueaBXMx9iz2JBy-rxLJ1w

Psychology Today, 2018. "What Is Self-Esteem?" [Online]. Available at: https://www.psychologytoday.com/intl/basics/self-esteem [Accessed 09 December 2018].

Pulliam D., 2017. "Effect of Student Classroom Cell Phone Usage on Teachers" [Online]. Available at: https://digitalcommons.wku.edu/cgi/viewcontent.cgi?article=2921&context=theses [Accessed 12 December 2018].

Ragan E. D., Jennings S. R., Massey J. D., and Doolittle, P. E., 2014. "Unregulated use of laptops over time in large lecture classes." *Computers and Education*, 78, pp. 78–86. [Online]. Available at: https://doi.org/10.1016/j.compedu.2014.05.002 [Accessed 12 December 2018].

Raja R., and Nagasubramani P. C., 2018. "Impact of modern technology in education" [Online]. Available at: https://www.researchgate.net/publication/325086709_Impact_of_modern_technology_in_education?fbclid=IwAR12IN7hJKMwsxW8trDrCKGt8nOIdKDoIfuuHVhWGnQBPtRTDipONox0ic0

Raths D., 2015. "Where Flipped Learning Research Is Going" [Online]. Available at: https://campustechnology.com/Articles/2015/04/15/Where-Flipped-Learning-Research-Is-Going.aspx?Page=1 [Accessed 6 December 2019].

Raut V., and Patil P., 2016. "Use of Social Media in Education: Positive and Negative impact on the students." *International Journal on Recent and Innovation Trends in Computing and Communication*, 4(1), pp. 281–285.

Reed M., 2015. "Narcissism and the Selfie: Investigating Millennial." [Online]. Available at: https://digitalcommons.andrews.edu/cgi/viewcontent.cgi?referer=https://scholar.google.gr/&httpsredir=1&article=1108&context=honors [Accessed 28 November 2018].

Rhea K., 2017. "Survey: 94% of Students Want to Use Their Cell Phones in Class" [Online]. Available at: https://campustechnology.com/articles/2017/12/12/students-want-to-use-their-cell-phones-in-class.aspx?m=1 [Accessed 4 November 2019].

Ritter B., 2008. "CYBERSEXUAL HARASSMENT: DEVELOPMENT AND VALIDATION OF A MEASURE OF THE ONLINE ENVIRONMENT AND ONLINE SEXUAL HARASSMENT." *Academy of Management Proceedings*.

Rosen L. D., 2011. "Social Networking's Good and Bad Impacts on Kids." *American Psychological Association*.

Ruston D., 2017. "Smartphones aren't a smart choice in middle school" [Online]. Available at: https://edition.cnn.com/2017/12/22/opinions/smartphones-middle-school-opinion-ruston/index.html [Accessed 14 November 2018].

Rutledge C. M., Gillmor K. L., and Gillen M. M., 2013. "Does This Profile Picture Make Me Look Fat? Facebook and Body Image in College Students." *Psychology of Popular Media Culture* 2013, Vol. 2, No. 4, pp. 251–258.

Sana F., Weston T., and Cepeda, N. J., 2013. "Laptop multitasking hinders classroom learning for both users and nearby peers." *Computers and Education*, 62, pp. 24–31. [Online]. Available at: https://doi.org/10.1016/j.compedu.2012.10.003

Schmelzer R., 2019. "AI applications in education" [Online]. Available at: https://www.forbes.com/sites/cognitiveworld/2019/07/12/ai-applications-in-education/#79962abd62a3

Sheldon P., 2016. "Computers in Human Behavior." *Elsevier*, May, pp. 89–97.

Sheninger E., 2016. "5 Ways Digital Tools Are Transforming the Education Space." [Online] Available at: https://edtechmagazine.com [Accessed 6 September 2018].

Siesage D., 2013. "The Internet never forgets, so be careful what you put on it" [Online]. Available at: https://www.independent.co.uk/student/istudents/the-internet-never-forgets-so-be-careful-what-you-put-on-it-8787706.html [Accessed 20 December 2019].

Solutech K., 2019. "Impact of social media on school and college students." Available at: http://www.klientsolutech.com/impact-of-social-media-on-school-and-college-students/ [Accessed 18 December 2019].

Spears B. A., Taddeo C. M., Daly A. L., Stretton A., and Karklins L. T., 2015. "Cyberbullying, help-seeking and mental health in young Australians: Implications for public health." *International Journal of Public Health*.

Stald G., Green L., Barbovski M., Haddon L., Mascheroni G., Ságvári B., Scifo B., and Tsaliki L., 2014. "Online on the mobile: Internet use on smartphones and associated risks among youth in Europe." London: *EU Kids Online*, LSE.

Stevenson, I. X. J. 2014. "Social media application in digital libraries." *Online Information Review*, 38(4), pp. 502–523.

Stice A., Schupak-Neuberg E., Shaw H. E., and Stein R. I., 1994, "Relation of Media Exposure to Eating Disorder Symptomatology: An Examination of Mediating Mechanisms." *Journal of Abnormal Psychology, 103(04)*, pp. 836-840.

Strommen E.F., and Lincoln B., 1992. "Constructivism, Technology, and the Future of Classroom Learning." Available at: https://journals.sagepub.com/doi/10.1177/0013124592024004004[Accessed 18 February 2015].

Sung Y., 2019. "Cyber-Sexual Violence Victimization of College Women Students: Test of Cyber Lifestyle-Routine Activity Theory." Korean Association of Criminal Psychology.

Tamplin H., 2017. "Instagram Users Are Massive Narcissists, Study Shows" [Online]. Available at: https://www.elitedaily.com/social-news/instagram-study-narcissistic-social-media-site/1848268 [Accessed 20 November 2018].

Tapscott D., 2008. *Grown up Digital: How the Net Generation is Changing your world*, Athens: Leader books.

Thompson C., 2018. "Cell Phones Gaining Acceptance Inside Some Schools, Survey Says" [Online]. Available at: https://boston.cbslocal.com/2018/04/02/cell-phones-in-school-survey-results/ [Accessed 5 December 2019].

Toscos T., Coupe A., Flanagan M., Drouin M., Carpenter M., Reining L., Roebuck A., and Mirro M. J., 2019. "Teens Using Screens for Help: Impact of Suicidal Ideation, Anxiety, and Depression Levels on Youth Preferences for Telemental Health Resources" [Online]. Available at: https://doi.org/10.2196/13230 [Accessed 20 December 2019].

Trish A., Tynan B., and James R. 2011. "The lived experience of learners' use of new media in distance teaching and Learning." *On the Horizon*, 19(4), pp. 321– 330.

Twenge J. M., n.d. "Egos Inflating Over Time: A Cross-Temporal" [Online]. Available at: https://www.ipearlab.org/media/publications/JoP2008a.pdf [Accessed 5 December 2018].

Tynan C. B. B., 2011. "OERs: new media on the learning landscape." *On the Horizon*, 19(4), pp. 259–267.

Walker J., 2013. "Interview: Humble Bundle On Humble Bundles." Rock Paper Shotgun. Retrieved 2013-08-23.

Wall D., 2002. *Crime and the Internet.* London: Routledge.

Weber N. L., and Pelfrey J., 2014. *Cyberbullying: Causes, Consequences, and Coping Strategies*. Lfb Scholarly Pub Llc, El Paso, Texas.

Wesolowski K., 2018. "Children and Cell Phones: Weighing the Risks and Benefits', Nationwide Children's." [Online]. Available at: https://www.nationwidechildrens.org/family-resources-education/700childrens/2018/10/children-and-cell-phones Accessed [30 November 2019].

Williams Z., 2012. "What is an internet troll?" [Online]. Available at: https://www.theguardian.com/technology/2012/jun/12/what-is-an-internet-troll [Accessed 20 December 2019].

Wright H., 2018. "Negative Effects of Cell Phones on Education" [Online]. Available at: https://www.techwalla.com/articles/negative-effects-of-cell-phones-on-education [Accessed:12 December 2018].

Yee N., 2007. "The psychology of massively multi-user online role-playing games: motivations, emotional investment, relationships and problematic us-age." In Schroder, R., & Axelsson, A.-S. (eds.). *"Avatarsat work and play: collaboration and interaction in sharedvirtual environments."* London: Springer-Verlag.

Yseul Choi G., and Lewallen J., 2017. "Say Instagram, Kids!": Examining Sharenting and Children's Digital Representations on Instagram, *Howard Journal of Communications*.

Ένωση πληροφορικών Ελλάδας, 2006. "Η αξιοποίηση των ΤΠΕ στην Πρωτοβάθμια Εκπαίδευση" [Online]. Available at: https://www.epe.org.gr [Accessed on 23 August 2019].

Κόμης Β., 2004. *Εισαγωγή στις εκπαιδευτικές εφαρμογές των ΤΠΕ*. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Μπαβέλης Α., 2002. "Οι Νέες Τεχνολογίες Στην Εκπαίδευση Προβλήματα Και Προοπτικές." [Online] Available at: http://www.inarcadia.gr/news/arthra/ekpaid/neestexnol.pdf (retrieved on 23 August of 2019).

Μπαμπινιώτης Γ., 2008. *Λεξικό της νέας ελληνικής γλώσσας*. Αθήνα: Κέντρο Λεξικολογίας.

Chapter 15 Digital Marketing

Abstract

Chapter 15 deals with the effects that digital media have on marketing methods. More specifically, a historical overview of Digital Marketing tools is described, from the early email Marketing method to the Websites, the Search Engine Optimization (SEO) and Search Engine Marketing (SEM) procedures, targeted advertisements, Customer Relationship Management (CRM) and contemporary social media Marketing. The last one can connect and interact on a much more personalized and dynamic level by utilizing the social aspect of the web, as it was described in Chapter 4, and therefore, is more thoroughly analyzed. A more practical approach is attempted by presenting an outline of Facebook and Instagram marketing and two social media marketing case studies, Adidas and Nike, to give a more applied overview of social media marketing effectiveness.

15.1 Introduction

The term “marketing” is widely used to describe the process and the communication mechanisms used to carry goods and services from the company to the consumer. It is common to confuse marketing with selling since both concepts are described as a pathway between the company and the customer. The major difference lies in the mentality of the practitioner. While selling is entirely focused on persuading the customer to pay for a product, marketing is more concerned with creating demand for the product by creating new ones, or satisfying the already existing needs of the consumer.

Theodore C. Levitt, a retired professor at Harvard Business School, once said: “Selling concerns itself with the tricks and techniques of getting people to exchange their cash for your product. It is not concerned with the values that the exchange is all about. Moreover, as marketing invariable does, it does not view the entire business process as consisting of a tightly integrated effort to discover, create, arouse, and satisfy customer needs.”

15.2 History

15.2.1 Marketing Through the Centuries

Although “marketing” as a term was first used in the early years of the 20th century, the concept of advertising has existed since ancient times. Historical accounts prove that forms of advertising were already standard practice in ancient Egypt, Greece, Rome, China, and Arabia. From carvings on wood, stone, and metal to signs and papyrus flyers, humans have tried to influence those around them long before the concept of marketing was invented.

In 2000 BC, Egyptians used papyrus to create posters and flyers, carvings on metal plaques, and wall paintings, thus inventing a primal outdoor advertisement. Similar tactics were also used in ancient Greece and Rome, where people carved or painted a common pattern on wood to advertize their products in the outdoor market, i.e., an apple for fruits, a diamond for jewelry or a boot for shoes. Evidence of advertisements has also been found in the ruins of Pompeii. Carved messages written in Latin, graffiti, and illustrations covered the walls of ancient Pompeii, serving as the very first billboard advertisements (Sampson, 1875).

The invention of printing brought forth the first notable innovation in the world of advertising, with the first printed advertisement in England during the 15th century. However, massive changes followed the development of the printing press. The ability to influence the masses was now a phenomenon that influenced politics, daily life, and the whole mentality of the world altogether.

The invention of the radio left another great mark on the marketing history. The oral presentation could be used instead of the commonly written advertisements for the first time, adding an extraordinary dramatic sense to the related products. In the late 19th century and early 20th century, the introduction of television established an utterly new level, as commercials were now transformed and combined with the audio-visual element that television made possible.

Towards the end of the 20th century, the advertising scenery shifted again with the birth of a unique medium, the internet, which was assimilated into the modern society with unprecedented swiftness, immediately becoming an invaluable means of communication and advertising. Moreover, thus came the dawn of the era of digital marketing.

According to the Ohio State University in 1965, marketing is the procedure in a community, with which the structure of demand for economic goods and services is predicted or extended. Accordingly, it is fulfilled by the conception, promotion, exchange, and physical distribution of these goods and services. According to Boone and Kurtz, in 1977, marketing was the development and economic distribution of products and services

to a specified and chosen group of consumers. Later, in 1995, according to Bennett, marketing was the procedure of planning and executing the conception, invoicing, presentation, and distribution of ideas, products and services to develop transactions that fulfill people's and organizations' purposes. Not long ago, in 2015, according to Kotler, marketing was the social procedure with which individuals and organizations acquired what they needed, by creating an exchange with others.

As can be discerned, while marketing is not synonymous with the act of selling, its ultimate goal is to achieve a lucrative transaction, thereby ensuring its effectiveness. In order to be successful, marketing's priority nowadays is to orient itself to consumers' needs and promote those goods that exist to satisfy them.

15.2.2 Inception of Digital Marketing

The evolution of marketing is undoubtedly connected to the advancement of technology. Intermittently, new technologies emerge and are being introduced to the market. Innovative practitioners seize the chance to utilize the newfound invention as a means of advertising, and gradually, the new technology becomes widely adopted and integrated into common marketing procedures.

The printing press, the radio, and the television all constitute decisive milestones in the evolution of marketing, but the actual revolution came with the introduction of the World Wide Web. The internet completely transformed business practice, progressively becoming vital to any business operation. However, marketing is about more than just technology; it is also people oriented. The success of a business is not guaranteed just through internet-based marketing techniques since the customers' point of view should also be considered. Therefore, it is imperative that, while integrating new technologies, the traditional marketing principles are not abandoned.

To survive the competition, advertising and offering their products online is certainly not enough for an online company. Establishing a solid e-brand is a decisive factor for the success of an online business. Moreover, customer loyalty and satisfaction are essential for that to be achieved, just like in traditional business. Several people hesitate to share their personal or credit card information with online companies without a security guarantee. In any case, companies use a unique encryption technology to safely receive information and state their privacy policies to convince the customers that the site is secure. Providing the customer with a positive shopping experience through adequate advertisement, a pleasant digital environment, excellent service, and customer support is fundamental in forging a strong and consequently successful e-brand.

The sales sector has dramatically benefited from the establishment of e-commerce, which allows the consumer to check product availability, compare prices, read reviews, place orders, and pay for products online. However, that does not necessarily entail effortless and smooth selling. The consumers can gather information at a speed and immediacy unforeseen in the traditional market, thus elevating the antagonism and enhancing the necessity for efficient product marketing. Marketers are now confronted with the challenge of presenting their products or companies in a way attractive enough to overcome competition and be distinguished. Furthermore, the fast-paced reality of the internet compels companies to monitor their competitors to be prepared to react at every possible opportunity to gain an advantage in the game of marketing. Consequently, the new marketing policies induced by the digital era are highly demanding but immensely beneficial for a dedicated and influential business.

It is interesting how pricing strategies differ between conventional retail and online shops. The internet allows online companies to avoid operational costs like rent, utilities, equipment and staff salaries, thus offering significantly lower prices. For example, online book and CD prices are 9 to 15 percent lower than in conventional retail stores (Clay, Krishan & Wolff, 2001). On a different note, the use of specialized software enables consumers to compare online prices and check the availability of a product in multiple online firms at

the same time and considering that the web has dismantled the distance barrier, making purchases from any part of the world is a viable possibility. As a result, the target audience is presented with a vast range of buying options.

Nevertheless, it is socking that despite the facilitations above, intended consumers are not constantly searching for the best possible price but often concern themselves with different matters like shipping fees or delivery time over pricing. A study on online shoppers found that 89% of book buyers, 84% of those who buy toys, 81% of music buyers, and 76% of those buying electronic products do not actively search competing sites but purchase from the first site they visit (Baker et al., 2001). Also, in a study of North American consumers, fewer than 10% of online customers aggressively sought for bargain prices; the rest returned to the same site when purchasing rather than searching for the best price (Baker et al., 2001).

15.2.3 The Rise of Digital Marketing in Modern Times

It has been nearly 25 years since the World Wide Web was introduced and triggered the commercial use of the internet. Since then, the widespread use of the internet and digital technologies have dramatically changed the behavior of consumers and simultaneously set a great challenge for marketers (Tajvidi & Karami, 2017). After the launch of Google and the invention of Web 2.0, the new internet age started, and the traditional marketing environment was urged to incorporate new digital techniques, which led to the recognition of digital marketing (García et al., 2019).

Digital marketing can be understood as a transition from the traditional methods of marketing that utilize the internet to carry out marketing activities. AT the same time, the focus is being placed on the consumer rather than on the product. businesses can establish an online presence by integrating digital marketing strategies such as SEM, SEO, affiliate marketing, and content marketing (Gibson, 2018). Furthermore, websites, videos, e-mails, blogs, social media, and mobile apps can be utilized to directly engage consumers anytime and anywhere via their computers, smartphones, or tablets (Kotler et al., 2017).

The rapid growth of Web-based platforms that facilitate online social behavior has significantly modified the nature of human activities, habitats, and interactions. Additionally, real-world social relationships have been migrated to the virtual world, resulting in online communities that bring people together from across the globe. This movement into the digital dimension allows individuals to share knowledge, entertain one another, and promote dialogues among different cultures. From a consumer's perspective, using information communication technologies offers several benefits, including efficiency, convenience, richer and participative information, a broader selection of products, competitive pricing, cost reduction, and product diversity. Online social networking enhances these benefits, as consumers can communicate more proactively. For instance, individuals can seek out others' opinions about specific products through social networking. In doing so, consumers have been shown to value peer judgments more than firm promotions, indicating a shift in the locus of persuasive power.

Today, there are 4.3 billion active internet users worldwide who spend approximately 6 hours and 42 minutes online daily, using (Tajvidi & Karami, 2017) social networks, consuming digital content, and searching for products (Statista, 2019; Tajvidi & Karami, 2017; We Are Social, 2019). Therefore, digital marketing represents a fundamental business tool enabling companies to meet the target audience in the right place and time.

15.3 Digital Marketing Tools

In recent times, Digital Marketing has been deployed using various digital media applications such as:

1. **EWOM** (Electronic Advertising word of mouth) is a highly effective digital marketing tool that bases its operation on the potential of collaborative content production. The most popular tools for that are social networking sites like Facebook, video sharing sites like YouTube, auction sites such as eBay, and reviewing or evaluation sites like Epinions.com.
2. **Blogs:** online journals or diaries hosted on certain websites, including the writer's information or personal issues or comments on issues of broader consumer interest.
3. **Podcasts:** audio files derived from blogs often distributed through digital applications such as Apple's iTunes.
4. **Online (brand) communities:** online communities whose members develop social ties between them based on common interests and expressing admiration for a brand, product, or company. In the international bibliography, three kinds are mentioned: communities exclusively managed by consumers, communities managed by companies where consumers and customers are involved, and those of mixed type commonly managed by businesses and consumers (e.g., Lego).
5. **Virtual reality and online games:** millions of people worldwide participate in online games like Second Life and There.com, where they choose virtual characters and simulate a "normal life." Within this "normal life," human characters consume and interact, and global brands participate in the "game," such as Coca-Cola, Vodafone, IBM, Toyota, Sony, and Adidas.
6. **Email marketing and permission marketing:** two modern forms of electronic correspondence and business communication with potential customers. This communication takes various forms, such as sending offers of new products and services via email or simple newsletters.
7. **Viral marketing (spiral marketing):** advertising content is carefully placed (seeding) at selected sites on the internet and is diffused by consumers to other users. The most common practice is short videos placed on sites like YouTube and viewed by thousands of spectators.
8. **Online and banner ads:** They are the most widespread form of online advertising as they can build awareness and target audiences based on geographic, demographic and behavioral data.
9. **Interactive television (iTV/webTV):** Interactive television offers the opportunity to gather information on the viewers' interests and to send personalized offers or advertising messages.
10. **SEO (search engine optimization):** a technique companies use to ensure their website's presence on the top of the result lists of search engines like Yahoo, Google, etc. Companies are looking for ways to ensure high rankings and the most common method is the "paid search."
11. **Cell phones (smartphones):** they benefit from the wireless broadband Internet Connection and exploit the explosive growth of these new digital channels for marketing purposes.
12. **Social media - social networking websites:** X, Facebook, MySpace, Instagram etc. Ordinary user participation includes discussions on brands, usage, and maintenance of products, advice on effective use of devices, troubleshooting or publishing feedback and reviews, etc.

Emails have been among the first to reach potential customers by sending advertisements, requesting business, or soliciting sales or donations, and introducing email marketing. With the World Wide Web, websites have been rich multimedia content resources aiming to diffuse information related to products or businesses. Search Engines have also been used as parts of a marketing strategy, the so-called Search Engine Marketing (SEM), by intervening in the algorithm that produces the resulting website list. Since the spread of smartphones, mobile marketing has been introduced as a marketing technique focusing disseminating content to mobile audiences via websites, e-mails, SMS, MMS, social media, or other mobile applications. These three digital marketing techniques and online ads are presented in more detail in the following paragraphs.

15.3.1 E-mail Marketing

Wikipedia defines email marketing, as "*a form of direct marketing that uses electronic mail as a means of communicating commercial or fundraising messages to an audience.*" It can be one of the most effective advertising, marketing, and sales tools when designed and implemented correctly. It can also become one of the most cost-efficient means of disseminating large amounts of information to a large audience at a low cost compared to traditional print media advertising and marketing campaigns (Brown, 2007).

Nowadays, everybody has at least one e-mail. With the advance of modern technology (smartphones, tablets, internet, etc.), most people are constantly connected using their mail access daily, both at work and home (Mullen & Daniels, 2009). email marketing allows the dissemination of information instantly and at a global level while it provides the capability to have a close and effective tracking and reporting-feedback system.

Some key areas for e-mail marketing are as follows: Businesses selling products, distributing news, maintaining contact with customers, promoting new business lines, producing and servicing, increasing revenues, announcing special events, offering coupons or discounts to customers, saving money (low advertising costs or limited advertising budget), competing (small businesses) big industry leaders, expanding customer base or reach into new market areas (Brown, 2007).

To use e-mail marketing, a company first needs a database of e-mail addresses. Those can be collected by letting people sign up for a newsletter or by buying a database of e-mail addresses, which is only possible when done according to the law and with the companies' agreement. E-mail marketing is used by 82% of the companies in B2B and B2C combined. Some interesting facts about e-mail marketing are the following:

- For every 1 USD spent, email marketing generates 38 USD in ROI.
- Revenue per e-mail was 0.11 USD in 2014 compared to 0.10 USD in 2013.
- The average order value of e-mail marketing is three times higher than social media's.
- A message via email marketing is five times more likely to be seen than via Facebook.
- E-mail marketing is 40 times more effective at getting new customers than Facebook or X.

Although technology is advancing and new ways of advertising are coming into everyday life, it is more than certain that email marketing is here to stay for the long term. Moreover, it is expected to grow in both frequency and volume. Of course, as a part of the overall marketing domain, it will have to face many challenges that, for sure, will play a significant role in the future.

Better data and personalization are two issues for the future. According to Statista, by2023, there will be an estimated 4.3 billion global email users. Since most users face promotional emails in the same way as spam, future email marketing efforts should try to be more personalized.

It is crucial for companies and commercial enterprises (not only for B2B (Business to Business) but also for B2C (Business to Consumers) to stay on top of their email marketing. Respectively, there are trends in email marketing for 2020:

- **User-generated content is an email-stimulated trend**: describing any content created by the (end) user or, in some cases, the public.
- **Responsive interactivity is a valued functionality**: responsive emails do well on mobile, driving engagement and looking for functional interactivity.
- **Accessible Content, Design, and Code – put email in a Future-proof Mode**: smart devices, speakers and voice assistants are expanding in more and more daily applications. Almost 250 million smart speakers, worldwide were in place in 2020. Thus, email marketers are designing with accessibility in mind.

- **Email Marketing Automation**: email marketing automation is a trend that cannot be changed. The number of workflows will increase daily as companies are using automation in all customer lifecycle stages.

As a marketing method, E-mail Marketing increases brand loyalty, delivers significant Return on Investment (ROI), and is one of the best tools in a marketing strategy, provided that it is appropriately used. No matter how many other innovative digital marketing tactics emerge, email marketing remains one of the best ways to reach and engage the target audience. Email marketing's power lies in its ability to provide businesses of all sizes with an attractive return on investment.

15.3.2 Mobile Marketing

Today's mobile marketing is not only about sending SMS, as in older times, when simple marketing messages were sent to subscribers. Nowadays, mobile marketing mainly occurs in the sphere of smart mobile phones. According to the Mobile Marketing Association, mobile marketing is a set of techniques that allows an organization to communicate and create connections that include interaction through a mobile phone network. According to Dushinski (2021), it is the way that allows businesses to contact consumers through cell phones, as long as they have assured their permission, at the right time and right place, while at the same time, this attempt adds value to the consumers.

Contemporary smartphones have made web searches and shopping easier than ever before, while payments and financial transactions can be fluently carried out with a few touches of the screen. Faster networks, more demanding customers, and small and big companies are and will continue to be the key players of the Web 3.0 marketing landscape described by huge investments, social communities, and activities supported by specific applications that will offer more than only provide information about products, e.g., can show where the nearest shop with the lowest price is where a specific product can be purchased.

According to the Yankee Group, financial transactions reached 1 trillion dollars in 2016. The total number of customers shopping directly from their cell phones in 2012 was 38%. The most popular product categories are movies, music, and games (43%), followed by clothing, shoes and jewelry. Mobile applications adjusted for iPhone and Android devices have been a universal shopping tool providing unique shopping experiences.

Mobile Marketing is an important sector because 25% of searches and 50% of website commercial visits nowadays come from mobile devices. Moreover, smartphone users spend double the time surfing the internet than those who prefer desktops. Commercial application development is also an important part of this type of marketing, as 80% of smartphone users prefer certain apps that effectively combine additional data, such as geolocation, to search for products and make online purchases.

Mobile Marketing considers several variables, such as the mobile potential buyers' diverse personal behavior covering the time space between product searching and purchasing. Usually, 60 seconds and a few clicks should be more than enough to offer the desired user experience, reflected by the design of web pages or applications. Optimized websites for mobile devices and mobile applications should include all basic properties to accomplish the task they have been designed for efficiently. Detailed descriptions of product, pictures, reviews, and locations of shops are the crucial elements of the design.

Among the most widespread and most used tools of mobile marketing are image and text ads while browsing the web with a cell phone. Sending advertising SMS or using QR codes are considered obsolete tools that do not offer users any exceptional content. However, they can still provide access to additional information about the advertisement in print. Optimized web pages or pure applications are now considered the proper media for advertisement where mobile users experience the transition from passive acceptance of

direct advertising to an active one where the customer decides when to download the application to register for sending newsletters, etc.

The most frequently mentioned benefits of mobile marketing are that advertising communication on mobile devices is felt more intensely, more trustworthy, and more positively because users consider their phones a personal issue.

In a global context, mobile marketing is in a continuous state of development and primarily utilizes concise marketing messages on mobile website pages. The cost of advertising in this medium is relatively affordable, and there remains ample room for innovation and the exploration of novel strategies to enhance brand visibility, product promotion, and service marketing.

15.3.3 Search Engine Marketing (SEM) & Search Engine Optimization (SEO)

The online search for products and services mostly occurs through big search engines such as Google or Bing. According to the American Marketing Association, Search Engine Optimization (SEO) is the procedure of developing and marketing a website, which aims to improve the initial ranking of this page in the search results. Appearing high in the search engine results pages (SERPs) is essential for generating traffic to the website and increasing sales. The websites at the top of the list at a search engine query and with higher frequency are more likely to be visited by consumers, as they are deemed more appropriate to their query. Their higher ranking is due to the digital marketing technique of Search Engine Optimization (SEO). For SEO, information like how search engines work and the actual search terms or keywords that people type into search engines when they search for something is really important (Pohjanen, 2019).

When a user searches for something using a search engine machine, several clickable links, the so-called snippets (that can include preview text to establish the webpage's relevance to the search) appear as a result of his request. The ranking of each snippet is determined by a complicated algorithm that includes more than 200 factors, determining if a user will visit that page. A snippet is organic if placed highly at a SERP only due to pure merit, as the traffic sent to a website from a search engine's organic results is free. On the other hand, it is inorganic or sponsored if the organization has paid a fee to gain that placement. A high ranking in the first SERP can reinforce an organization's visibility. This improved visibility in organic search results, along with improved traffic volume and quality of website traffic, is exactly the product of SEO (Gudivada et al., 2015).

While SEO is an organic strategy that achieves its goals without a price, other strategies, such as Search Engine Marketing (SEM) and Search Engine Advertising (SEA), require payment to function. SEM involves buying traffic using paid ads, while SEA requires a bid for higher ad rankings (Pohjanen, 2019).

In order to succeed in having a profitable outcome, search engine machines such as Google have developed tools, to assist marketers in developing strategies and campaigns that tend to develop SEM and make the results of SEM countable. Tools such as Google AdWords (explained later) or Word Tracker have been developed to form lists with keywords that users search for to buy and include in businesses' websites, improving their page's ranking in the results list.

Specialized online marketers support the idea that businesses should invest in SEO to succeed in a long term, sustainable impact on the brand's name. Eventually, marketing's innovation and turn to digital form has also created a theoretical evolution in digital marketing, which is Search Engine Marketing Management, which is about managing all the above SEM functions.

Search engine optimization techniques can be divided into "White Hat SEO" and "Black Hat SEO." A further division is between "On Page SEO" and "Off Page SEO."

15.3.3.1 Black-Hat Search Engine Optimization

Black Hat SEO refers to techniques that improve a website's non-sponsored search engine visibility by affecting only the search engine's quality ranking process. Search engines are typically against black hat SEO and claim that manipulation of search engine results negatively affects the consumers' satisfaction. In addition, it is common for websites to be removed from the organic list if their Black Hat SEO activities are discovered. Search engines publish guidelines about undesired practices. The SEO techniques that do not comply with the search engine's guidelines are considered Black Hat (while the ones that do are considered White Hat). Businesses are highly advised to use White Hat SEO techniques to provide the best possible content for the consumers (Gudivada et al., 2015).

White hat SEO improves the site content, increasing visitor satisfaction and making the site more relevant, while black hat SEO only improves the ranking of a site among search results without improving its quality. The black hat strategy is designed to "trick" search engines to improve a website's position in organic search results (Gudivada et al., 2015).

More specifically, Black Hat SEO, also known as Spamdexing, refers to deceitful practices meant to achieve top placement in the first Search Engine Results Page (SERP). This is achieved by building webpages that trick search-engine algorithms and, therefore, artificially boost the page's ranking. Even a page irrelevant to the search word or phrase can be placed highly. The most common black hat strategies are the following:

Automatic page generation

Webpages are generated through scripts using algorithms that disperse random text with sought-out keywords. Machine-translated text may also be present on the page that a human has not reviewed and edited. Also, new text may appear that complicates existing text using synonyms. Content taken word for word from more esteemed sites is also used without the concern of relevance or copyright violation. Webpages can be automatically generated from snippets of either search results or web pages that contain desired keywords. This type of page usually includes only the generated snippets without any real content.

Redirecting

URL redirecting, which regards sending the user to a different URL than the one they requested, can be useful and malicious. For example, it can aid a website move to a new address. However, it can also show the user different web pages for the same URL. This way, a user may click on a page for children's stories and be redirected to a page with pornographic images, for instance.

Cloaking

Bots and users see the same page in different ways. For example, bots see content with the desired keywords and follow approved guidelines, while users see content that is often malicious or undesirable. Some hackers use cloaking to keep the webmaster from detecting their work.

Link Spam

Link spam includes any sort of link in a webpage that exists only to increase its ranking, links being outgoing or incoming. The purchase and sale of links, the excessive exchange of links, the mutual linkage of partner pages, the acquisition of keyword-rich anchor text links through article marketing, and the insertion of comment links in blog postings are all considered link spam schemes.

Hidden Text and Links

Excessive keywords are hidden from a user but visible to search engines. Methods to hide text include placing text behind images, setting the text font size to zero, and using cascading style sheets to position text offscreen.

Doorway Pages

Doorway pages dispose of content that has low quality but is optimized to rank high for specific keywords. They are meant to channel users to a single page, usually one they did not select.

Embedded Malicious Behavior

When the user clicks on a link, a malicious action, like the installing advertisements, viruses, malware, trojans, and spyware on the user's computer, occurs. The user might also click on a specific button and make another unwanted link on the same page to activate.

User-Generated Spam

Some website users can produce comment spam, namely comments that include advertisements and links to irrelevant pages. They can also create poor-quality links to their competitors' websites so that the latter get search-engine penalties, such as a lower ranking in the SERPs or removal from the index. Backlink blasting, a software-driven link scheme that produces thousands of backlinks (external links pointing to the webpage), plays a vital role in this behavior. Both comment spam and backlink blasting are used so often that Google has devised a tool, Disavow, to tackle them (Gudivada et al., 2015).

Most of these methods are aimed at providing certain content only to the spiders, while actual users see completely different content.

15.3.3.2 White-Hat Search Engine Optimization

Conversely, white hat SEO can improve a website's visibility by making the website more relevant for consumers. White hat strategies conform to the guidelines posed by search engine companies. Additionally, search engine companies provide starter guides to website developers on indexing documents and processing queries. Based on these resources, businesses can develop successful SEO strategies. (Gudivada et al., 2015). White-hat SEO has two main categories: on-page and off-page optimization.

On-page optimization deals with website structure and content and comprises various practices. First, a good SEO strategy includes choosing effective keywords or key phrases optimizing the site. Consumers can find the most informative or elegantly designed site with them. The SEO process starts with developing a list of keywords or key phrases that will be related to each website, and relevant to the audience's interests and needs. Good keywords commonly recommended by SEO professionals include, for example, words and phrases naming the problems or needs that the organization resolves (Pohjanen, 2019).

The words should be chosen to create precise, pertinent, helpful, and legitimate content. Natural and authentic word phrases, both short and long, should be included in the content to help readers understand the page's topic. The differences in user's vocabularies should be considered in a SEO strategy, as these differences must be accommodated through a mix of theme words and phrases. Content should look credible, and keywords should be spread across the entire page. Keywords should be used in HTML tags (title, meta descriptions, and headings) (Gudivada et al., 2015).

To continue, short but substantial URLs are better for webpages, and natural keywords shape the foundation for URL text. The same applies to anchor text. Anchor text should capture the topic of the page that the anchor link points to. Search engines also use refined indexing algorithms like latent semantic indexing (LSI). LSI calculates whether a page is relevant based on keywords and the general topic of the page. This means the sole focus on a specific keyword does not guarantee that the webpage will land highly on a SERP. Content like a picture, an audio, or a video can be part of SEO and can be described with the alt attribute, which is the HTML attribute used in HTML and XHTML documents to specify alternative text. Furthermore, the title tag must reveal the topic of the page. Every page must have its own distinguishable and suitable title.

Page content must be demonstrated in the snippet's first line. HTML5 semantic elements and heading tags should reflect the page content's hierarchical organization. The meta description tag's keywords and phrases can be used to generate snippets.

Moreover, to achieve a higher ranking in a navigational search, businesses should include text in the webpage title, body, first four heading levels, and the anchor text of inbound links and their number. Also, a page that describes the site's privacy policy, such as what personal information the site collects and its use and distribution, should be included on every website. The privacy policy can reflect that the website is managed professionally, and some search engines consider websites that include it to be more trustworthy.

In addition, web servers return a 404 page when the search engine cannot find the requested webpage. This way, users are kept on the site, and their search experience can be enhanced. Customization might involve adding a pointer to the site's homepage or providing links to other site content related to the search (Gudivada et al., 2015).

It is important to mention that Google appreciates content and websites with better quality content, as they prevail over weaker websites. A website should be written and structured for people, rather for search engines. Search engines also value the elegance and accessibility of one's writing. Poor content and low writing quality, frustrate the users and are badly received by search engines, as search-engine spiders understand language. Users' attention will be captured by useful and informative content. Additionally, it is now easier for search engines to discover duplicate content. Website owners who publish content identical to what has already been published on the web are punished. Lastly, a frequently updated website can score a higher ranking on a SERP (Gudivada et al., 2015).

Off-page optimization deals with the best practices for integrating inbound and outbound external links. A carefully designed directory structure for website content is necessary for site maintenance and allows bots to traverse a website and index its content. Website navigation structures include breadcrumbs and sitemaps, robot meta tags, text links, and backlinks (Gudivada et al., 2015). Breadcrumbs indicate the user's navigation trail on a website and are used to improve site usability. If the breadcrumb information is available as HTML markup in the body of a webpage, it can be included in SERPs. Navigation should always ensure that it does not create distinct URLs for the same content in order for websites to avoid penalties like reduced ranking. Sitemaps are a crucial element of well-designed websites as they represent the website's structure, which enables site navigation. A sitemap should be in both XML format for the search engine and plain text format for the user. The XML sitemap version should contain information about every website page, including the URL, last modified date, page-update frequency, and the URL's priority value relative to the site's other webpage URLs. The most important URLs will have priority 1 (highest), with lower values indicating decreased importance. Search engines use these values to determine the web page's indexing order. Because a search engine might index only some pages, the values can promote the most important pages. Webmasters typically submit the XML sitemap version to the search engine because it is more likely to result in complete site indexing.

The robot's meta tag specifies whether or not a web crawler can index a page or whether or not it can traverse the links on a page. With bans like the "no archive directive" and "the no snippet directive," a page-specific approach can control how search results index individual pages and show them to users. If the site lacks a map, text links are important in facilitating web crawlers to navigate through pages. Crawlers also index text links (indexing information that search engines use), even though not all pages are indexed.

Backlinks refer to links back to another website. If a website has many backlinks, search engine algorithms evaluate it positively, and the more backlinks a website has, the more popular it can get. While backlinks help achieve a higher SERP ranking, the quality of the links is critical. Link spam and other black-hat methods can artificially boost backlinks. If the artificial links cannot be avoided, the rel=nofollow attribute can

be used in the HTML anchor element to inform search engines that they should turn down the link when calculating the rank of the page the link points to. The external links that a page points to should point to trusted and authoritative sites. Differently, penalties can be imposed for the external links on that page, and even the entire site's risks can be removed from the search engine's index (Gudivada et al., 2015).

15.3.4 Online Ads: The Case of Google AdWords and Facebook Social Ads

Advertising delivered over the Internet has become a significant source of revenue for web-based businesses (Anon, 2014). Following Schumpeter, internet-based advertising is a "*gale of creative destruction*" sweeping across the advertising and media landscape (Schumpeter, 1942).

The birth of online advertising dates back to 1994, when HotWired, a web magazine, sold a banner ad to AT&T and displayed the ad on their webpage. The ad was sold based on the number of individuals who saw it, which was the model followed by most traditional media for branding advertisements. The "*cost per mille,*" often seen as "CPM," which is advertising terminology for the cost per 1,000 viewers of an ad, was the main trait of digital advertising. It was only in 1996 that this norm changed. Procter & Gamble negotiated a deal with *Yahoo!* that compensated the portal only if users we clicked on the ad. This was the web version of paying for direct response commonly used by advertisers for mail and telephone solicitations, commonly known as "*CPC*" or "*cost per click.*" As of 2008, most "display ads" on websites—the ads that look like those in newspapers and magazines—were still sold based on thousands of views (Anon, 2014).

15.3.4.1 Google AdWords

Google AdWords is an online advertising platform developed by Google, where advertisers pay to display brief advertisements, service offerings, product listings, and video content and generate mobile application installs within the Google ad network to web users (Support.google.com, 2018). It was introduced in 2000, and since then, many changes have been made to its features and branding.

Firstly, in 2018, Google AdWords went through an overall rebranding. Its name changed from Google AdWords to Google Ads. Secondly, the logo and the internal interface changed dramatically to comply more with the market. However, the most significant change was how ads were displayed and put in Google's search engine.

In its initial steps, AdWords advertisers paid monthly services in Google to set up their campaigns. Because of the controversy involving this practice and in order to help smaller-scale businesses who wanted to orchestrate their campaigns on their own, Google launched the AdWord self-service program and, in 2005, Google Advertising Professional (GAP) Program to certify individuals and companies who completed AdWords training and passed an exam.

Google Ads' system is based partly on cookies and keywords determined by advertisers. Google uses these characteristics to place advertising copies on pages where they think it might be relevant. Advertisers pay when users divert their browsing to click on the advertising copy. Partner websites receive a portion of the generated income (Support.google.com, 2018).

The Google Ads program includes local, national, and international distribution. Google's text advertisements are short, consisting of three headlines with a maximum of 30 characters each, two descriptions with a maximum of 90 characters, and a display of two URLs of 15 characters each. These are called AdWords expanded text Ads. These mimic what the average search result looks like on Google. Image ads can be one of the several standardized sizes designated by the Interactive Advertising Bureau (IAB). In May 2016, Google announced its reformatting of ads to help consumers and advertisers succeed in a mobile-first world. The new format, called Expanded Text Ads, allows 23% more text. This new format is available on both the Google Search Network and the Google Display Network. It features two headlines with 30 characters

each, replacing the standard of a single headline with 30 characters. The display URL has been replaced with two 15-character paths, not including the root domain.

Google Ads has evolved into Google's primary source of revenue, contributing to Google's total advertising revenues of US$95.4 billion in 2017. Google Ads offers services under a pay-per-click (PPC) pricing model. Although an advanced bidding strategy can automatically reach a predefined cost-per-acquisition (CPA), this should not be confused with a true CPA pricing model (Support.google.com, 2018).

According to a survey conducted worldwide by Statista from 2001 to 2018, advertising accounted for most of Google's total revenue in 2018, which amounted to 136.2 billion US dollars. In the most recent fiscal period, advertising revenue through Google Sites comprised 70.9 percent of the company's revenues. These figures are unsurprising as Google accounts for most of the online and mobile search market worldwide. As of January 2019, Google was responsible for almost 90 percent of global desktop search traffic. The company holds a market share of around 90 percent in a wide range of digital markets, with minor to no domestic competition (Statista, 2019).

15.3.4.2 Facebook Social Ads

In November 2006, Facebook was the first social media to unveil official ads in its content by launching Facebook Ads, an ad system for businesses to connect with users and target advertising to the exact audiences they want. Through Facebook Ads, these users can learn about new businesses, brands, and products through the trusted referrals of their friends who interact directly with brands easily and build a new relationship between consumer and producer.

According to the press release of Facebook over the event that launched its initiative, businesses now not only have the opportunity to create a page to share their brand identity exactly as they would like, but they also have the interface to gather insights into people's activities that concern marketers significantly (About Facebook, 2006).

In other words, what Mark Zuckerberg and his colleagues introduced with this new feature is the vast adoption of social ads in "every day" digital marketing. Social advertising relies on social information or networks to generate, target, and deliver marketing communications. Many current examples of social advertising use a particular interpretation service to collect social information, establish and maintain relationships with consumers, and deliver communications. The procedure involves targeting and presenting ads based on relationships articulated on those same services. Social advertising can be part of a broader social media marketing strategy to connect with consumers (Tucker, 2012).

Facebook's ad system serves Social Ads that combine social actions from your friends—such as a product purchase or restaurant review—with an advertiser's message. This enables advertisers to deliver more tailored and relevant ads to Facebook users that now include information from their friends so they can make more informed decisions. No personally identifiable information is shared with an advertiser in creating a Social Ad. Social Ads can appear within a user's News Feed as sponsored content or in the ad space along the left side of the site. Facebook Insights gives access to data on activity, fan demographics, ad performance, and trends that better equip marketers to improve custom content on Facebook and adjust ad targeting. Facebook Insights is a free service for all Facebook Pages and Social Ads.

Facebook earned $16.6 billion in ad revenue for the second quarter of 2019, a 28% increase year-over-year. Facebook CFO David Wehner said the strongest ad growth on a regional basis belonged to North America and Asia-Pacific, both up 30%. The company's total revenue for the quarter was 16.9 billion, more than three times what it has to pay as part of its settlement with the FTC over privacy violations (Gesenhues & Gesenhues, 2019).

Instagram is not examined separately as a social network involved with social ads because it belongs to "The Facebook" association. The same holds for WhatsApp and other popular social media platforms. Socials ads work within Facebook's sphere almost the same way as on Facebook. Nevertheless, according to a report by eMarketer, Instagram had 713.9 million monthly active users in 2018, and its ad revenue was about 9 billion. eMarketer expects Instagram's growth to accelerate over the next few years. It is estimated that this number will grow to 989.1 million by 2022 (Market Realist, 2019).

15.4 Social Media Marketing

The market dynamics have been markedly changed by the emergence of social networking websites and social media as means of communication (Alves et al., 2016; Kaplan & Haenlein, 2010). Social media is characterized as internet-based applications facilitating the creation of user-generated content, which is exchanged among participants of virtual communities and networks. Weinberg (2009) defines social media as "the sharing of information, experiences and perspectives throughout community-oriented websites."

Over the last two decades, the popularity of social media skyrocketed and gave rise to communication in the virtual world. The way people interact was reshaped, revolutionizing communication between marketers and customers. The implementation of social media into business strategy became essential, and therefore, social media marketing as a marketing discipline emerged (Alves et al., 2016; Patel, 2017).

Social media marketing constitutes the fundamental component in today's marketing strategy, incorporating social media into establishing a company's brand image and reputation among its potential clients (Felix et al., 2017). Marketers utilize social media channels such as social networking sites (Facebook, Instagram, LinkedIn), microblogs (X), or content communities (YouTube, Flickr) to design, communicate, and share content that generates additional value for the organization (Alves et al., 2016; SI, 2015; Tuten & Mintu-Wimsatt, 2018). However, designing a suitable social media marketing strategy requires analyzing and understanding of the distinctive features of social media. Zhu and Chen (2015) divided social media into two types based on the nature of connection. Firstly, profile-based social media sites such as Facebook, X, or LinkedIn are where people connect with other users mainly due to interest in the other users' profiles. Secondly, content-based social media such as Instagram, Pinterest, or YouTube, where the posted content represents an integral part of communication. Therefore, marketers must identify and understand the purpose of each social media if they want to produce an adequate social media campaign that will be in accord with the company's overall marketing efforts.

15.4.1 Social Media as Marketplace

From the marketing standpoint, social media represent perfect platforms with hidden business potential. Many consumers are in the same place simultaneously, and the possibility of catching their attention by promoting a product there is incredibly high. It has already been proven that "Social media users are 47% more likely to spend money on clothing, shoes and accessories" (Quintana, 2013).

Social media allows companies to keep their customers close and build long-term relationships with them. The way to gain loyal customers is simply creating an account of a company with as many followers as possible. Users following a specific brand are influenced daily by its advertisements, special offers, and marketing tricks, putting the brand in a desirable position. Willingness to buy a product of a specific brand then automatically increases. Statistical data collected by Quintana (2013) says that "*61% of Twitter users, and 51% of Facebook users, are more likely to buy brands they follow online.*"

Equally important for online marketing is a personal factor. In history, this concept was described as word of mouth, but in an online world, it is simply sharing feedback on products and services. People tend to

trust each other, and therefore a good recommendation of a product made by a friend or acquaintance can be as valuable as good advertising. The truth is that "50% of social media users under 35 follow their online friend's products and service recommendations" (Quintana, 2013).

Social media can also be understood as a marketplace where users are potential customers and companies are businessmen trying to boost their brand image by creating and presenting marketing strategies.

15.4.2 Marketing through Social Networks

15.4.2.1 Customers vs. Companies

Social networks are very useful marketing tools for different purposes. Large companies use these sites to gain information from their target audience to understand their feelings and satisfaction with their products. These sites are also handy tools for gaining information about the competitors. Small companies are using social networks to promote their brand. Networks allow several people to connect and meet new customers that may benefit the companies. Especially connecting with different people is an excellent way to create new contacts and, thus, new customers.

A considerable advantage of the marketing used on social networks is that the sites allow selling the services to a large market without the cost. Companies can reach a mass market free of charge every day. For instance, the most popular social networking site, Facebook, offers free sections where people can post, for example, items for sale, available services, etc. Companies can place their advertisement regarding their products and services as well. SNSs are also beneficial for companies who want to create e-mail lists, send coupons or advertisements through mail. Companies can post their newsletters or bulletins on their social networking site and thus encourage people to sign up. Many companies can increase their mailing list thanks to SNSs.

Marketers also monitor social networks; discovering how people view their brands. They can also monitor the competitors and how their customers see the competitors. The feedback from the customers allows marketers to understand if they are targeting the right market, what these people like/dislike about their products and services, and what should be changed and improved to avoid a mistake. This process will be analyzed later in the chapter.

15.4.2.2 Communication

Communication in the world of traditional marketing has mostly a one-way character. The company that presents some brand or product uses agents that transmit a message about the product to the audience. It is expected for the audience to respond to the message by their purchasing behavior. These are templates and customs of traditional marketing communications, which are valid only very restricted or not at all in the social network environment. Social networks as a communication platform are, from the beginning, based on two-way communication. This means that if we constantly share something with our audience and do not consider the feedback, these effective communication tools may have the opposite results (Janouch, 2010).

15.4.2.3 Trustworthiness

Social media is becoming more and more important for the development of business reputation and branding. The internet and the social media, that are changing consumers' behaviors and their decisions immediately.

Social media is rapidly growing in terms of trustworthiness. Even though information from traditional media was considered earlier to be more trustworthy, social media is quickly taking over as the best way to exchange ideas and start discussions.

A study by ING in 2012, concerning social media on financial decisions showed that social networks lead to changes in consumer behavior. Around 23% of the respondents said that posts published in SNSs can change their opinion about a financial situation both positively and negatively.

Another benefit to businesses using social networking sites is contacting the youth. Even though more and more people who are 65+ years old are using these platforms, the majority of the users are still young. Young people are impacted much more because they use social networks often and trust them more than people who grew up using only traditional media. This is an excellent opportunity for businesses to positively impact young users through social networks and keep them as customers for a long period.

15.4.2.4 Targeting

By viewing users' profiles, marketers and companies are able to gain useful information about their potential customers. They can gather demographic and psychographic information, thus better identify potential customers who fit into their target market. Finding this information is usually time-consuming and can also be expensive. Some social networks allow users to create specific groups according to the topics they are interested in. It can be a very helpful tool for marketers to find the required information regarding their target market, and their competitors in one place.

Hypertargeting is the ability of social networking sites to target ads based on very specific criteria. Outsourcers can target ads to potential buyers based on age, gender, location, education, employment status and hobbies. For example, suppose a company's product is designed for men in the city of Brighton, Great Britain, who are 40-55 years old, and interested in golf. In that case, a campaign can be deployed to target profiles of users meeting these criteria. Eventually, fewer resources are used, and the communication message can be received only those with a genuine interest.

Hypertargeting is easy to manage thanks to the information that users share on their social network profiles. People show their presence, express their identity, and emotionally connect with their friends, uncovering enormous demographic and psychographic information. The standard is to share sex, date of birth, city of birth, education and employer information, marital status, etc. Sharing user's political preferences, religion, hobbies, favorite artists, or books is not unusual. All this information makes hypertargeting easier. Ultimately, advertising campaigns can reach new levels of precision and efficiency by using data mining techniques to tailor users' profiles. By using hypertargeting, the advertisers can skip some segments of the audience, in whose case the probability of purchase is zero or very low and thus focus on the advert to the buyers with a higher probability (Janouch, 2010).

15.4.3 Social Media Marketing Across Platforms

15.4.3.1 Facebook

According to Dunay and Krueger (2010), it has been asserted that if Facebook were treated as a nation, it would rank as the sixth most populous in the world. This presents a unique and highly advantageous marketing prospect, as companies have the ability to effectively reach and showcase their offerings to a vast audience. Facebook is an attractive marketplace, because it is an affordable space with many potential customers and all-important information companies need to know about them. It enables registered users to create their own (personal or business) profiles. Additionally, users can upload different content, such as photos or videos. Another feature of Facebook is the messaging service; users can send messages and communicate with other instances worldwide. Facebook is available in 37 different languages and hence offers its service globally (Dean & Rouse, 2014).

On top of that, Facebook offers diverse features that are related to producing UGC on a direct basis. For instance, Facebook offers a "Marketplace," where users can react or post to advertise; it also offers "Groups" and "Events" where users can either talk about diverse topics of their interest or post a specific event and invite and publicize it (Dean & Rouse, 2014).

Generally speaking, each user's profile is made up of different components. Most noticeable is the so-called "wall", which can be found in every profile, irrespective of whether it is a private or a professional profile. This wall can be viewed as an online pin board, where other users can leave messages, meaning content in different forms, as has already been described (Dean & Rouse, 2014). Simultaneously, each user can make and use online photo albums, which can be managed by uploading pictures from the person's computer or directly to smart device (Dean & Rouse, 2014). Other users can then comment on these pictures, depending on the individual privacy adjustments. The last important component that should be mentioned to get a comprehensive understanding of what Facebook is refers to something that can be understood as microblogging. Microblogging is a combination of blogging and instant messaging that allows users to create a short message posted on their profile. Websites allow these messages to be delivered on cell phones, which allows microblogging to provide a quick way to communicate with a group of people" (Nations, 2014). In terms of Facebook, this microblogging feature is labeled as "status updates" (Dean & Rouse, 2014).

As a result, Facebook serves as a social media podium with diverse opportunities in terms of usage. The following subsections will be discussed which factors an organization has to consider before engaging in Facebook, how a business can use its tools to its advantage and which challenges an organization may encounter.

Creating a Facebook page is the easiest way for a company to start marketing on this platform. It is also a great benefit because it is for free and allows businesses to introduce themselves to users and integrate with them. First, a Facebook page includes a cover photo, which should match the company's activities. Therefore, choosing a company logo is the most effective way to attract users. Then, the company can share general information about itself in the "About" section. Moreover, it can also publish contact information there. To get in touch with the customers, a company can post photos or videos on the wall representing a new collection, special prices, or interesting facts connected to its activity. Latest surveys show that "videos now lead in terms of organic reach. Between October 2014 and February 2015, videos received organic reach of 8.71%, compared to a reach of 5.77% for text-only status" (DeMers, 2015).

To gain customer feedback, a company can post a status with a specific question on the customers or use a questionnaire. However, it is important to mention that communication with users is supposed to be loose since Facebook is a social media where people prefer to spend their free time, not do business.

Once a company has established its page, it can use it in many ways. A very useful trick is to host a contest where users can win a company product or a service (Baldassarre, 2015). Facebook now allows creating a contest without using any third-party application, which is easier for companies than ever before. Furthermore, it will certainly increase awareness about the company's brand.

Advertisements on Facebook bring along many benefits for a company. First, Facebook includes personal information about millions of its users, which puts companies in a great position to target their customers. Targeting can be done according to relevant information such as location, marital status, age, education, or interest. Additionally, Facebook allows companies to upload a mailing list of customers with whom they already have a relationship, so these people are automatically added to the target group. Furthermore, it is possible to customize advertising for a specific demographic group. It means that a company selling T-shirts with zodiac signs ensures that advertising for people born in December will promote the Sagittarius sign to catch their attention.

Another benefit of Facebook advertising is choosing placement according to the company's preference. Three potential placements include desktop newsfeed, mobile newsfeed, and desktop right column. All three options will be used If a company does not set a preference, (DeMers, 2015).

The budgeting of Facebook ads is based on a per-click or a per- impression basis. It depends on whether the company wants to pay when users click on the ad, or when it is shown. Nevertheless, companies may find it helpful to set a daily advertising budget, making it easy to control the costs.

From what has been stated above, Facebook has the potential to offer many opportunities in the field of Digital Marketing. As stated earlier, the first opportunity can be derived from having a Facebook page as a business, meaning that an organization creates its profile. These pages are similar to the common user profiles, just differentiating in how those pages represent the specific company and not a single individual (Stay, 2008; MaxFusion Media, 2014). Through such a Facebook page, a business represents its brand and can attract users interested in the company's products or services. Interested users can become "fans," which means that the user is following the businesses' Facebook activities. The more fans a business has, the more people will notice the interaction and this can, in the best case, lead to more fans, which leads to a higher spread of your brand representation throughout Facebook (Stay, 2008). Hence, the more often a fan shares content provided by a business, the higher the potential customer reach. The term "share" can be defined as "The practice of sharing content from a website on a social media site or application" (Oxford University Press, 2014). Consequently, if a business provides information via its Facebook page, the users can easily access it, leading to higher popularity (MaxFusion Media, 2014). However, it has to be kept in mind that providing information on Facebook also requires regular updates based on the constant consumption of the businesses' information by its followers (MaxFusion Media, 2014). This can be related to the notion of the customer as the center of attention, providing sufficient up-to-date content that can lead to an even higher spread of your business awareness (Beal, 2014; Bosari, 2012; Stay, 2008).

An additional feature may be using "groups" on Facebook. This feature does not include the "fan" option, but since the whole idea of Web 2.0. is the customer generated content, a group discussing information related to a specific business can add value regarding business awareness (Stay, 2008; Beal, 2014).

Next, there is the option of using Facebook's business advertisement option. Using this opportunity can enable an organization to attract more potential customers, referring to consumer targeting (MaxFusion Media, 2014; PsPrint, 2013). Since every business must manage and maintain its Facebook appearance, it offers the opportunity to decide on specific target groups directly, based on factors which a company must define beforehand (see also chapter: Facebook for Businesses – Important Factors for Consideration); for instance, based on age or location (MaxFusion Media, 2014). Consequently, the businesses' advertisement effectiveness can be enhanced by appropriate targeting.

Another opportunity is to link a business's traditional website to the Facebook page; the direct linkage enables a firm to circulate content published on the business website directly via Facebook. In turn, all content published on the Facebook page can also be shown on the business website. This boosts traffic to the company's content (MaxFusion Media; Stay, 2008). The word traffic can be understood as "the amount of data moving between computers or systems at a particular time" (Cambridge University Press, 2014), which, consequently, means the more traffic, the better for the company.

Because Facebook has drastically invested in digital marketing, it also allows businesses to install different applications on its page. These can be free or paid apps like X, YouTube, or Flickr. Installing applications like this improves the organizations' overall social media appearance and advertisements (Max Fusion Media, 2014; PsPrint, 2013).

Another opportunity to ensure customers' attention is to custom design the company's Facebook page. Facebook enables organizations to individually design welcome pages, allowing the businesses to post all kinds

of content, for example, videos or pictures. This is associated with successfully keeping the customers' attention and interest since the customers are thought of as being curious about the different contents (MaxFusion Media, 2014). Therefore, the custom-designed Facebook welcome page can trigger customers' attention.

Facebook also offers the opportunity to enhance business exposure by allowing its users to comment, like, and share different content, which in the best scenario, has been uploaded by the business (Max Fusion Media, 2014; PsPrint, 2013). As long as Facebook fans of a specific business keep on discussing a business's information, business exposure will be enlarged.

Since the most significant opportunities offered by Facebook seem to have been highlighted by now, it becomes evident that the major strength of Facebook for businesses has to do with increasing business awareness and related brand loyalty (PsPrint, 2013), which can in the end lead to increases in sales (Stelzner, 2012).

Facebook enables businesses to promote their services or products, and because it is an interactive platform, fans or users also have the chance to propose criticism to a specific product or service, for instance, which the business can use to improve that product or service (Max Fusion Media, 2014; PsPrint, 2013). On top of that, Facebook, of course, helps to attract and gain new or more customers. All in all, it is a phenomenal social media tool for marketing; consequently, most companies have been using it for marketing purposes. Some examples are given below.

Disney

Disney Parks and Make a Wish Foundation have a long-lasting partnership. Therefore, Disney devised a simple idea involving the Make a Wish Foundation. The idea was that for every photo displaying Mickey Mouse ears and having the hashtag "#ShareYourEars" uploaded on Facebook, Instagram or X, Disney would donate $5 to Make a Wish. The campaign was really successful, and Disney donated $2 million. This proves that marketing does not only have to be about the brand itself. People appreciate when a genuine value is provided by the brand, in this case, a charitable donation.

Shutterfly

The power of free things should not be belittled, as many companies sometimes come up with completely free offer. The company Shutterfly is one of these companies that specialize in products that have been modified by digital photography. An example of their products is a personalized photobook with your combined Instagram photographs.

To increase their sales, Shutterfly started an advertising campaign that stated that one would get a free ceramic mug with any motive they would choose. They wanted to target mothers with kids at home for this campaign and together with Facebook's feature Offer Claims, the company could spread this campaign so quickly that it had 16,000 claims in 3 days. However, giving away 16,000 mugs was to lure customers in purchasing more items from their store and so they did; the result of the campaign generated 8,000 purchases of different items, which in the end gave them the initial investment of the cups back 11 times over.

Oreo

Oreo has a Facebook fan page that has become viral due to a campaign where they had 100 Facebook posts in 100 days promotion to celebrate their 100th birthday. This turned trending news into treats. Because of this, they increased their fans to over 1 million, and their Facebook engagement went up by 195%. Many of their posts were shared over 1,000 times.

Pringles

Pringles knew that the Facebook audience would favorably react to comedy, so Pringles used funny videos to market Pringles. They would have people singing funny songs or other videos with props in a way that would be funny to people watching them. This was good for Pringles as Pringles knew that people would refer other Facebook fans to the page for the videos, thus being introduced to Pringles snacks.

Adidas

Adidas has a fan page on Facebook and has gained many fans by running a contest with an all-expenses paid house party for a lucky winner. The contest was promoted before, during, and even after the contest. Videos of the winners' house party were even shown, which was shared on Facebook so that people could see the party. This was well received by fans of the Adidas fan page.

Red Bull

Red Bull sees itself as a lifestyle rather than a simple caffeinated drink. They do not post Red Bull can images on their Facebook page; instead, they post images of extreme sports and athletes. This is to look like a lifestyle choice. They get many likes just from amazing images of athletes in action and extreme sports as they happen in the images.

IKEA

Ikea has separate pages its various markets across countries like the UK, USA, and Canada. However, the customer engagement strategies employed by the company exhibit remarkable consistency across these markets. These strategies primarily involve sharing updates featuring visually appealing room displays furnished with Ikea furniture and accessories. The social team also includes links to photo albums, videos, and questions used to interact with the fans of the IKEA fan page.

H&**M**

H&M, a clothing retail giant posts several updates on weekdays, but fewer on weekends. They interact with their fans and have promotions that differ from many other promotions. The difference in the promotions is that people are to submit photos of themselves rather than the usual likes, or retweets on X. They even have an exclusive "Enjoy an exclusive front row seat" award for a fall fashion award show on Facebook.

15.4.3.2 Instagram

Instagram is a mobile, desktop, and internet-based photo sharing application and service that allows users to publicly or privately share pictures and videos. It was created in 2010, and today, it belongs to the public's favorite social media, reaching 700 million active users in April 2017 (Constine, 2017).

The main idea of Instagram is to share photos, live videos, or Instagram stories with other followers. Additionally, users can edit photos using a variety of filters, set a specific location indicating where the photo was taken and add descriptions in the form of hashtags. Users can also use the Explore tab, which "displays popular photos, photos taken at nearby locations, and others", this way they find new accounts which may match their interests and decide to follow these accounts (Constine & Josh, 2012). Communication is also possible through Instagram chat. Furthermore, users can link their Instagram account with other social media such as Facebook.

With over than 40 billion images shared and over than 1 billion monthly active users, Instagram generates an average of 80 million photos per day. The mobile-based photo- and video-sharing social network has created a community among users around the world. The platform has grown significantly in its user base and almost every demographic group. Although Instagram started as a photo-sharing app, users may publish everything from videos to graphics to animated GIFs.

Instagram is a unique social networking platform where the photo is the basic unit of interest. Therefore, building a marketing strategy based only on photo sharing may seem a little strange. Nevertheless, in the beginning, what may seem like a disadvantage can be a powerful weapon while using the power of visual storytelling. Following this approach, Instagram became a favorite social media platform for marketing, and many marketing techniques were developed here. As people join Instagram in droves, brands have a unique opportunity for engagement with their fans: Instagram posts generate a per-follower engagement rate of 4.21%, 58 times more engagement per follower than Facebook and 120 times more than X. Engagement is the greatest advantage of Instagram over other social networks, as people surf the internet more often through their cell phones than their desktops.

The first step is the creation of an Instagram Account, where a company can briefly describe its activities. Then another goal is to gain as many followers as possible. To do this, it is advised to use an Instagram tab on the post on Facebook or share a link to the company's homepage in the bio. This way, users will easily identify a company's identity and decide to follow it. After all, a company should use only high-quality photos to capture its products, preferably authentically.

An excellent marketing trick is the usage of the so-called Instagram influencers. Famous people, including bloggers, sportspeople, or artists, can help a company promote its brand on this social network. "*They have a large follower base and are trusted for their opinions on the latest products and trends"* (King, 2015). Therefore, cooperation with them will ensure the company's increased brand awareness. Moreover, the simplicity of using promo codes is based on posting a picture with a specific code, allowing customers to gain discounts in stores after saying this code. This is an effective way for a company to monitor the engagement of its customers. Eventually, regarding hashtag contests, the main objective is to motivate followers to post a photo using a specific hashtag connected with the company. Followers actively engage with the brand and those who win, usually get free products or services, increasing positive vibes about the company (Wishpond, 2017).

Some examples of brands using Instagram to attain their marketing goals are below.

Dunkin Donuts

An example of Instagram marketing and branding is the case of Dunkin Donuts. The company's account had three pictures that showed emotion. The first picture was associated with the fear or anxiety somebody gets when not having a donut of this brand. The second image tried to portray the nostalgic element of "mom's baking", featuring an apron and homemade cookies in the pictures. The third and last picture depicted happiness, indicating how happy someone can feel by holding a cup of coffee on a cold winter day. Apart from these three images, they also displayed other elements to draw people's attention, for instance, posts with pranks, fun images, textual and visual cues etc. They also had an Instagram contest to reward dedicated fans of Dunkin Donuts. Additionally, they have also used seasons and holidays to make their product popular and recognizable. For example, they have seasonal drinks like the "Latte Pumpkin Creme Brule" for autumn so that people will associate their brand name with the season due to the use of their brand name, logo, colors, and products; Dunkin Donuts has created a strong brand presence on Instagram. People can easily recognize it because of the above and this has strengthened their name and their connection with their fans.

Starbucks

Starbucks fans are some of the most loyal, and they create remarkable content that is often shared on the coffee brand's official social accounts. They also interact with fans through terrific contests. In April 2014, Starbucks challenged their creative customers to customize their iconic white cups and tag their submissions on Instagram with #WhiteCupContest. The winning design would then be used for a limited-edition reusable cup available for sale in the stores. The competition showcased the brand's creative and devoted supporters,

as well as their dedication to promoting sustainability by advocating for the adoption of reusable cups. The campaign received over than 4,000 submissions in three weeks and awarded a young art student in Pittsburgh with the winning title for her creative cup design.

Starbucks regularly expresses its gratitude to selected followers by acknowledging and showcasing the creative individuals who capture compelling images featuring their products. This appreciation is demonstrated through periodic shout-outs and the incorporation of these images into the company's Facebook covers, which are sourced from the Instagram platform.

Adidas & Champs #AdicolorTV

Adidas Originals and Champs powwowed for a great collaboration for #adicolorTV, mini videos featuring Adidas products and various celebrities that would only be aired on the official Champs Sports Instagram account. The campaign was launched in July 2014 and included twenty-fifteen-second "episodes" for six weeks.

15.4.3.3 Snapchat

Launched in 2011, Snapchat is a social media platform that allows users to take pictures and videos, add text, and send them to friends or share them with followers. Facebook took an interest in Snapchat and offered 3 billion to buy it. Once viewers open the Snap, they only have ten seconds (or the duration of the video) to view it before it automatically deletes itself and is gone.

Snapchat is ideal for creating a sense of urgency. Because the Snap only lasts 10 seconds, it is easier to keep people's undivided attention before the picture is gone, even if they have scrolled past the same image on Instagram without glancing at it. This sense of urgency can encourage users to act faster and be a powerful motivator.

However, Snapchat's primary weakness is its limited audience of teenagers and college students, mainly women. Compared to most other social media platforms, this audience is extremely narrow, though admittedly very distinctive. The automatically deleted images might also be a weakness, even though this feature has its benefits. The 10 second duration does have some drawbacks, too.

If people need to pay more attention to the image, or if they want to show their Snap to their friends, or if they accidentally open it without realizing it, the message will be lost, and the marketing potential for that Snap is gone. Timing is everything for Snapchat because the image will not hang around to be viewed later at a more opportune time. There is no permanence. Some of the success of marketing can come from prevalence, where users will scroll over an ad or an image multiple times before they succumb to the temptation of purchasing or clicking. Snapchat does not give this option. It is there, and then it is gone forever.

Snapchat is also used well for campaigns that seek to utilize or create a sense of urgency or timeliness. Having a post that only lasts ten seconds makes users a lot more likely to take action on it before the image is gone.

Fashion retailer H&M had once carried out a marketing stunt in 2015, in which they hid tickets to an exclusive party named Boiler Room in stores. H&M then sent out cryptic clues via Snapchat as to the whereabouts of the hidden tickets.

The results were:

- 943 new Snapchat followers.
- Over 200 people playing the game.
- 3.8m unique users learned that H&M was behind the launch of Boiler Room.
- Lots of positive media coverage.

15.4.4 The Significance of Social Media Marketing

In the previous paragraph, it is clear that social media has reshaped the business landscape into a more competitive market (Tajvidi & Karami, 2017). Furthermore, the expansion of advanced electronic devices and social media caused the relationship between brands and customers to evolve (Ghorbani, 2013). Today, consumers have unlimited access to information about brands, products, services, prices, and recommendations from other consumers. They are more empowered and sophisticated in comparing and purchasing products or services (Chen et al., 2011; Palmatier & Steinhoff, 2019). 63% of customers expect customer service to be available on social media and 90% have already used it to communicate with a brand or a company (We Are Social, 2019). Therefore, firms are pressured to become digitally present on social media platforms and to rethink their marketing strategies (Tiago & Veríssimo, 2014). Under these circumstances, social media is increasingly significant for firms.

Currently, 90% of marketers recognize social media as a crucial component of a marketing strategy (Tuten & Solomon, 2017). Adopting and exploiting social media functionalities is becoming a common practice among organizations. Effective and well-organized marketing activities on social media sites enable businesses to improve branding, CRM, research, and sales promotion (Alves et al., 2016; Ashley & Tuten, 2015; Naeem, 2019; Olanrewaju et al., 2020). With 3.48 billion users, social media represents a great platform for firms to promote products, services, and access potential customers among the global audience (Olanrewaju et al., 2020; Sawicki, 2016). By marketing products and services on social media, the level of product awareness and customer online reviews are exponentially rising and leading to electronic word of mouth. Nowadays, eWOM is recognized as a powerful and highly persuasive tool to attract new customers and is significantly more credible than traditional advertising (Naeem, 2019; Reimer & Benkenstein, 2016; Tajvidi & Karami, 2017). For businesses, it provides enhanced product visibility, brand awareness, consumers' purchasing intention, which in return drives sales (Alves et al., 2016).

Furthermore, social media platforms are becoming the primary venue for communication between companies and customers (Tuten & Solomon, 2017). It allows more adaptive and interactive communication, it develops, and maintains customer trust, relationships, and loyalty (Lipiäinen, 2014; Tajvidi & Karami, 2017). Moreover, social media is a source of a vast amount of data obtainable by data mining, CRM applications, and other techniques. Businesses have, therefore, an opportunity to conduct social media analysis and increase the effectiveness of social media marketing strategy. Valuable customer information can be collected, evaluated and interpreted from social networks. Data transformation into social media metrics is conducted by specialized organizations or businesses (Garrigos-Simon et al., 2012; Kaplan & Haenlein, 2010; Misirlis & Vlachopoulou, 2018). By successfully utilizing customers' data and insights, firms' social media marketing becomes a more personalized and meaningful communication (Lipiäinen, 2014). As such, businesses can satisfy individual customer needs, deliver tailored customer experience, and maintain brand loyalty beyond traditional marketing capabilities (Alves et al., 2016). Social media marketing is, therefore, a prerequisite for building online brand communities, driving leads and sales, improving business performance, and sustaining a competitive position in the market.

15.4.5 Challenges of Social Media Marketing

Besides the fact that social media marketing is a very useful tool for businesses of any kind and size, it certainly also brings along some deficiencies or weaknesses.

The most obvious challenge related to social media marketing is that it is very time consuming and, hence, needs significant commitment. This is because social media platforms need constant updates and maintenance, which forces companies to assign staff to take care of their Facebook presence (MaxFusion Media, 2014; Stelzner, 2012). This issue is highly important since a business aims for an overall good

reputation, which can only be established and kept if online appearance is adapted and maintained. If a firm fails to maintain its social media presence properly, it can lead to a loss of customers and in turn to a lack of brand loyalty (MaxFusion Media, 2014; Stelzner, 2012, PsPrint, 2013). So, a constant social media monitoring is of crucial importance, even though it is time and resource consuming.

In further exploring the concept of a company's reputation, it is important to recognize that effective reputation management is essential for organizations to harness the advantages of social media. This must be reflected to the concept of the customers being the center of attention, hence users that post unfavorable comments about a company requires well-trained employees who deal with the complains to avoid loss of reputation (Beal, 2014; MaxFusion Media, 2014; Stelzner, 2012). Logically, suppose a firm fails to deal with negative comments. In that case it may face severe problems of overall loss of reputation, which can, again, lead to customer loss and consequently result in financial losses.

The next challenge derives from the importance of communication objectives. It is important to ensure a well-rounded communication strategy since miscommunication may lead to distrusting consumers in the worst case (McQuerrey, 2014; MaxFusion Media, 2014). A failure in doing so may again lead to losses in all terms, namely consumers, consumers' trust, brand loyalty and a loss of reputation, as stated before.

Continuing this thought highlights the challenge of the high consumption of time and resources again. Whenever a business decides to run a Facebook page, resources in terms of staff and IT knowledge, for example, are necessary, and therefore financial resources are also required (Kelleher, 2013; Stelzner, 2012). Following this logic, financial resources are also needed to be able to take an active part in the market competition. If the business aims to grow with the help of Facebook, it needs to spend a noticeable amount of money to be able to pay for Facebook's advertisement service. Businesses must pay, once their advertisements have been watched 1,000 times or more. On top of that, organizations also have to "Pay for Click" (CPC), meaning a certain amount a company has to pay if users click on the company's ads.

However, the challenges are not only linked to financial issues or potential customer loss. Having a well-managed social media presence also requires what is related to the skills of the people working within a company. Managing social media platforms calls for high demands on staffs' talents because it can be difficult to always come up with content perceived as creative or interesting enough to the consumer. Therefore, managing a social media website requires highly creative employees that know which content seems relevant to the fans to satisfy customer needs (PsPrint, 2013). Without talented staff, the whole concept of a good Facebook presence may fail and efforts and money would be wasted (Kelleher, 2013).

Another problem, which may not seem obvious from the beginning, is the challenge of dealing with a certain amount of losing control. To a certain degree, the loss of control is repeatedly reliant on the concept of Web 2.0. It puts the consumer in the center of attention (Collins, 2003; Bosari, 2012). It can, therefore, happen that consumers do not react in a favorable manner, which can harm and thus cause a lasting damage to a business (MaxFusion Media, 2014).

Therefore, to avoid failures in terms of a business's social media presence, special factors need to be considered. Otherwise, social media involvement bears a significant risk for all businesses.

Ultimately, numerous individuals in their youth predominantly engage in an internet-based existence through a limited range of social media platforms; nevertheless, this trend is not as prevalent among older demographics. Consequently, corporations aiming to reach individuals aged 55-70 perceive social media marketing as a futile strategy. Additionally, an adverse consequence may arise if a company excessively prioritizes social network marketing and neglects the upkeep of its website. Nevertheless, by acknowledging these concerns, companies can prevent such errors.

15.5 An Applied Social Media Marketing Approach: The Case of Adidas and Nike

Adidas and Nike are two multinational corporations manufacturing sport equipment with a significant global market share. Both soon enough engaged in applying social media marketing techniques of different orientations to reach potential customers. Companies can generally monitor the influence of such techniques by using software that measures or calculates the so-called social media metrics, and various parameters that describe the phenomenon. These observations allow them to adjust their approaches for more successful results. Three basic broadly used Facebook metrics are described below, namely Engagement, Reach, and Impressions:

- **Engagement** is when people perform actions on a Page. For example, they may like a post, click a link, or comment on an image. Facebook Insights defines engagement as post clicks, likes, shares, and comments.
- **Reach** in Facebook is the number of unique people who saw a specific content. It affects every metric that can be tracked: engagement, likes, comments, clicks, and negative feedback. Moreover, there are different kinds of reach: post, page, organic, viral, and paid.
- **Impressions** are another Facebook metric related to the visibility of your posts. While reach describes how many people saw specific posts, impressions measure the number of times that these posts were seen. That metric considers if one's post was seen multiple times by a single user.

In the following paragraphs, a simplified example of social media metrics observation is outlined using data from Nike's and Adidas' activities on Facebook and X.

15.5.1 Adidas

Adidas AG, a German multinational corporation based in Herzogenaurach, Germany, that designs and manufactures footwear, clothing, and sports accessories. It is the largest sportswear manufacturer in Europe and the second largest in the world, with over 60,000 new employees in over 160 countries. It was registered as an enterprise on August 18, 1949, by Adolf Dassler, following a family dispute at Gebrüder Dassler Schuhfabrik between him and his older brother Rudolf, who had previously founded Puma, which quickly became the company's business rival.

The Adidas brand is one of the innovators in using social media to campaign and promote its image by using X, Facebook, and blogs. It is actively involved in social networks, creating more pages to expand its audience in several sectors. For example, in 2009, when X recorded one of the largest increases among social networks and was ranked third, Adidas created several pages on this platform, including Adidas Running, Adidas Malaysia, Adidas US, Adidas UK, and the most popular so far, Adidas Originals. By diversifying its pages, Adidas attracts more followers and potential consumers from more markets, such as Adidas UK, which focuses on consumers in the UK, or even Adidas Football, which attracts more football fans.

In **Table 15.1,** data from Adidas' X network were mined in June 2018: the number of tweets, the number of followers, the number of accounts followed by Adidas, the number of appreciations and the date each account was created. Analysis of the collected data showed that:

Table 15.1 *Data mined from Adidas activities on X in June 2018 (own elaboration).*

	Adidas	Adidas Originals	AdidasUS	Adidas Football	Adidas Running
Tweets	7 K	15.8 K	11.4 K	25.8 K	9.6 K
Followers	3.14 M	3.73 M	762 K	3.02 M	1.04 M
Follow	145	435	366	680	889
Assessments	6,097	8,141	5,187	749	9,985
Date	May 2011	February 2009	July 2009	November 2010	February 2009

- Adidas Originals account (@adidasoriginals), created in February 2009, was the company's most popular page on X, registering 3,727,115 followers, followed by @adidas with 3.14 million and @adidasfootball with 3.02 million.
- Adidas account (@adidas), created in May 2011, was the one that records the highest growth among the company's accounts, attracting 3,136,757 followers from the date of incorporation until June 2018, followed by @adidasfootball and @adidasoriginals.
- Adidas Football account (@adidasfootball), created in November 2010, was the most active account of the brand, posting by that time 25,798 tweets, followed by @adidasoriginals with about 15.8 thousand and @adidasUS with 11.4 thousand tweets.
- Adidas Running account (@adidasrunning) was the most appreciated fan page, registering 9,985 likes, followed by @adidasoriginals with 8,141 and @adidas with 6,097 likes.

Adidas' renaissance began with the relaunch of its iconic Stan Smith shoe model. This is based not only on feelings of nostalgia but also by emphasizing heritage, which has helped strengthen the brand's influence on streetwear and subcultures such as Brit-pop and hip-hop. The social media campaign surrounding the launch was cleverly made to make consumers feel part of the story. The "*Stan Yourself*" initiative involved asking users to tweet a photo of them for a chance to win a pair of custom shoes.

Adidas also posts the video and the visual content they have used on all Facebook pages on other channels. Another tactic of Adidas to gain influence on Facebook is to embrace other accounts. In particular, they share the content posted by other accounts owned by Adidas users and athletes, clubs, or national teams. If Adidas launches new equipment by posting relevant content, these accounts are also highly expected to share it.

Table 15.2 presents data collected from three Adidas Facebook accounts, namely @adidas, @adidasoriginals, and @adidasfootball, including the number of likes, followers, etc.

Table 15.2 *Data mined from Adidas activities in Facebook in June 2018 (own elaboration).*

	Adidas @adidas	Adidas Originals @adidasoriginals	Adidas Football @adidasfootball
Followers	27.34 M	30.1 M	22.5 M
Number of likes	27.5 M	30.6 M	22.67 M
Talk about	155,869	58,685	133,323
Number of photos	1,665	21,175	26,071
Date	September 2014	October 2015	October 2015

Analysis of the collected data showed that:

- Adidas Originals (@adidasoriginals) was again the most famous account of the brand, with 30,609,750 people who appreciated the given account, out of which 30,069,340 follow it. In terms of popularity, @adidasoriginals was followed by @adidas, even though it was created a year later, with about 27.5 million likes, and 27.34 million followers, and @adidasfootball with 22.67 million appreciations and 22.5 million people following the account.
- Adidas (@adidas) was the account with the most followers, registering 155,869 people in the Talk About section. This figure was more gratifying than the number of followers or appreciation because it also indicated the involvement rate of the people who follow the account, which is higher than the other two. Adidas (@adidas) was followed by @adidasfootball with 133,323 and @adidasoriginals with 58,685 respectively,
- Adidas Football (@adidasfootball) was the account with the most photos and video posts, thus being the most active. We identified 26,071 photos posted, which reflected the number of active followers, which was quite large in relation to the total number of followers. According to the number of photos posted, @adidasfootball was followed by @adidasoriginals with 21,175 visual posts and @adidas with 1,665.

In **Figure 15.1** the statistics of the followers of the @adidas account are presented. Most of the fans were from the Philippines, namely 1,348,214, i.e., 7.9% of the total, followed by fans from the USA, with 954,421 followers, i.e. 5.6% of the total, and then those from Malaysia, being 926,387 followers in number, i.e. 5.4%. Regarding the number of followers of @adidas, countries from South Asia, where most of the brand's products are produced, were on top.

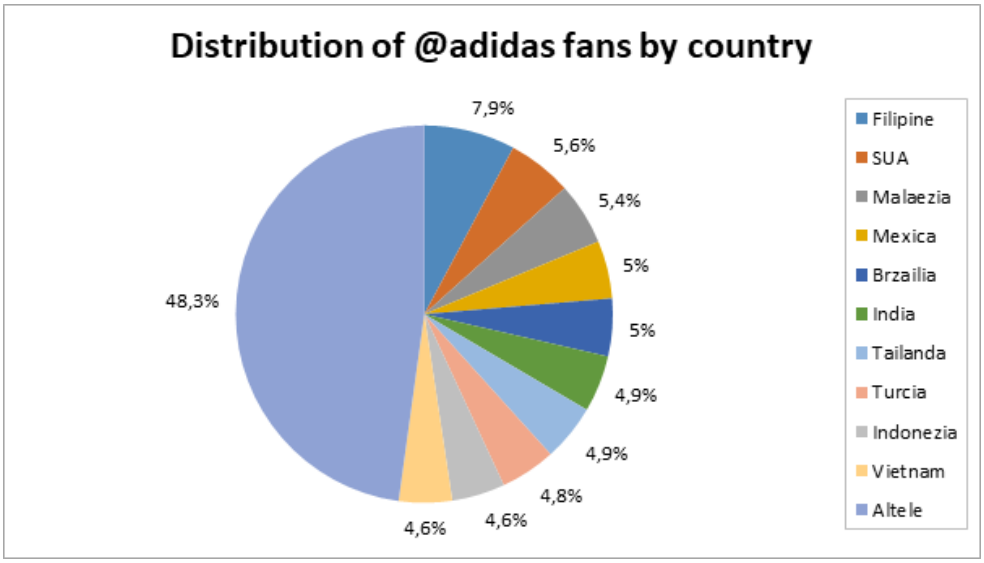


Figure 15.1 *Distribution of @adidas fans by country (own elaboration using www.trackalytics.com).*

Adidas Instagram profiles are used to generate brand and product awareness. The great visual content on the channels contributes to the increase potential customers' enthusiasm and desire to obtain Adidas products. In terms of real-time marketing, Instagram is a social channel that Adidas uses professionally. For example, at the organization of the Women's Soccer World Cup in Montreal, Adidas provided the balls for the match. They posted an image with the ball of the final match and entered the event's location so that more people could find the given content and observe the post on Instagram. This is another way to make a brand visible and active through Social Networks, not just through hashtags and existing followers.

15.5.2 Nike

Nike Inc. is an American multinational corporation that designs, develops, produces, and sells footwear, clothing, equipment, sports accessories, and services worldwide. The company's headquarters are in the Portland metropolitan area near Beaverton, Oregon. Bill Bowerman and Phil Knight founded the company Blue Ribbon Sports on January 25, 1964by and officially became Nike Inc. on May 30, 1971. The company sells its products under its own brand, as well as Nike Golf, Nike Pro, Nike+, Air Jordan, Nike Blazers, Air Force 1, Nike Dunk, Air Max, Foamposite, Nike Skateboarding and subsidiaries such as Brand Jordan, Hurley International and Converse. Nike is one of the biggest brands in the world, and therefore, it is not at all surprising that they have such a huge immensity in the social media field.

Being a company of American origin, Nike started its promotion campaign on the social network X just a year after its appearance, when it had just become known in the USA. The company created its first X account in May 2007 under the name Nike Basketball (@nikebasketball), focusing on the fact that basketball is one of the most popular sports in the US. Nike soon increased the number of accounts: @nikestore in November 2008, @nikefootball in May 2009, @nikesportswear in December 2011, and many others.

The most important data from the @Nike, @nikestore, @nikefootball, @nikebasketball, and @nikesportswear accounts in June 2018 have been extracted and are presented in **Table 15.3**:

Table 15.3 *Data mined from Nike activities on X in June 2018 (own elaboration).*

	Nike	Nike.com	Nike Football	Nike Basketball	Nike Sportswear
Tweets	32 K	301 K	44.5 K	36.4 K	9.6 K
Followers	7.05 M	4.39 M	3.25 M	2.19 M	1.4 M
Follow	156	163	495	378	58
Assessments	5,473	910	1,523	1,161	1,840
Date	11.2011	11.2008	05.2009	05.2007	12.2009

Analysis of the collected data showed that:

- The Nike (@Nike) account, created in November 2011, was the most popular of all, with a rather impressive number of 7,047,462 followers after five and a half years, which recorded the highest increase. The second most popular was @nikestore with 4,385,978 followers, followed by @nikefootball with 3,249,794.
- The Nike.com X account (@nikestore) was the most active, recording 301,149 tweets, and being the absolute leader. It was followed by @nikefootball with 44,452 tweets and @nikebasketball with a total of 36,421 ones.
- Most recently created, Nike (@Nike) was also the most beloved page with 5,473 likes. It was impressive that it was followed by @nikesportswear with 1,840 likes, the account with the fewest followers of all, as mentioned in **Table 15.3.** The third in rank was @nikefootball, with 1,523 appreciations.

Table 15.4 *Data mined from Nike activities on Facebook in June 2018 (own elaboration).*

	Nike @nike	Nike Basketball @nikebasketball	Nike Football @nikefootball
Followers	28.1 M	8.3 M	44.4 M
Number of likes	28.4 M	8.5 M	44.5 M
Talk about	405,975	43,115	70,365
Number of photos	281	1,307	2,014
Date	19 September 2013	20 September 2013	19 September 2013

Nike stands out on X because it interacts with its followers and responds to almost any mention they receive with interesting tips and answers, making consumers feel appreciated.

Like on X, Nike has more Facebook accounts, while smaller specialized accounts that seem to be more active than the “key” accounts. Running has always been one of Nike’s main areas of interest. Their @nikerunning account was one of the most popular, regularly posting much content about running, ranging from the launch of new sneakers made for this kind of activity, to information about relevant events. For example, the Kenyan national running team is involved in the latest Nike Running campaign. It is present in a large volume of Facebook posts, including videos and quotes of team members.

Data from three of the company's most popular Facebook accounts as of June 2018 are presented in **Table 15.4.**

Analysis of the collected data showed that:

- The Nike Football account (@nikefootball) was the most appreciated and followed, counting 44,508,958 likes and 44,367,288 followers, respectively. Second in this ranking was @nike, with 28,375,603 likes and 28,107,644 followers.
- Nike (@nike) was the account with the most followers involved, with 405,975 people in the Talk About chapter. Nike (@nike) was followed by @nikefootball with 70,365 followers and @nikebasketball with 43,115, respectively.
- Most posts with visual content were recorded on accounts dedicated to sports. Regarding the @nikefootball account, 2,014 published photos were identified, 1,307 for @nikebasketball and 281 for @nike only.

15.5.3 Comparative Analysis

Nike and Adidas have chosen slightly different approaches to presenting their brand and products through social media marketing. While Nike is a sportier and performance-oriented brand, Adidas focuses on originality, fashion style, and celebrities. Things were the same between the two giant sporting goods manufacturers in the early 2000s.

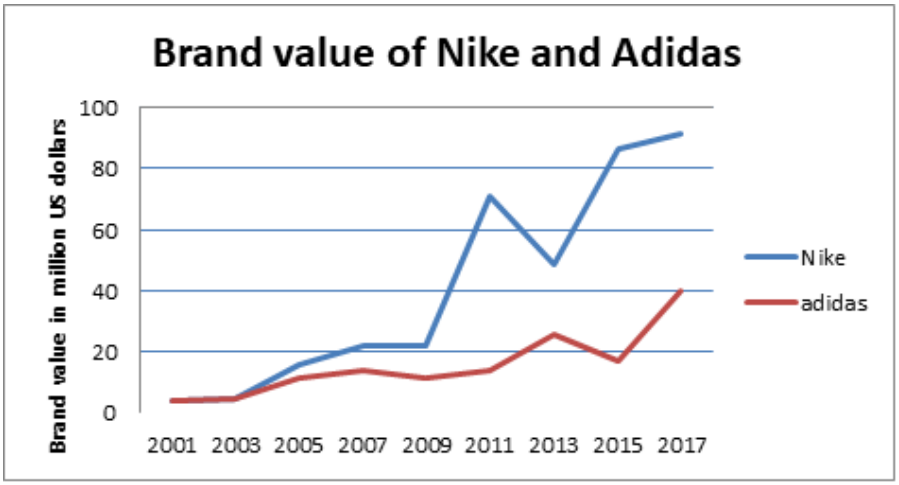


Figure 15.2 *Brand Value of Nike and Adidas in million US dollars (Statista).*

However, 2010 was a spectacular financial year for Nike, with its revenue reaching $19 billion. This means that Nike made more money than the entire nation of Honduras, raising its market cap to 63.45 billion dollars. The company ended strongly with an impressive quarter and an accelerated momentum in the business. "*Nike is best when we focus on the two core values - innovation and inspiration*," Mark Parker commented. Meanwhile, Adidas finished the decade behind its financial rival, being listed on the market at just $14.61 billion, about 4.34 times less than Nike.

Figure 15.2 shows the brand value of companies since the 2000s. For many, the large increase in the company's value in the stock markets began in 2009-2010 due to the active involvement in social media campaigning. This is partly presented by the parameters in the tables above, giving analysts a reason to investigate and correlate social media metrics and variables like the brand value in **Figure 15.2**. Analysts argue that Nike has proven that proper promotion on social networks can bring the company to impossible levels. For example, in the United States, which accounts for 40% of worldwide sporting goods sales, Nike equipment

is introduced on a huge scale. In terms of running, Nike owns 60% of the total sales of sporting goods, and in terms of basketball, the company surprises US with 90% of the total.

15.6 Customer Relationship Management (CRM)

The birth of the Customer Relationship Management (CRM) system is inextricably linked to the emergence of marketing philosophy. It all started in the 1960s when firms' interests shifted from recurring sales to substantial satisfaction of consumer needs. Thus, their goal was to identify, through marketing research, the needs of consumers rather than sell a large number of products that did not really meet their desires. This new marketing philosophy contributed to the "birth" of CRM systems.

15.6.1 Using CRM

In the early 1990s, with the invention of the World Wide Web (www), which allowed Internet users to search for information by moving from one document to another, companies faced many difficulties in organizing the vast amount of data created by customers. In response, specialists developed hardware and software solutions to handle this huge amount of customer information better. These new technologies included Sales Force Automation (SFA) and customer service support. With their help, firms could analyze consumers' behavioral patterns more effectively and build trustworthy relationships with them. As time passed, marketing specialists started to use the term "CRM" to refer to the improvement between firms' and customers' relationships.

CRM systems are designed to gather customer information s through various channels or points of contact between the company and its customers. These contact points include the company's website, telephone, live chat, direct mail, marketing materials, and social media. CRM systems can also provide detailed information about customers' personal information, concerns, buying preferences, purchase history, etc. (CRM, 2013). CRM aims to improve business relationships with customers, assisting in keeping customers and driving sales growth.

The extended use of CRM systems has led to various definitions in an attempt to describe its main characteristics. In the beginning, as Buttle and Maklan report, Internet experts usually defined CRM as "an information industry term for methodologies, software and usually Internet capabilities that help an enterprise manage customer data in an organized way." For them, CRM was considered a technological tool for them to manage customers' data. Nowadays, companies present CRM as software and as a process, philosophy, and intention to fulfill customers' needs and desires. As they mention, CRM "is the process of managing all aspects of interaction a company has with its customers, including prospecting, sales, and service. CRM applications attempt to improve the company/customer relationship by combining all these views of customer interaction into one picture. CRM's primary goal is to improve long-term growth through a better understanding of customer needs and behavior."

This strategic approach shifts the emphasis from gaining customers, to turning them into loyal and profitable advocates. There are also supporters of the managerial approach, who link the CRM system with the customer experience (CX) movement. This movement consists of an attempt to improve customers' experience of as they interact with the company. When a company adopts effective CRM technologies, consumers, and customers can better interact with that company by having a greater experience.

Among the first companies to apply CRM techniques were Apple and Amazon. When consumers buy an Apple device, they are asked to create an Apple ID—a unique account that synchronizes their information across all Apple devices they may have. These accounts save their preferences and allow Apple to provide more personalized recommendations based on their interest and previous search history. For consumers, this

is a convenient and time-saving solution. These accounts constitute a part of Apple's CRM strategy and, therefore, provide data that allow insights about customers' needs and build the potential for implementing targeted marketing techniques.

Amazon is the most well-known platform for online purchases. One of the main reasons for its success lies in the ideal utilization of the CRM system. When customers purchase an item from Amazon, they need to create a private account. This way, Amazon can track their purchases and browse their purchasing history to build more personalized marketing and email campaigns effectively. Moreover, Amazon allows them to adjust their accounts to carry out purchases in one click. Consumers appreciate the fast checkout processes and the targeted product proposals. The better their experience, the more likely they will become loyal customers.

Customer relationship management (CRM) is a term closely related to social networking. It refers to strategies, practices, and technologies companies use to analyze data and interactions with customers and for data on the whole customer lifestyle. On social media websites, a customer is an integral part of the sales process, and CRM is adapted to support the new marketing role of the customer. Information from social media platforms is gathered using social analytics tools, enabling them to offer accurate insights regarding an individual's level of brand advocacy and the specific stage of their journey towards becoming a brand advocate. The new role of the customer is then based on the relationships and shared activities that are played in social media websites. This role of the customer can be understood and managed by some traditional practices and ideas of CRM (Evans & McKee, 2010).

15.6.2 Artificial Intelligence for CRM: The Rise of Chatbots

In recent years, Artificial Intelligence (AI) has been growing rapidly. According to Frankenfield, AI is the simulation of human intelligence in machines that are programmed to act like humans and mimic their behaviors. AI methods and technologies are not used only for scientific reasons. Nowadays, businesses leverage AI technology for administrative, managerial, or marketing purposes. One example is the use of AI "bots," or "chatbots," by firms in order to optimize their CRM system (Kouroupis et al., 2022).

Botadra points out that a bot is also referred to as a Web Robot, Internet Bot, Spider or WWW Bot. The first bot in history (1964) was "ELIZA" whose purpose was to mimic a psychotherapist using Natural Language Processing programming. The user asked a question and Eliza answered by following the program code. With time, various bots were introduced, like "Siri" by Apple in 2013, "Alexa" by Amazon in 2014, and "Cortana" by Microsoft in 2014. Bots are software applications that automate specific tasks fast and seamlessly, assigned to them through coding. Bots can be Chatbots, Crawlers, Transaction Bots, Informational or Entertainment bots. On the other hand, they can perform harmful tasks and be Hacking bots, Spam bots, Scrapers, Impersonators, or Zombie bots.

Chatbots are a category of bots that act online in chat or messaging platforms like Facebook, Messenger, etc. Botadra and Aberer et al. explain that these bots can carry out a conversation with humans. There is a tiny promise in the word "chatbots"; these bots are designed to perform a conversation and interact with users via auditory and textual methods. Brandtzaeg and Følstad define chatbots as "machine agents that serve as natural language user interfaces to data and services through text or voice. Chatbots allow users to ask questions or make commands in their everyday language and get the needed content or service conversationally." Chatbots have been around since 1964, but their real expansion was in 2016 when Facebook and Messenger allowed firms to place chatbots on their social networking platforms.

The rise of chatbots is inextricably linked with the expansion of social media. On average, people spend most of their time on messaging platforms like Facebook or Messenger, and 2.5 billion users have at least one messaging app installed on their phones. In 2017, for example, Messenger had 1.2 billion active users. Another interesting fact is the phenomenon of "app fatigue." App platforms like Apple's Appstore offer a tremendous

number of apps, but users are unwilling to add new apps to their smartphones. A recent study in 2016, showed that 80% of a person's online time is dedicated only to apps like Facebook, Messenger, Instagram or Google and that Facebook and Google created 9 out of the top 10 most used apps.

These fundamental changes in the behavior of online users led companies to adopt chatbot technology. Nowadays, firms leave aside the creation of new apps and prioritize chatbots to reach their audience. Technology legends like Google and Amazon and customer service companies like Starbucks tend to reach their customers by using chatbots. By 2021, more than 50 percent of companies will invest in chatbot or bot technology rather than traditional app creation.

The mechanism that led chatbots to be part of the firms' CRM system is explained shortly. Companies consider that, in general, the primary motivation for someone to use a chatbot is to obtain specific services or information. In response, they use chatbots mainly for customer support (Kouroupis et al., 2022). With customer support, a company helps or advises its clients. These humanized interfaces (chatbots) provide personalized, more automated 24/7 support. The chatbot learns many things about customers' needs. It acts like a friend who understands their desires and fulfills them. Also, the fact is that it is designed to be fully personalized, optimize customer satisfaction, and increase firms' sales. These automated assistants help the CRM system fulfill its primary goal: to understand customers' needs better and establish long-term relationships with them.

Here are some case studies. British Airways has a chatbot in the Messenger app. This bot includes events that happen in London, provides hotel discounts, and sells tickets. Moreover, a well-known example is the Kayak Facebook Messenger bot (Figure 4), which provides information about discounts on flight tickets, and hotels, keeps records of previous conversations and uses Kayak's search history to personalize its content. The fact that this bot has an internal database with customers' previous purchases and reviews makes communication between the company and its customers more efficient. Extended personalization is achieved with the chatbot" Alexa," directly connected to Amazon's CRM. Several Amazon devices, such as Amazon Echo, are powered by Alexa, a voice personal assistant that accompanies the user all the time. Some of its main abilities are playing music, informing about the weather, ordering food, or finding the nearest store. This bot consists of a digital entity that acts on behalf of the customers and improves Amazon's CRM by personalizing their profile or storing their data. Hence, Amazon can track their desires and create efficient marketing campaigns. Undeniably, chatbots can be considered" tiny" treasures that help CRM optimize the company's interactions with its clients. For this reason, a chatbot is designed to be a friendly automated personal assistant that can engage with the customer in more a natural dialogue to enhance his/her trust and experience. A study has shown that many clients put too much trust in advice given by an automated assistant and are more willing to accept an incorrect chatbot recommendation rather than one from a traditional advisor. Additionally, a bot is created to personalize customers' characteristics and store a large amount of their data. As a result, by interacting with it, people do not see a machine; they see another human who can understand their needs, provide them with a service, and give solutions to their problems. Hence, consumers have a highly relative and intimate attitude towards a company and are willing to pay higher prices to purchase a product or service (brand loyalty).

15.7 Conclusion

The use of classical media in marketing is considered by many to be on the decline. Television and radio do not have the same power as decades ago, nor does advertising through this type of media. The leading position now belongs to digital media, mainly the Internet and social media, where millions spend their free time. Consequently, the potential of gaining the attention of new potential customers online is higher than ever before. In such a huge space, reaching target customers is easier, and social media advertisements can be

much more effective. Moreover, digital marketing can be cost saving, since involving activities are, depending on the circumstances and the goals set, for minimal costs. Other advantages for companies using digital marketing include a broader spectrum of customers, increased brand recognition, and brand loyalty (DeMers, 2014). However, there are also challenges involved. For instance, in the case of large-scale digital media strategies, the process requires greater expense.

To conclude, digital media provide great chances for marketing since the opportunities seem to outweigh the challenges. Their success is dependent, of course, on several factors and, in many cases, it requires a lot of dedication and effort. However, if marketers are trained and experienced in this constantly expanding field, Digital Marketing appears to be an advisable tool for all scales of businesses or organizations.

References

About Facebook, 2006. "Facebook Unveils Facebook Ads." About Facebook. [online] Available at: https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

Alves H., Fernandes C., and Raposo M., 2016. "Social Media Marketing: A Literature Review and Implications." *Psychology and Marketing,* 33, pp. 1029–1038. https://doi.org/10.1002/mar.20936

Anon D. S., 2014. "The Online Advertising Industry: Economics, Evolution, and Privacy." *The Journal of Economic Perspectives*, Published By: American Economic Association, Vol. 23, No. 3 (Summer, 2009), pp. 37–60 [online]. Available at: http://www.jstor.org/stable/27740539

Ashley C., and Tuten T., 2015. "Creative Strategies in Social Media Marketing: An Exploratory Study of Branded Social Content and Consumer Engagement." *Psychology and Marketing*, 32, pp. 15–27. https://doi.org/10.1002/mar.20761 [Accessed 16 April 2019]

Baker W., Marn M., and Zawada C., 2001. "Pricing Smarter on the Net. Harvard Business Review" (February). Available at: https://hbr.org/2001/02/price-smarter-on-the-net [Accessed 17 January 2019].

Baldassarre R., 2015. "8 Ways Businesses Can Benefit From Facebook." Retrieved from Entrepreneur: https://www.entrepreneur.com/article/244837 [Accessed 13 March 2019].

Barry C., and Charleton D., 2009. "In search of search engine marketing strategy amongst SME's in Ireland." *In e-Business and Telecommunications* (pp. 113–124). Springer Berlin Heidelberg.

Beal V., 2014. "What is User-Generated Content (UGC)?" Available at: http://www.webopedia.com/TERM/U/UGC.html [Accessed 19 April 2019].

Berman R., and Katona Z., 2013. "The Role of Search Engine Optimization in Search Marketing." *Marketing Science*, 32(4), pp. 644–651. https://doi.org/10.1287/mksc.2013.0783

Blackshaw P., 2006. "The consumer-generated surveillance culture." Available at: http://www.clickz.com/showPage.html?page=3576076 [Accessed 19 January 2019].

Blackshaw P., and Nazzaro M., 2006. "Consumer-generated media (CGM) 101: Word-of-mouth in the age of the web-fortified consumer." Nielsen Buzzmetrics.

Bosari J. 2012. "The Developing Role of Social Media in the Modern Business World." Available at: http://www.forbes.com/sites/moneywisewomen/2012/08/08/the-developing-role-of-social-media-in-the-modern-business-world/ [Accessed 13 March 2019].

Bouncken R. B., and Reuschl A.J., 2016. "Coworking-spaces: how a phenomenon of the sharing economy builds a novel trend for the workplace and for entrepreneurship." *Review of Managerial Science,* 12, pp. 317–334. https://doi.org/10.1007/s11846-016-0215-y

Brown B., 2007. *The Complete Guide to e-mail marketing: How to create successful, spam free campaigns to reach your target audience and increase sales*. Atlantic Publishing Group, Ocala, Florida.

Bulygo Z., 2017. "Facebook Marketing: A Comprehensive Guide for Beginners." Available at: blog.kissmetric: https://blog.kissmetrics.com/facebook-marketing/ [Accessed 25 January 2019].

Cambridge University Press, 2014. "traffic noun" - definition in the Business English Dictionary. Retrieved from http://dictionary.cambridge.org/dictionary/business-english/traffic_1

Carlson N., 2010. "How Facebook Was Founded" - *Business Insider*. Available at: http://www.businessinsider.com/how-facebook-was-founded-2010-3?op=1 [Accessed 17 January 2019].

Carter B., and Brooks G., 2007. *Digital Marketing for Dummies*. John Wiley and Sons Ltd, West Sussex, England.

Chaffey D., 2007. *Total E-mail Marketing, Maximizing your results from integrated e-marketing*. Elsevier Ltd.

Chaffey D., and Chadwick F.E., 2012. *Digital Marketing: Strategy, Implementation and Practice*, Fifth Edition, Pearson.

Chen Y., Fay S., and Wang Q., 2011. "The Role of Marketing in Social Media: How Online Consumer Reviews Evolve." *Journal of Interactive Marketing, 25*, pp. 85–94. https://doi.org/10.1016/j.intmar.2011.01.003

Clay K., Krishnan R., and Wolff E. 2001. "Prices and Price Dispersion on the Web: Evidence from the Online Book Industry." *The Journal of Industrial Economics*. [E-commerce] Borenstein and Saloner.

Collins H., 2003. "Web 2.0." Retrieved from http://www.thefreedictionary.com/Web+2.0

Constantinescu T., and Devisch O., 2018. "Portraits of work: mapping emerging coworking dynamics." *Information Communication and Society*, *21*, pp. 1263–1278. https://doi.org/10.1080/1369118X.2018.1459775

Constine J. 2012. "Instagram's New 'Explore' Brings The Future Of Photo Discovery Into Focus." Retrieved from Techcrunch: https://techcrunch.com/2012/06/25/instagram-explore/

Constine J., 2017. "Instagram's growth speeds up as it hits 700 million users." Retrieved from Techcrunch: https://techcrunch.com/2017/04/26/instagram-700-million-users/ [Accessed 20 June 2019].

Microsoft Dynamics CRM, 2009. "CRM and Social Networking: Engaging the Social Customer" [online]. Available at: http://www.storm.ie/PublishingImages/Documents/CRM%20and%20Social%20Networks.pdhttp://www.storm.ie/PublishingImages/Documents/CRM_and_Social_Networks.pdf [Accessed 19 January 2019].

Cross J., 2015. "Social media marketing trends nowadays #part1." Island Media Management [online]. Available at: https://www.islandmediamanagement.com/social-media-marketing/ [Accessed 19 January 2019].

Dean A., and Rouse M., 2014. "What is Facebook?" Retrieved from What Is?.com website: http://whatis.techtarget.com/definition/Facebook

DeMers J., 2014. "The Top 10 Benefits of Social Media Marketing." Retrieved from http://www.forbes.com/sites/jaysondemers/2014/08/11/the-top-10-benefits-of-social-media-marketing/

DeMers J., 2015. "The Definitive Guide to Marketing Your Business On Facebook." Available at: https://www.forbes.com/sites/jaysondemers/2015/08/20/the-definitive-guide-to-marketing-your-business-on-facebook/#1c11e9462f51 [Accessed 20 June 2019]

Desouza, A., 2020. "What is the Role of SEO in Digital Marketing?" *Search Engine People Blog*. Available at: https://www.searchenginepeople.com/blog/what-is-the-role-of-seo-in-digital-marketing.html [Accessed 20 February 2019].

Dunay P., and Krueger R., 2010. *Facebook Marketing for Dummies*. Hoboken: Wiley Publishing, Inc.

Dushinski K., 2021. *The Mobile Marketing Handbook: A Step-by-Step Guide to Creating Dynamic Mobile Marketing Campaigns,*, CyberAge Books, Second Edition.

Evans D., and Mckee J., 2010. "Social Media Marketing: The Next Generation of Business En-gagement" [online]. Canada: Wiley Publishing, Inc., 2010 [cit. 2016-01-08]. Available at: http://dragossorinnicula.ro/wp-content/uploads/2011/12/Social-Media-Marketing.pdf [Accessed 20 February 2019].

Felix R., Rauschnabel P. A., and Hinsch C., 2017. "Elements of strategic social media marketing: A holistic framework". *Journal of Business Research 70*, pp. 118–126. https://doi.org/10.1016/j.jbusres.2016.05.001

García J. J. L., Lizcano D., Ramos C. M. Q., and Matos N., 2019. "Digital marketing actions that achieve a better attraction and loyalty of users: An analytical study." *Future Internet 11*. https://doi.org/10.3390/fi11060130

Garrigos-Simon F. J., Alcamí R. L., and Ribera T. B., 2012. "Social networks and Web 3.0: Their impact on the management and marketing of organizations." *Management Decision, 50*, pp. 1880–1890. https://doi.org/10.1108/00251741211279657

Gesenhues A., and Gesenhues A., 2019. "Facebook reported strong ad revenue growth in Q2, Instagram ads continue to drive impression growth", Marketing Land. [online] Marketing Land. Available at: https://marketingland.com/facebook-reported-strong-ad-revenue-growth-in-q2-instagram-ads-continue-to-drive-impression-growth-264398

Ghorbani A., 2013. "Marketing in the cyber era: Strategies and emerging trends, Marketing in the Cyber Era: Strategies and Emerging Trends." IGI Global. https://doi.org/10.4018/978-1-4666-4864-7

Gibson C., 2018. "The Most Effective Digital Marketing Strategies & Approaches: A Review of Literature." *International Journal of Scientific and Research Publications,* 8, 12.

Green D.C., 2003. "Search Engine Marketing: Why it Benefits Us all. *Business Information Review*." 20(4), pp. 195–202. https://doi.org/10.1177/0266382103204005

Gudivada V. N., Rao D., and Paris J., 2015. "Understanding Search-Engine Optimization. Computer", 48(10), pp. 43–52. https://doi.org/10.1109/mc.2015.297

Hanson A.Ward, Kalyanam Kirthi, 2007. *Internet Marketing and e–Commerce*. Thomson Higher Education, 5191 Natorp Boulevard Mason, OH 45040, USA. How to Use Search Engine Optimization Techniques to Increase Website Visibility. (2013, March)

Janouch V., 2010. *Internet Marketing: Carry out on the web and social network*s. Ed. 1st Brno: Computer Press.

Kaplan A. M., and Haenlein M., 2010. "Users of the world, unite! The challenges and opportunities of Social Media." *Business Horizons,* 53, pp. 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Kelleher D., 2013. "5 Problems with Social Networking in the Workplace." Available at: http://www.cerait.com/5-problems-social-networking-workplace [Accessed 12 November 2018],

King C., 2015. "13 Instagram Marketing Tips from the Experts." *Social Media Examiner*. Available at: http://www.socialmediaexaminer.com/13-instagram-marketing-tips-from-the-experts/ [Accessed 10 December 2018]/.

Kouroupis K., Vagianos D., and Totka A., 2022. "Artificial Intelligence and Customer Relationship Management: The Case of Chatbots and their Legality Framework." Accepted for publication in the 2021 issue of the *East European Yearbook on Human Rights* (https://eeyhr.eu/).

Kotler P., Armstrong G., Harris L. C., and Piercy N., 2017. *Principles of Marketing*. Pearson Education Limited.

Kubátová J., 2014. "The cause and impact of the development of coworking in the current knowledge economy." *Proceedings of the European Conference on Knowledge Management*, ECKM 2, pp. 571–577.

Lipiäinen H., 2014. "Digitization of the Communication and its Implications for Marketing", JYVÄSKYLÄ STUDIES IN BUSINESS AND ECONOMICS, UNIVERSITY OF JYVÄSKYLÄ.

Market Realist, 2019. "Instagram's Ad Revenue More than Doubled in 2018." *Market Realist*. [online] Available at: https://marketrealist.com/2019/01/instagrams-ad-revenue-more-than-doubled-in-2018/

MaxFusion Media, 2014. "Pros and Cons of Using Facebook for Business Marketing and Advertising." Available at: http://maxfusionmedia.com/pros-and-cons-of-using-facebook-for-business-marketing-and-advertising/

McQuerrey L., 2014. "Marketing Communication Objectives." CHRON. Available at: http://smallbusiness.chron.com/marketing-communication-objectives-61476.html

Misirlis N., and Vlachopoulou M., 2018. "Social media metrics and analytics in marketing – S3M: A mapping literature review." International Journal of Information Management. https://doi.org/10.1016/j.ijinfomgt.2017.10.005

Mullen J., and Daniels D., 2009. *E-mail Marketing, An Hour a Day*. Wiley Publishing, Inc, Indianapolis, Indiana.

Naeem M., 2019. "Do social networking platforms promote service quality and purchase intention of customers of service-providing organizations?" *Journal of Management Development,* 38, pp. 561–581. https://doi.org/10.1108/jmd-11-2018-0327

Olanrewaju A. S. T., Hossain M. A., Whiteside N., and Mercieca P., 2020. "Social media and entrepreneurship research: A literature review." *International Journal of Information Management,* 50, pp 90–110. https://doi.org/10.1016/j.ijinfomgt.2019.05.011

Oxford University Press, 2014. Social sharing: definition of social sharing in Oxford dictionary (British & World English). Retrieved from http://www.oxforddictionaries.com/definition/english/social-sharing

Palmatier R. W., and Steinhoff L., 2019. *Relationship Marketing in the Digital Age*. Routledge.

Patel D., 2017. "Social Media Marketing Fundamentals - For Certifications." Google LLC.

Pohjanen R., 2019. "The Benefits of Search Engine Optimization in Google for Businesses." Master's Thesis. Available at: https://core.ac.uk/download/pdf/344907526.pdf [Accessed 14 September 2020].

PsPrint, 2013. "Social Media Marketing Pros and Cons." Available at: http://www.psprint.com/resources/social-media-marketing-pros/ [Accessed 15 November 2018].

Quintana R., 2013. "How Social Media Influences People – Infographic." *Social Magnets.* Available at: http://www.socialmagnets.net/how-social-media-influences-people/ [Accessed 15 October 2019].

Reimer T., and Benkenstein M., 2016. "Altruistic eWOM marketing: More than an alternative to monetary incentives." *Journal of Retailing and Consumer Services,* 31, pp. 323–333. https://doi.org/10.1016/j.jretconser.2016.04.003

Ryan D., and Jones C., 2009. *Understanding Digital Marketing: marketing strategies for engaging the digital generation*. London and Philadelphia, Kogan Page.

Sampson H. 1875. *A history of advertising from the earliest times: Illustrated by anecdotes, curious specimens and biographical notes*. London, Chatto and Windus.

Sawicki A., 2016. "Digital Marketing." *World Scientific News*, pp. 82–88.

SI S., 2015. "Social Media and Its Role in Marketing." *Business and Economics Journal,* 07, pp. 1–5. https://doi.org/10.4172/2151-6219.1000203

Schumpeter J. A., 1942. "Capitalism, Socialism, and Democracy." University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship. Available at: SSRN: https://ssrn.com/abstract=1496200

Statista, 2019. "Global digital population." Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/?fbclid=IwAR1-UxBuTvp6yNiZrumGLCGVVo1xZWkQVA-3EKy9jLVsnIFldRkXe7mHQzY [Accessed 26 September 2019].

Statista, 2019. "Google: ad revenue 2001-2018." Statista. [online] Available at: https://www.statista.com/statistics/266249/advertising-revenue-of-google/

Statista, (n.d.). "Social media - Statistics & Facts." Available at: https://www.statista.com/topics/1164/social-networks/ [Accessed 26 September 2019].

Stay J., 2008. "Facebook for Business: Opportunities and Limitations" - Inside Facebook. Available at: http://www.insidefacebook.com/2008/07/28/facebook-for-business-what-it-needs-what-it-has/ [Accessed 14 September 2018].

Stelzner M. A., 2012. "Social Media Marketing Industry Report." Available at: https://www.socialmediaexaminer.com/social-media-marketing-industry-report-2022/ [Accessed 14 September 2018].

Support.google.com, 2018. "About Target CPA bidding." Google Ads Help. [online] Available at: https://support.google.com/google-ads/answer/626863

Support.google.com, 2018. "Google AdWords is now Google Ads." Google Ads Help." [online] Available at: https://support.google.com/google-ads/answer/9028765

Tajvidi R., and Karami A., 2017. "The effect of social media on firm performance." *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2017.09.026

Tiago M.T.P.M.B., and Veríssimo J. M. C., 2014. "Digital marketing and social media: Why bother?" *Business Horizons,* 57, pp. 703–708. https://doi.org/10.1016/j.bushor.2014.07.002

Tucker C., 2012. "Social Advertising." *SSRN Electronic Journal*.

Tuten T. L., and Solomon M.R., 2014. *Social Media Markerting* (2nd ed.). Sage Publications.

Tuten T., and Mintu-Wimsatt A., 2018. "ADVANCING OUR UNDERSTANDING OF THE THEORY AND PRACTICE OF SOCIAL MEDIA MARKETING: INTRODUCTION TO THE SPECIAL ISSUE." *Journal of Marketing Theory and Practice,* 26, pp. 1–3. https://doi.org/10.1080/10696679.2018.1393277

Tuten T. L., and Solomon, M.R., 2017. *Social media marketing*, SAGE Publications Ltd (3rd edition).

Van Rijn J., 2020. "The Future of Email Marketing & Marketing Automation." 2020 edition. Available at: https://www.emailmonday.com/email-marketing-automation-trends-predictions/ [Accessed 04 February 2020].

Waber A., 2016. "Instagram Advertising: What's working?" [online] Available at: http://marketingland.com/instagram-advertising-whats-working-157977 [Accessed 14 September 2018].

We Are Social, 2019. "Global Digital Report 2019." We Are Social.

Weinberg T., 2009. "The New Community Rules: Marketing in the Scoial Web." 1st ed. O`Reilly Media, Inc., Sebastopol, CA.

Wishpond, 2017. "52 Tips: How to Market on Instagram." Wishpond. Available at: http://blog.wishpond.com/post/59612395517/52-tips-how-to-market-on-instagram [Accessed 20 September 2018].

Zhu Y. Q., and Chen, H. G., 2015. "Social media and human need satisfaction: Implications for social media marketing". *Business Horizons,* 58, pp. 335–345, https://doi.org/10.1016/j.bushor.2015.01.006

This book surveys the rapid development of digital media such as digital television, the participatory Internet, multimedia services, social networking sites and mobile technology, focusing on their social diffusion and analysing the impact of these media broadly on society, local and international politics and Economics. It aims to provide an integrated platform for students to engage and critically analyse the issues surrounding the multifaceted relationships between digital media and the society in general. For this purpose, it attempts to include most critical areas of influence of digital media in the context of Social Sciences: Society, Politics and Economics. In the first three chapters, the introductory terms and notions are presented, including the Information Society and the transition to the Networked Society. In the following chapter, the transition from Web 1.0 to Web 2.0 is described and social media and Social Networking Analysis are introduced. Two chapters of this book are dedicated on implications of social media in Politics, Education and the New Generation. In five chapters of the book the Habermasian Public Sphere issues are investigated through the lens of digital media. Therefore, the Digital Divide is initially defined followed by an analysis of many critical areas including Democracy in the Digital Age, e-Government, e-Business and e-Commerce. Subsequently, Social Movements and Activism in the Digital Age are analysed. The book "Digital Media and Society: Convenient Regulators of Society, Politics and Economics: aims to become an essential reading for undergraduate and postgraduate students of Social Sciences generally without a special scientific or technical background, who aim to explore and potentially seek motivation for more in depth investigation of one (or more) of the following dynamically evolving areas such as the realm of digital media, the Internet, social media, the public sphere, the mobile culture, Internet Politics and Digital Marketing.

This book has been created within the framework of the project KALLIPOS+	
Funding	Ministry of Education and Religious Affairs, GREECE, National Development Programme 2020-2025
Implementation	Special Account for Research Funds of the National Technical University of Athens
Operation	Hellenic Academic Libraries Link (HealLink)
Duration of the 2nd Phase	2020-2023
Objective	The creation of more than 700 open-access academic e-books • Undergraduate and Postgraduate textbooks • Monographs • Translations of open-access textbooks • Bibliography Guides
Scientific Coordinator	Nikolaos Mitrou, Professor ECE, NTUA
ISBN: 978-618-5726-25-6	**DOI:** http://dx.doi.org/10.57713/kallipos-221

This book was funded by the Greek National Public Investment Program (PIP)
through the Ministry of Education, Research and Religious Affairs