

**The Future of Freedom of Expression, Privacy, and Democratic Governance at the Digital Age**

---

A Thesis presented to the Faculty of Law and Political Science at Notre Dame University-

Louaize

---

In Partial fulfillment of the requirements for the Degree of Master of Arts in Political  
Science – Human Rights

---

by

Nivine Nassar

December 2020

**©COPYRIGHT**

By

Nivine Nassar

2020

All Rights Reserved

**Notre Dame University – Louaize**

Faculty of Law and Political Science

Department of Law and Political Science

We hereby approve the thesis of

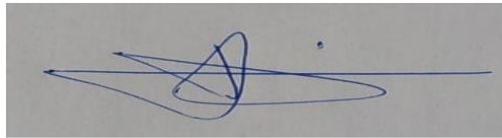
Nivine Nassar

Candidate for the degree of Master of Arts in Political Science - Human Rights

---

Dr. Dany Ghsoub

Chairperson, Assistant Professor



---

Dr. Maria Noujaim

Committee Member



---

Dr. Celine Merheb

Committee Member



## Table of Contents

<b>Chapter 1: Introduction</b> .....	6
Statement of the Problem .....	8
Research Questions .....	10
Objectives of the Study .....	11
Scope and Limitations .....	11
Significance of the Study .....	12
Methodology .....	12
<b>Chapter 2: Literature Review</b> .....	13
<b>Chapter 3: International Legal Framework of Protection of the Right to Freedom of Expression, the Right to Data Protection, and the Right to Privacy</b> .....	23
Section A. International Legal Framework .....	23
Section B. European Legal Framework .....	27
Section C. Types of Internet Intermediaries .....	34
Section D. General Models of Liability for third party generated content .....	35
<b>Chapter 4: Impact of Internet on Human Rights</b> .....	39
Section A. Undermining the freedom of expression online .....	39
Section B. Data Protection and the Right to Privacy .....	47
Section C. Mass Surveillance and Human Rights .....	56
<b>Chapter 5 – Findings of the Study</b> .....	67
<b>Chapter 6- Recommendations and the Way Forward</b> .....	70
Section A. Recommendations on Freedom of Expression at the Digital Age in China .....	70

Section B. Recommendations on Data Protection at the Digital Age in EU.....73

Section C. Recommendations on Mass Surveillance at the Digital Age in The United States.....77

**Chapter 7 – Conclusion** ..... 80

**Bibliography** ..... 82

## List of Acronyms

CIL	Customary International Law
CJEU	Court of Justice of the European Union
DNS	Domain Name System
EU	European Union
GDPR	General Data Protection Regulation
HRW	Human Rights Watch
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
IETF	Internet Engineering Task Force
IHRL	International Human Rights Law
ITU	International Telecommunication Union
OHCHR	Office of the High Commissioner for Human Rights
UDHR	Universal Declaration for Human Rights
UN Norms	UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises
UN	United Nations
US	United States

## **Abstract**

The twenty-first century cyberspace offers unprecedented opportunities for prosperity and development, but also a series of new and evolving threats to international peace, security, and human rights. For some years now, there have been sustained efforts from civil society groups across the world to harness the Internet for human rights causes. However, by publicizing human rights abuses in near-real time to mass audiences, the new uses of digital technologies may also challenge the legitimacy of the international legal order itself, especially if states are not able to action their legal obligations to prevent those crimes. This thesis examines some examples of the interplay internet intermediaries, digital tools, and open data, and the capacity to deploy innovative digital ways to assist human rights monitoring. It also considers both the opportunities and challenges involved in using digital tools to assist in the prevention of human rights abuses, such as freedom of speech, data protection and right to privacy.

## **Chapter 1: Introduction**

### *Human Rights at the Digital Age: Establish or Limit Internet Rights*

Focusing on human rights at the digital age is key. We are in a period of profound societal change and disruption, almost a tectonic shift, brought on by the rapid expansion of digital communication infrastructure and exponential adoption of digital technology. Protection of human rights in the 21<sup>st</sup> Century will rest on our ability to articulate how to apply enduring human rights principles in the digital context. But we are behind the curve. Digital technology has transformed the means through which human rights are both exercised and violated around the globe. The internet has

become an indispensable tool for the realization of a range of human rights, and for accelerating economic development. Yet, every day, there are new examples of how digital technologies play a role in undermining human rights; whether through a prime minister banning Twitter in Turkey<sup>1</sup>; a death sentence for a posting on Facebook in Iran<sup>2</sup>; bulk electronic surveillance of American citizens by the National Security Agency<sup>3</sup>; a court ruling on the right to be forgotten in Google searches in Europe<sup>4</sup>; or a requirement that Internet users supply real names to service providers in China<sup>5</sup>.

Moreover, data collection is already happening on an industrial scale. States, political parties, various organizations and, in particular, businesses hold remarkably detailed and powerful information about us (Bachelet, 2019). More and more aspects of our lives are being digitally tracked, stored, used, and misused. Nevertheless, digital technology already delivers many benefits. Its value for human rights and development is enormous. We can connect and communicate around the globe as never before. We can empower, inform and investigate. We can use encrypted communications, satellite imagery and data streams to directly defend and promote

---

<sup>1</sup> See Carnegie Europe (Judy Dempsey's Strategic Europe) *Judy Asks: Is Erdoğan Abandoning Democracy? An article describing Erdoğan's ongoing efforts to control traditional and social media in Turkey during Elections in 2014, which represented a threat to participation and freedom of expression.* <https://carnegieeurope.eu/strategieurope/55101>

<sup>2</sup> See Human Rights Watch (2014): On November 24, 2014, Iran's Supreme Court upheld a criminal court ruling sentencing Soheil Arabi to hang for insulting the prophet on Facebook <https://www.hrw.org/news/2014/12/02/iran-death-sentence-facebook-posts>

<sup>3</sup> See Reuters's report on NSA collected Americans' phone records in 2017 despite law change following Snowden's revelation in 2013 which entailed having the National Intelligence spying on their citizens. <https://www.reuters.com/article/us-usa-security-surveillance/nsa-collected-americans-phone-records-despite-law-change-report-idUSKBN17Y2LS>

<sup>4</sup> The right to be forgotten is a data protection right which the EU Court of Justice developed in the 2014 "Google Spain" case. In this ruling, the Court established that users can ask search engines to hide certain URLs from search results when a search is conducted using their name: it gives individuals the ability to exercise control over their personal data by deciding what information about them should be accessible to the public through search engines. <https://www.accessnow.org/eu-court-decides-on-two-major-right-to-be-forgotten-cases-there-are-no-winners-here/>

<sup>5</sup> The Chinese government started making tech companies keep a record of the identities of people posting comments online since 2017 to limit internet speech and spread false information <https://www.ft.com/content/1c18614e-eab6-3571-a5fb-c9d7259d3a73>



human rights. We can even use artificial intelligence to predict and head off human rights violations. However, we cannot ignore the dark side. It cannot be expressed more strongly than this: The digital revolution is a major global human rights issue.

## **Statement of the Problem**

### *Gap in the Universal Declaration of Human Rights*

Although the UN General Assembly and the Human Rights Council have affirmed that the same rights exist online and offline, we cannot afford to see artificial intelligence and cyberspace an ungoverned or ungovernable space because it still embodies a gap in human rights. This statement is founded based on actors such as governments and individuals not respecting the conduct that should be used online nor following the Universal Declaration for Human Rights (UDHR) which weakens it to be inadequate.

Although the scale and pace of digital development is surely overwhelming, yet we do need to understand the specific risks. In other words, to further elaborate on the problematic of the paper, we discuss cases of online harassment, trolling campaigns and intimidation that polluted parts of the internet and posed real offline threats. In one of the deadliest cases, social media posts targeted the Rohingya community in Myanmar in the run-up to the mass killings and rapes in 2017 (Stecklow, 2018). In fact, human rights investigators at Reuters found that Facebook and its algorithmically driven news feed had helped spread hate speech and incitement to violence<sup>6</sup> (ibid.). These grave violations of human rights leave no room for doubt. Failure to take action will result in further shrinking of civic space, decreased participation, enhanced discrimination, and a

---

<sup>6</sup> Reuters investigates allocated a special report to the Myanmar massacre under an article named “Hatebook” on their website entitled Mynamar burning. Investigators found more than 1,000 examples of posts, comments and pornographic images attacking the Rohingya and other Muslims on Facebook. A secretive operation set up by the social media giant to combat the hate speech is failing to end the problem.

continuing risk of lethal consequences; in particular for women, minorities and migrants, for anyone seen as “other”.

Nonetheless, the overreaction by government regulators and the use of the online space is also a critical human rights issue. Several countries are limiting what people can access, controlling free speech and political activity, often under the pretense of fighting hate or extremism. Internet shutdowns seem to have become a common tool to suppress legitimate debate, opposition and protests. The NGO Access Now counted 213 shutdowns in 25 states in 2019<sup>7</sup>, almost three times the number (75) recorded in 2016 (AccessNow, 2019). Other states are deliberately ruining the reputations of human rights defenders and civil society groups by posting false information about them or orchestrating harassment campaigns. Others are using digital surveillance tools to track down and target rights defenders and other people perceived as critics.

Alongside these risks, we are also seeing unprecedented risks to the right to privacy. Safeguards around privacy are failing in far too many cases. Many might be completely unaware of who holds their data or how it is being used. And because data is held on a vast scale, the risks and impacts of its misuse are also vast. The dark end of the digital field threatens not just privacy and safety, but undermines free and fair elections, jeopardizes freedom of expression, information, thought and belief, and buries the truth under fake news. Hence, these issues have been multiplying at the

---

<sup>7</sup> Democratic countries, those under authoritarian regimes, and countries in transition have all disrupted internet connections for months at a time. Benin, Zimbabwe, Eritrea, Gabon, and Liberia are some of the countries new to the list in 2019. India tops the list globally of countries that have shut down the internet, with a staggering 121 incidents of shutdowns. Following India, Venezuela was a global “leader” for shutdowns, blocking access to social media platforms at least 12 times in 2019. After Venezuela, Yemen, Iraq, Algeria, and Ethiopia were the countries with the most shutdowns.

digital age with unprecedented cases. Technology and ungoverned internet companies continue to put human dignity at risk and undermine the UDHR which has not been able to fulfill one of its mandate of universally protecting fundamental human rights online.

### **Research Questions**

The framers of the UDHR, led by Eleanor Roosevelt, envisaged three parts to the postwar human rights enterprise: a set of general principles; the codification of those principles into law; and practical means of implementation (Glenn, 2001). Today implementation takes many forms, ranging from top-down monitoring by human rights treaty bodies and adjudication by international courts and tribunals, to capacity building in civil society organizations and human rights education at the grass-roots level. We should recognize that effective implementation includes not only retrospective complaint mechanisms, but also forward-looking efforts to cultivate respect for human rights. This is reflected in the mandate of the Office of the High Commissioner for Human Rights, which is both to promote and protect human rights. The Commission's starting point in considering human rights implementation online and offline raises the question of why the human rights embedded in the UDHR are far from realized today, and what more the international community can and must do to make real the ideal of human rights for all.

- Who has the obligation/ responsibility to reinforce the articles enshrined in the UDHR, that already exists, and make it more relevant to protect human rights at the digital age?

From that statement, a correlation is studied between the internet and the human rights to form the main research question which shall be addressed in the discourse of the study while generating additional sub questions:

- To what extent are human rights being disrupted at the digital age? And how is technology affecting Human Rights?

Since new technology has been empowering individuals, both for good and ill, rights seem more important than ever. And how governments protect them in the digital age will determine whether the internet will be a force that liberates or enchains us. Therefore, the State remains the primary duty-bearer under international law, and cannot revoke its duty to set in place and enforce an appropriate regulatory environment for private sector activities and responsibilities. National legislation and policies must detail how the State's human rights obligations will be discharged at national, provincial and local levels, and the extent to which individuals, companies, local government units, NGOs or other organs of society will directly shoulder responsibility for implementation.

### **Objectives of the Study**

The general objective of the study is to explain the human rights status at the digital age and whether it is being protected by the UDHR or if it should be tailored respectively along with technology on a regular basis. Additional objectives should be studied as well by comparing this study in 3 different countries focusing on Europe, the United States and China recognized respectively as democratic, democratic/republican and authoritarian.

### **Scope and Limitations**

The research is limited to the freedom of expression, data protection and government surveillance, which are some of the main pillars of human rights at the digital age. Hence, the number one limitation of the study was to focus on these three rights and not to widen the scope into discussing the dark web which is as highly important online platform with 60% of illegal activities such as drugs, credit card thefts and criminal acts also putting the human rights at risk (McGuire, 2016). Although the dark web plays a contributing factor in the violation of human rights online, this study will focus on the primary and basic human rights dimensions leading to liberty, equality and

fraternity. Another limitation to writing the paper was working overseas and roving between Middle East countries for job purposes. During that same time, The Covid-19 outbreak also restricted the ability of conducting fieldwork and tightened the window for investigating one on one cases.

### **Significance of the Study**

This study will be a significant endeavor in promoting the protection of human rights online. It will help the community and the society understand the measures taken while participating in online activities and using social media platforms.

Furthermore, the study would serve as a reference for further analysis to be conducted on the same or related area; especially it is fertile ground of the future researches with regard to technology and human rights particularly with regard to assessing the impacts of the internet on user's rights.

### **Methodology**

The research is a qualitative research for it tries to study the influence of the digital age on human rights in the 21<sup>st</sup> century. In order to achieve this method, process tracing is considered a fundamental tool of qualitative analysis followed by an additional tool of comparative studies.

As mentioned above, Europe, the US and China will be subject to a case by case analysis, carried out based on the qualitative data collected from primary sources such as the UDHR, the International Covenant on Civil and Political Rights (ICCPR) and the Customary International Law (CIL). Moreover, the data will be supported by secondary sources from academic articles and official reports. Therefore, China, the United States and the European Union are the dialogue set for discussing the sphere of human rights online.

The reason for designating these states will vary depending on the level of democracy practiced within each territory and how governments can adapt to respecting the freedom and dignity of

individuals at the digital age. The first option being China with an authoritarian system, restricting the use of internet to Chinese citizens and limiting freedom of expression. The United States being a democracy and a republic, using different approaches depending on their interest and national security while enhancing government surveillance. Finally, the European Union which plays an active and leading role in adapting the existing human rights framework to technological developments especially while responding to data privacy and protection online.

## **Chapter 2: Literature Review**

### *Internet Right is a Human Right*

The literature surrounding internet access and human rights, began to accelerate in the last decade as politicians and scholars deliberated on the effects of the role of social media during conflict and in contexts of civil dissent (Arab Spring; Chinese Internet firewall, etc.)<sup>8</sup>, the fear of increasing offensive cyber capabilities and legal questions about targeted internet deprivation. As digital factors increasingly affect human rights dilemmas, the debate turned from individual policy questions to whether internet access itself is a human rights issue. In 2012, internet visionary Vince Cerf asserted that “technology is an enabler of rights, not a right itself” (Cerf, 2012). In contrast to this, scholars echoed Best’s preceding assertion that “a symmetric information right to some extent

---

<sup>8</sup> Social media indeed played a part in the Arab uprisings. Networks formed online were crucial in organizing a core group of activists, specifically in Egypt. Civil society leaders in Arab countries emphasized the role of "the internet, mobile phones, and social media" in the protests. Additionally, digital media has been used by Arabs to exercise freedom of speech and as a space for civic engagement. As for the Chinese Internet Firewall and Before Xi Jinping, the internet was becoming a more vibrant political space for Chinese citizens. But today the country has the largest and most sophisticated online censorship operation in the world.

requires the internet, thus to be excluded from this information technology is, effectively, to be excluded from information, full stop” (Best, 2004).

### *Legal Regulations for Human Rights*

Three main bases have been presented to explain how internet access could gain human right status: 1) Article 19(2) of the ICCPR; 2) Article 19 of the UDHR; and 3) A CIL approach based on the positions of different international bodies. The first approach contends that Article 19(2) of the ICCPR offers sufficiently broad protections that extend to new technologies including the internet: “everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.” This clause uses extremely broad language that supports an expansive interpretation (i.e. “regardless of frontiers”; “through any other media of his choice”). Portions of the legislative history of this treaty indicate that the language was drafted in intentionally broad terms to provide protections that cover future developments (Tenenbaum, 2014).

Although this argument possesses merit, it relies on a legalistic interpretation of ambiguous language drafted more than half a century ago and the argument that it supports a stand-alone right has not gained traction (Haugen, 2014). The second approach is based on a similarly legalistic interpretation of article 19 of the UDHR, which guarantees that: ‘everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers’ (Haugen, 2014). The use of the broad phrase ‘regardless of frontiers’ is tempered by the clause’s technological neutrality, which lacks a focus on specific media and forms of communication. This

argument was debated and effectively rejected by UN bodies in the 1970s and 1980s, UNESCO in particular, in the context of deliberations on a proposed 'right to communication'.

While some scholars continue to claim that this debate was tainted by Cold War rivalries and that a fair reading of the text offers implicit support for a right to communicate in general (Joyce, 2015), it is more commonly accepted that the freedom of expression protections in the ICCPR and UDHR are insufficient to find a positive obligation to access the internet (D'Arcy, 1983). Finally, a third approach argues that the perceived institutional support offered by current senior United Nations (UN) officials and assemblies comprises CIL in support of internet access as a human right. Proponents of this theory point to a 2011 Report by Frank La Rue, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (United Nations, Human Rights Council, 2011), and a 2016 resolution by the United National Human Rights Council that advocated for a "human rights based approach" to facilitating internet access" (United Nations, Human Rights Council, 2016). The specific phrase of La Rue's report that gave rise to such excitement was: "Given that the internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy [...] to make the internet widely available, accessible and affordable to all segments of population" (United Nations, Human Rights Council, 2011) .

### *Internet Access as an auxiliary right*

While, this paragraph does not explicitly state that internet access is a human right, it received strong support by those who claimed that this was the underlying implication (Mathiesen, 2012).



On the other side of the debate, critics insisted that this technology was immune from human rights considerations (Cerf, 2012) and that there were still significant normative challenges that needed to be met before formal recognition could be granted (Tully, 2014). Despite the enthusiasm these statements gathered, these reports do not advocate for a positive right to internet access, but rather constitutes a call for states to adopt policy positions that make internet access available, accessible and affordable.

As the dominant paradigms reviewed above have not gained traction, this research supports a fourth argument that explains the relationship between internet access and human rights; that internet access has become an auxiliary right in support of three primary human rights. Internet access does not originate from the human condition, and to this end, Cerf is right in arguing that internet access is not a primary right (Cerf, 2012). Yet not all rights flow from a person's inherent humanity, nor need they transcend the social conditions in which we live. According to rights theorist Carl Wellman (1999), primary rights can give birth to either derived or auxiliary rights. "Derived rights may be either more specific forms of some generic right, as the freedom of the press is a special case related to the right to free speech; or auxiliary rights that serve to protect some primary right, as the right to habeas corpus<sup>9</sup> serves to prevent a violation of the individual's right to liberty" (Wellman, 1999).

An auxiliary right is a secondary human, or civil or political right with all of the protections and limitations of the primary human (or civil or political) right that it serves. What makes it a secondary right is not its import or authority, but simply that it is born as a result of its connection to a primary right. Just as the right to liberty can be frozen in certain situations, and so the right to habeas corpus would be automatically denied, so too would an auxiliary right to internet access

---

<sup>9</sup> A writ of habeas corpus (which literally means to "produce the body") is a court order demanding that a public official (such as a warden) deliver an imprisoned individual to the court and show a valid reason for that person's detention.

rely on the authority and applicability of any primary rights that it is connected to. The value of this right is that it recognizes modern manifestations of particular rights, preventing a scenario where society protects human rights while forbidding people “to engage in the concrete activities of exercising those rights” (Mathiesen, 2012).

An auxiliary right is clearly not a status that is granted to any supportive tool or technology that assists in the realization of primary rights. Rather, it must be a central and integral component in the realization of the primary right. We adopt the following standard to guide our normative and empirical investigation: An auxiliary right is indistinguishably linked with the primary right, such that in its absence the primary right would lose all value and substance. This test poses an intentionally high standard in respect to the importance of human rights. It is derived from the language of Griffin (2008) who places emphasis on the context and social circumstances in which the right has allegedly formed. An example of this contextual extension of rights is the right to a free press, which was only born following the invention of the printing press, but without which today the right to free expression and the exercise of autonomy would be completely hollow (Griffin, 2009).

### *The Power of Internet on Political, Social, Economic and Cultural Development*

According to International Telecommunication Union (ITU) in 2019, more than half of the world’s population is now online. At the end of 2019, 53.6 per cent of individuals, or 4.1 billion people, were using the internet. This represents an important step towards a more inclusive global information society. In developed countries, most people are online, with close to 87 per cent of individuals using the internet. However, in the least developed countries, only 19 per cent of individuals are online in 2019. Europe is the region with the highest Internet usage

rates, Africa the region with the lowest internet usage rates. (ITU, 2019). The internet is undoubtedly one of the most widespread and commonly used tools for communication and expression. The unique characteristics of cyberspace provide individuals with endless possibilities to deliver their ideas and opinions to anyone willing to listen across borders at relatively low cost, more so than has ever been the case before (Dickerson, 2009).

Some supporters of cyberspace have even gone further, arguing that online space might constitute a restructuring of the political institutions, avoiding state-adopted laws and challenging the territorial sovereignty of nation states (Netanel, 2000). However, it is important to note how the issues related to the internet can be seen through the lens of human rights discourse. Despite the unique nature and characteristics of the internet that enable it to serve as a vehicle for promoting free expression, as well as to bring significant changes in political, social, economic and cultural development (IACHR, 2013), as with any powerful innovation, it also has a great potential for abuse (Dickerson, 2009). Therefore, in particular cases and situations it is necessary to find something of a balance between the proper functioning of the internet and the protection of human rights, including, but not limited to, the right to freedom of expression online and relevant competing interests such as the protection of others' rights and national security interests.

### *Internet and Democracy*

While human rights clearly provide a normative basis for these debates, the perspective of rights itself can be associated with several different normative frameworks. Jorgensen argues that debates on human rights challenges in the context of the internet and information society involve different framings which highlight different human rights aspects: The infrastructure dimension focuses on the internet as a global resource that enables communication; the public sphere perspective

highlight the internet as a public space for democratic participation; the media dimension draws attention to the internet as a new media platform, and its differences with conventional media, and finally the cultural dimension focuses on the social norms and practices of the internet (Jorgensen, 2013).

In the academic literature, several scholars have approached the new digital policy problems from the normative perspective of the public sphere and democratic participation (Dahlberg, 2011). Others have approached the same problems from a distributive justice perspective, emphasizing the importance of equal access and the fair distribution of information resources (Tirosh & Schejter, 2015). Yet another perspective, especially relevant in the debates on digital technologies and development (Kleine, 2014), is provided by the “capabilities” approach to human rights, and its focus on the real communicative opportunities that people enjoy and the structural preconditions that they entail. All of these approaches use the framework of human rights, yet they frame the normative questions differently and focus on different aspects of freedom, equality and rights in the digital era.

### *Digital Rights Groups*

Besides academic debates, a growing range of social movements and digital activism groups have framed their aims and activities in the language of human rights. These movements do not share a fixed conception of digital rights but cover various positions and ideologies.

The spectrum of these movements includes established human rights organization, such as Amnesty International or Human Rights Watch (HRW); more specifically digital rights and information policy oriented organization like the Electronic Frontier Foundation or the internet Rights and Principles Coalition; and even new political parties like the Pirate Parties in different

countries. Many of the digital-rights groups' work still reflects the ideals of the early cyber liberties movements, which largely mobilized against rights violations by governments around the world (Drake & Jorgensen, 2006). Furthermore, newer digital rights movements, such as the Pirate Parties born in Northern Europe, have adopted a different type of thinking, which combines cyber libertarian ideals with "cultural environmentalism" and the notion of "commons" to defend internet culture against both corporate and state colonization (Burkart, 2014). Yet other strands of communication rights activism focus more on the democratic and participatory aims associated with digital technology. The Communication Rights in the Information Society Campaign, for example, which mobilized a range of civil society organizations around the World Summit on the Information Society<sup>10</sup> process in the early 2000s, defended a broader conception of "communication rights", which included not only negative freedoms but also positive rights of individuals to access and effectively deploy information and knowledge to promote democratic participation and the diversity of cultures and identities online (Alegre & Siochru, 2005).

Various groups and movements with less organizational unity and more free-form activities and causes, such as WikiLeaks, Anonymous, and even individual hacktivists, have emerged to defend human rights and freedom of information against various forms of restrictions in the digital world (Brevini, Hintz, & McCurdy, 2013). Many of these have been seen as disruptive forces, which bring attention to a range of injustices and political issues, without necessarily following any specific political program or manifesto. While all of these groups claim to promote human rights, there is also criticism of their activities. Sorell, for example, criticizes the means and forms of

---

<sup>10</sup> The UN General Assembly [Resolution 56/183](#) (21 December 2001) endorsed the holding of the World Summit on the Information Society to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms.

WikiLeaks and Anonymous for lack of transparency, arbitrary selection of causes, and lack of concern for the rights of their “targets”, which can make their activities even “subversive of central tenets of human rights” (Sorell, 2015).

Rather than a specific framework or a paradigm, digital rights can thus be understood as a broad umbrella framing for a host of normative ideals. Beyond their status as existing legal obligations, rights can be articulated with a variety of framings and associations employed by different actors for different purposes. From this perspective, one crucial challenge for research on human rights and in the digital context is to clarify the concrete policy and practical implications of these different alternative visions.

### *Public Sector Vs. Private Sector in the Digital Sphere*

Whereas governments are formally tasked with setting regulatory policies and human rights standards, in the digital environment the public sector often delegates this regulatory responsibility to private actors. Thus, public sector participation in the regulation of human rights in the digital sphere is very limited and primarily relies on private sector such as notice and takedown procedures for enforcement of copyright infringement, defamation or other content that is considered illegal. Various private actors such as the Internet Engineering Task Force (IETF)<sup>11</sup> and the Internet Corporation for Assigned Names and Numbers (ICANN)<sup>12</sup>, as well as platform and service providers such as Google and Facebook, do *de facto* govern and mediate human rights on the internet via their standard contractual clauses and internet design such as Domain Name

---

<sup>11</sup> IETF is a large open international community of network designers, operators, vendors and researchers concerned with the evolution of the internet architecture and the smooth operation of the internet.

<sup>12</sup> ICANN is a not-for-profit public benefit corporation with participants from all over the world dedicated to keeping the internet secure, stable and interoperable. ICANN has an important impact on the expansion and evolution of the internet. See [www.icann.org](http://www.icann.org)

System (DNS)<sup>13</sup> (Zalnieriute, 2017). Yet these actors and internet architecture are mostly invisible in our everyday life. These characteristics and lack of regulatory intervention and public-sector participation have been described as a digital “global default” (Wagner, 2019), whereby private actors establish boundaries to human rights online, most notably freedom of expression, data protection, and privacy, in accordance with their respective business models. And in the context of this indiscriminating global default, the basic tools of accountability and governance both from public and legal pressure, have lost control, with private actors holding most of the power (Buni & Chemaly, 2016).

We assert that there is a void which occurs when human rights are public. In other words, only state actors can be sued for not respecting human rights and the internet architecture, through which human rights online are mediated and governed today, is mainly privately owned or privately operated (Deva & Bilchitz, 2017). Hence, this emptiness creates a human rights gap whereby the delegation of human rights enforcement to private actors avoid both international human rights law and often domestic laws and constitutions as well. In spite of having individual rights such as freedom of speech playing a key role in the design of the internet as we know it, we still see the battle for connecting the internet architecture to the respect and enjoyment of human rights worldwide as a concern.

In conclusion, human rights issues and governance online are not only dependent on internet content but on the underlying system of technological architecture that supports the internet as well. Many aspects constraining the exercise of our fundamental rights online are connected into the technical architecture of the internet and incorporated into a variety of policies and methods from actors creating or managing the design. While end users commonly assume that the internet

---

<sup>13</sup> DNS is a naming database in which internet domain names are located and translated into internet protocol (IP) addresses. The system maps the name people use to locate a website to the IP address that a computer uses to locate a website.

technology is neutral, the implications of the ever-growing privatization of human rights enforcement via internet architecture and private policies by actors, such as social media platforms and ICANN, are huge and profound, not least because such privatization in essence evades the protections afforded to individuals by the international human rights framework. The political and civic power held by these various private actors exercising influence on the internet architecture does not seem to be diminishing; quite to the opposite, it appears to be expanding at a fast pace.

### **Chapter 3: International Legal Framework of Protection of the Right to Freedom of Expression, the Right to Data Protection, and the Right to Privacy**

#### Section A. International Legal Framework

In this first part, we will examine the international and European legal instruments of protection of the rights to freedom of expression and data protection before studying how these rights can be affected online.

The UN Human Rights Council, in a resolution of 2012, affirmed that “the same rights that people have offline must also be protected online” (UN Human Rights Council, 2012). At the international level, freedom of expression is entrenched in the UDHR of 1948 (UN General Assembly, 1948), which applies to the 193 UN members, and in the ICCPR of 1996, which is legally binding on its 169 State parties (UN General Assembly , 1966).



Moreover, Article 19 of the UDHR enshrines freedom of expression in general terms, defining it as a right that includes “freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers”. Article 19 of the ICCPR includes almost the same definition, stating that:

*Everyone shall have the right to hold opinions without interference.*  
*Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice (ICCPR, 1976).*

The same principles apply to all forms of expression online, in this regard, the Human Rights Committee in its General Comment number 34 on Article 19 affirms that “Article 19 of ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression” (Human Rights Committee, 2011). Furthermore, the Joint Declaration on Freedom of Expression and the Internet of 2011 that was issued by the Special Rapporteurs on freedom of expression, draws attention to the fact that “approached to regulation developed for the other means of communication, cannot simply be transferred to the internet” but that “tailored approaches which are adapted to the unique characteristics of the internet” should be developed to deal with illegal content online (Joint Declaration on Freedom of Expression and the Internet, 2011). However, Article 19 in its paragraph 3 admits that freedom of expression is not absolute and that it can be subjected to restrictions under three conditions: the restriction must be provided by law, pursue a legitimate aim and be necessary and proportionate. It translates as follows:

*The exercise of the rights provided in paragraph 2 of this article carries with its special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*

- (a) For respect of the rights or reputations of others;*
- (B) For the protection of national security or of public order, or of public health or morals (ICCPR, 1976).*

With this respect to restrictions, General Comment number 34 notes that:

*Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government (ICCPR, 2011).*

As for data protection, no specific mention of this right is found in the UDHR and the ICCPR. Nonetheless, it is guaranteed through the provisions relating to the right to privacy. Also, it is recognized that the latter includes the core principles of data protection. Article 12 of the UDHR describes the right to privacy in the following terms:

*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks (UDHR, 1948).*

Whereas Article 17 elaborates further more upon this definition stating that:

*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, not to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks (ICCPR, 1976).*

Additionally, the Human Rights Committee has issued General Comment number 16 relating to Article 17 (UN Human Rights Committee, 1988). Among other things, the Committee establishes that effective protection of Article 17 requires states to implement laws providing minimum data protection guarantees, applicable to both public and private entities as follows:

*The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination (ICCPR, 1976).*

## Section B. European Legal Framework

### *The Council of Europe*

Within the Council of Europe, the most important human rights instrument is the European Convention on Human Rights (ECHR) of 1950<sup>14</sup>. The European Court of Human Rights is the international jurisdiction responsible for guaranteeing the respect of the Convention by its 47 Member States (ECHR, 2008). By that token, Freedom of expression is guaranteed under the first paragraph of Article 10 of the Convention by stating the following:

*Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises (ECHR, 1998).*

Equivalently to Article 19 of the ICCPR, the second paragraph provides a three-step test under which a restriction on the right is lawful, namely a test of legality, legitimacy and proportionality. This is explained by the following words:

*The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restriction or penalties as are*

---

<sup>14</sup> Formed in 1949, the Council of Europe is completely separate from the European Union and much larger, with 47 members compared to the EU's 28. The Convention consists of numbered articles protecting basic human rights.

*prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety. For the prevention of disorder or crime, for the protection of health and morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary (ICCPR, 1976).*

As for data protection, there is no specific provision enshrining the right. However again, data protection falls within the scope of the right to private life. Indeed, the European Court has stated that “the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life” (ECHR, 2008).

On this subject, right to private life is guaranteed by Article 8, which reads as follows:

*Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (ECHR, 2018).*

Hence, it is within the framework of the Council of Europe that the first legally binding international instrument in the field of data protection has been adopted. This instrument is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal

Data, commonly called Convention 108, that counts 50 State Parties (Council of Europe, 1981). Accession to the Convention is open to non-member states and Mauritius, Uruguay and Senegal have ratified it (Council of Europe, 2017). The Convention 108 applies to all processing of personal data carried out by public authorities and private entities. It is mainly aimed at protecting individuals against the abuses that the collection and the processing of data can imply, by providing guarantees in respect to the manipulation of these data. Likewise, it seeks to regulate the cross-border flows of personal data (Council of Europe, 1981).

### *The European Union (EU)*

Moving forward to the European Union, the latter has proclaimed the Charter of Fundamental Rights of the European Union in the year 2000 (European Union, 2000). Yet, it was a mere declaration without binding force until the adoption of the Treaty of Lisbon in 2007. Since the entry into force of the treaty, in 2009, the Charter is legally binding on the EU Member States and the EU institutions. With this regard, freedom of expression is entrenched in Article 11, which indicates that the right includes “freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers” (European Convention on Human Rights, 2007).

Concerning the protection of personal data, the Charter stands out from the legal instruments that have been studied above, by granting the right to data protection in a specific provision, besides the one dedicated to the right to private life. The former enshrined in Article 8 of the Charter and the latter in Article 7. Article 8 reads as follow:

*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority (FRA, 2007).*

More importantly, Article 52 sets out conditions under which restrictions to the rights guaranteed by the charter can be considered lawful. These conditions are similar to those we have already seen in the ICCPR and in the ECHR. We must also mention the limited scope of the charter. In other words, according to Article 51, it applies to the EU institutions and to the EU Member States, but to the latter only they implement EU law. However, the Court of Justice of the European Union (CJEU) has interpreted broadly this provision by ruling that when a national law was falling within the scope of EU Law, the charter was applicable (CJEU, 2013).

Also, important instruments regarding the protection of personal data can also be found in EU secondary law. The first one and the text of reference in the field, inspired by the Convention 108 of the Council of Europe, is the Directive of 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (The European Parliament and the Council , 1995). The provisions are applicable to both national authorities and private entities. It sets out rules guaranteeing the non-abusive use of data by these actors and regulating the cross-border flows of data.

Even though, the directive doesn't apply to the police and judicial cooperation in criminal matters. This legal gap has been filled in 2008 with the Council Framework Decision on the protection of

personal data processed in the framework of police and judicial cooperation in criminal matters (The Council, 2008).

Consequently, a reform of the existing system of protection has been adopted, aimed mainly at reconciling the two sets of rules mentioned above and at adapting them to the new technological evolutions (Maubernard, 2016). The new legal framework of reference in the area is constituted of a new General Data Protection Regulation (The European Parliament and the Council, 2016) completed by a Directive (The European Parliament and the Council, 2016) replacing the Council Framework Decision 2008/977/JHA previously mentioned. The Data Protection Regulation would improve the protection regarding the use of data by internet intermediaries operating within the European Union (Mackinnon, Hickok, Bar, & Lim, 2015). The Directive entered into force on 5 May 2016 and the Member States had until 6 May 2018 to transpose it into their national laws. Therefore, the regulation entered into force on 14 May 2016 and became applicable as of 25 May 2018 (European Commission, 2017).

Finally, the specific rules established by the Directive of 1995 and by the NEW Data Protection Regulation will be studied more in depth in the next part. This section will be dedicated to the study of government liability of internet intermediaries in respect, on the one hand, to data protection and, on the other hand, to the content generated by users.

### *Government Liability of Internet Intermediaries*

We have already discussed that states rely more and more on internet intermediaries to advance their policy objectives and require them to police content on their behalf or to provide them data on internet users. To note that internet intermediaries have also their own policies regarding



content restriction and data processing in their terms of service. Thus, these private actors play an increasing role in the protection of data and expression online. In this part of the paper, we will examine the rules laying down their obligations with regard to content generated on their networks and the processing of personal data. Furthermore, the study will analyze legal regimes of liability of internet intermediaries for third party generated content. With respect to the right to protection of personal data, we will mention, as well, the rules aiming at ensuring the conformity of the collection and the processing of data by internet intermediaries with this right. After that, we will look at a new right, the right of delisting, which has implications on both data protection and freedom of expression.

Nonetheless, before getting into the heart of the analysis, an important observation must be made. Legal regimes of liability are implemented by states and impose obligations on internet intermediaries regarding the processing of data or the handling of content online. Intermediaries have to comply with these obligations in order not to be held accountable and face penalties under these specific governments. This type of responsibility has to be distinguished from the liability for human rights violations that can result from the application of these regimes and that must be assessed in the light of international standards of protection of human rights. Indeed, in this latter case, both internet intermediaries and states can bring responsibility upon oneself, depending on the circumstances.

#### *Accountability of internet intermediaries for third party generated content*

As specified above, a growing number of states have put pressure on internet intermediaries to act as “gatekeepers” by removing or blocking content online that they consider illegal or harmful. The most common grounds of measures aimed at restricting content online are the public health and

morality protection, counter-terrorism and national security, the protection of intellectual property rights and the protection of the reputation and personal data of individuals (Council of Europe, 2015).

In a majority of states, this goal has been achieved through legal rule of liability, compelling intermediaries to police content on the behalf of the state. If they refuse to do so, they can expose themselves to accountability for content generated by third parties on their services. The adoption of these specific rules can be explained by the growth of the internet which has increasingly enabled users to interact and post content online. In this context, the presence of illicit content has increased, and the main difficulty is that it is not always possible to prosecute the authors of such content, because of their minority, their financial constraints, their anonymity or their location. Therefore, the new environment required new rules, and the internet intermediaries were easier to be held accountable than the authors, due to the fact that they are known and, generally financially sound (Castets-Renard, 2012). In this context, liability therefore means the “likelihood of intermediaries being sued for damages, issued injunctions, or otherwise charged over illegal content that is created, uploaded or downloaded, stored or distributed on their system” (Horten, 2016).

Undoubtedly, we have to keep in mind that each removal or blocking of content online has an impact on freedom of expression. In fact, both measures affect the right of internet intermediaries to communicate information and ideas created and published by third parties, the right of the creators and publishers to pass such information and ideas and finally the right of the internet users to receive and access them. Hence, since they constitute an interference with freedom of expression, these measures have to meet the requirements prescribed by Article 19, paragraph 3 of

the ICCPR, Article 10 paragraph 2 of the ECHR and Article 52 of the EU Charter of Fundamental Rights. Any restrictions of content should therefore rest on a clear and accessible legal basis, follow a legitimate aim and be necessary and proportionate.

### Section C. Types of Internet Intermediaries

The principal categories of internet intermediaries that will be deliberated in this thesis are internet access providers, web hosting providers, social media platforms and search engines. These mediators play different roles. Internet access providers control and make available to subscribers the physical infrastructure needed to access the internet in return for payment, while web hosting providers rent Web server space and make it possible for websites to be published and accessed online. The term “host” has however taken a more general meaning and refers generally to websites which enable users to post and upload material. Social media platforms allow their users to post content and transmit messages between them. These intermediaries are usually considered hosts for the implementation of liability governments. As for search engines, they perform an essential role in the accessibility of all internet content for all individuals by enabling the latter to search in their data base (Mackinnon, Hickok, Bar, & Lim, 2015).

Moreover, it is essential to note that some internet mediators have substantially enlarged their services and can therefore fall into different categories. For example, Google is most well known as a search engine but besides this service, it has developed Google+ which is a social media platform<sup>15</sup> (Article 19, 2013).

---

<sup>15</sup> Article 19 is an international human rights organization, founded in 1987, which defends and promotes freedom of expression and freedom of information worldwide. It takes its mandate from the Universal Declaration of Human Rights, which guarantees the right to freedom of expression and information.

In this regard, these dissimilarities also impact the business models of the intermediaries. In fact, internet service providers need to be physically present in the same jurisdiction as their users to be able to offer their assistances. Likewise, they have to make consequent investments in resources, equipment and staff within the country in which they operate, and they therefore need state permission and must comply with the domestic laws. For this reason, states have a specific leverage over this type of intermediaries. In contrast, the three other categories of intermediaries raised above do not need to operate within the country of the users to whom they offer their services. For instance, a user in Ethiopia can do research on Google or communicate via Facebook despite the fact that these companies have no equipment or personnel in the country (Mackinnon, Hickok, Bar, & Lim, 2015). Nevertheless, states are considerably trying to impose their laws on these new international actors.

#### Section D. General Models of Liability for third party generated content

In this context, we identify three general models of liability, starting with the strict liability model. Under this government of responsibility, internet intermediaries are accountable for all illegal content they carry and have to constantly monitor the internet in order to avoid liability. If they do not comply with these obligations, they face various sanctions that can range from fines to criminal punishments or the revocation of their business license in the most extreme cases. This model is found for example in China (Article 19, 2013), which will be later discussed in the comparative case studies. Secondly, there is the safe harbor model. In this model, internet intermediaries can escape liability for illegal content processed through their services when several conditions are met. This regime of liability is found for example in the European Union and in the United States which will also be studied later in the thesis. The latter, however, applies only to specific content

such as copyright. With respect to this model, internet access providers who act as no more than channels to provide technical services, benefit from almost full immunity.

However, with regard to hosting providers, social media platforms and search engines, a notice and take down procedure is at the core of the safe harbor regime. According to this procedure, mediators do not expose themselves to liability when they take down content upon notice of its illegal character (Article 19, 2013). Lastly, there is the broad immunity model where internet intermediaries' profit from a large immunity for third party generated content. As such, the United States is the most well-known example of implementation of this model, even though certain types of content are excluded from the scope of this general regime (Article 19, 2013).

#### *The European Union as a liability government*

The EU has adopted legal rules of liability of internet intermediaries for content online, aimed at harmonizing the national laws of its Member States in the field. These rules seek to achieve a fair balance between the necessity to restrict illegal or harmful content online and the need to support the freedom enterprise of internet intermediaries and freedom of expression online. As a result, the regime of liability for third party generated content is provided mainly by two directives: The E-Commerce Directive<sup>16</sup> and the Information Society Directive<sup>17</sup> in some of its provisions. The latter applies to copyright claims and bring one important clarification regarding the general regime of liability included in the E-Commerce Directive. It protects the right of reproduction of copyright holders bur provides “temporary acts of reproduction: whose main purpose is to “enable a

---

<sup>16</sup> The E-Commerce Directive is the legal framework for online services in the Internet Market. The purpose of the Directive is to remove obstacles to cross-border online services in the EU and provide legal certainty to business and citizens.

<sup>17</sup> This Directive of the EU was enacted to implement the World Intellectual Property Organization treaty and to harmonize aspects of copyright law across Europe.

transmission in a network between third parties by an intermediary” is not a violation of that right (The European Parliament and the Council, 2001).

As a result, internet intermediaries cannot be held accountable for such temporary acts of reproduction on their networks. Also, the general regime of liability is provided by the Directive on Electronic Commerce, that we will call the E-commerce Directive. This Directive was developed with the purpose to achieve free movement of information society services within the European Union. Free movement of services is important since it constitutes a part of freedom of expression. In order to reach this free movement of services, it was important to harmonize the national laws with regard to the legal regimes of liability of internet intermediaries in a way to avoid unfair competition and to promote cross-border services between Member States (Baistrochhi, 2003).

Nonetheless, the E-Commerce Directive provides a safe harbor for “information society services” against liability under certain circumstances. According to the Directive, internet access providers, who act as “mere conduits”, meaning that they transmit content regardless of what it is, are not liable for the information conveyed, as long as they do not start the transmission, select the receiver or modify the information contained in the transmission<sup>18</sup> (E-Commerce Directive, 2000). With respect to hosting intermediaries, the directive provides that they are not liable for illegal content stored on their sites or platforms when they have no “actual knowledge” that they are hosting illegal content or when, “upon obtaining knowledge”, they act with speed to remove and disable access to the illegal material<sup>19</sup> (E-Commerce Directive, 2000).

---

<sup>18</sup> Article 12 of the E-Commerce Directive.

<sup>19</sup> Article 14 of the E-Commerce Directive.

Furthermore, the Directive prohibits the imposition of a general obligation to monitor the internet intermediaries<sup>20</sup>. This commitment would require mediators to constantly watch content posted on their networks and remove or block those that seem illegal independently of any notice. The Court of Justice of the European Union has ruled that convincing intermediaries to continuously monitor or take preventive action is not compatible with EU law<sup>21</sup>. In other words, this prohibition applies to both categories of intermediaries by imposing an obligation to “install a system for filtering information which is stored on its servers by its device users; which applies indiscriminately to all of those users; as a preventative measure; exclusively at its expense; and for an unlimited period” and “which is capable of identifying electronics containing musical, cinematographic or audiovisual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright”<sup>22</sup> (Horten, 2016).

Similarly, the so called “stay down” orders are incompatible with the prohibition of the general obligation to monitor. Such order means requiring from internet intermediaries that once illegal content has been removed, they have to ensure that this material never appears again on their platforms. Therefore, for these types of stay down injunctions, it would require a scanning and filtering system which is also very difficult to achieve given the number of files at stake, necessitating it to be made by algorithms rather than by humans. Yet, algorithms do not understand the law and do not differentiate between legal and illegal content but work on the basis of keywords and database matches. Consequently, it increases the chance of error and can lead to the taking

---

<sup>20</sup> Article 15 of the E-Commerce Directive.

<sup>21</sup> CJEU, *Scarlet Extended and Sabam v. Netlog* rulings, 24 November 2011

<sup>22</sup> *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, op.cit.*, § n° 53.

down of legal content. The perspective regarding take down actions has been stated by EU national courts and then has been supported by the Court of Justice of the European Union (Horten, 2016).

Equivalently, the Regulation and Open Internet Access<sup>23</sup> entered into force in 2016. The new Regulation bans internet access providers to voluntary block content. For that reason, it means that from now on, self-regulation mechanisms of internet access providers are prohibited and that every blocking measure has to be ordered by a national authority (The European Parliament and the Council, 2015).

An important note must also be mentioned related to the European Commission which laid down proposals in the framework of the Single Digital Market in 2016, that are targeting internet intermediaries (European Commission, 2015). The reform does not seek to amend the E-Commerce directive but seeks to adopt special measures to impose more responsible behavior on internet intermediaries in particularly sensitive fields such as the fight against terrorism and hate speech. These proposals consist of a “Terrorism Directive” that was adopted in 2017, and an amendment to the Audiovisual Media Services Directive concerning hate speech content online (Horten, 2016). These initiatives very much increase the burden of intermediaries for content linked to terrorism or hate speech and raise particular concerns regarding human rights.

## **Chapter 4: Impact of Internet on Human Rights**

### **Section A. Undermining the freedom of expression online**

---

<sup>23</sup> The Open Internet access Regulation (Regulation (EU) 2015/2120) grants end-users the directly applicable right to access and distribute the lawful content and services of their choice via their Internet access service.



### *Freedom of Expression and the Internet: a new frontier for Human Rights*

The internet is one of the most powerful inventions of the digital age. It has the potential to empower and educate, to cross cultural boundaries and to create global communities. It offers the means for any individual with access to a computer and a gateway to the internet to participate in a free flow of information and ideas with others across the world. Yet, that very potential to surpass national borders and impart information regardless of frontiers means that the internet is also the subject of joint efforts by governments to restrict freedoms and violate basic human rights such as the rights to privacy, freedom of expression and freedom of information (Goldsmith & Wu, 2006).

In some countries where holding different opinions from established doctrines is suppressed, the struggle for freedom of expression is now taking place online as governments allocate increasing resources and attention to controlling access to information on the internet and to surveillance of users. Their objective is often to prevent dissemination of information that is critical of them, as well as to track and monitor dissidents, some of whom may subsequently be imprisoned for exercising their right to freedom of expression (Amnesty International , 2004).

The internet itself can become a tool of repression where the monitoring of communications, the censoring and filtering of information and the collection of immense databanks of information enhance the ability of repressive governments to restrict the freedoms and basic human rights of their citizens. Such national restrictions can affect not just those living in that country but all who seek to communicate or receive information about it.

However, there are some legitimate cases in which restricting access to certain information is an important step in protecting human rights, for example preventing access to child pornography. Nevertheless, international human rights bodies have expressed their deep concern about blocking and filtering measures. In particular, the special mandates on freedom of expression in their 2011 Joint Declaration on Freedom of Expression on the Internet held that mandatory blocking of entire websites is an extreme measure, for example where necessary to protect children against sexual abuse (OHCHR, 2014). As well as content filtering systems imposed by the government or a service provider which cannot be justifiable as a restriction on freedom of expression as long as they are proportionate with international law<sup>24</sup> (Article 19, 2015).

Similarly, the UN Special Rapporteur has recognized that website blocking may be justified in limited circumstances in order to deal with categories of content which are prohibited under international law, namely: child sex abuse or child pornography, incitement to commit genocide, advocacy of national, racial or religious hatred that constituted incitement to discrimination, hostility or violence, and incitement to terrorism (Human Rights Council, 2011). At the same time, these measures aimed at preventing users from accessing certain types of content to protect them as well as preventing them from downloading illegal material and potentially committing an offense. In this sense, blocking and filtering can be framed as measures to combat and reduce criminality.

Yet, before these procedures are adopted or implemented, the key question that must be answered is whether blocking or filtering are necessary and proportionate to tackle the problems they

---

<sup>24</sup> Blocking or filtering are sometimes presented as a remedy to various social ills, from sex abuse images, adult pornography, intellectual property infringement, privacy violations, defamation, illegal gambling, hate speech, terrorism or other national security threats.

supposed to address. Thus, the response very much depends on the technology used for blocking content and its impact on the rights to freedom of expression and privacy, as some technologies are more intrusive than others, and we see some of the examples in the following sections.

### *The role companies play in internet repression: the case of China*

It is fundamental to mention how governments require the assistance of companies that are providers of information and communications technology to fulfil these repressive functions effectively. Hence, this raises questions about the collaboration of these companies in human rights violations that are being committed by states. In such conditions, a company runs the risk of being complicit in a violation through its provision of equipment, technology or services to a repressive government.

While the use of information and communications technology to suppress, protestors for example, has been documented in many countries. It is the example of China that has generated the most public and political concern internationally (Reporters Without Borders, 2016). In part, this is because the structure of internet repression is considered to be more advanced in China than in any other country, and in part, because of the willingness of internet hardware and software companies to cooperate with the Chinese government in their quest to develop a large and profitable market (The OpenNet Initiative, 2005).

The control of the Chinese authorities to maintain over their citizens' rights to freedom of expression and information is continuing and spreading widely. This has put the spotlight on the

contribution of internet companies such as Yahoo, Microsoft and Google<sup>25</sup> to China's efforts to maintain such control and restrict fundamental freedom. In assisting the Chinese administration by complying with its censorship demands, these companies are seen to be facilitating or sanctioning the government's efforts to control the free flow of information. As a result, they violate established international norms and values, and compromise their own stated principles.

Consequently, international concern regarding the role of US companies in China's internet censorship policy has led the US House of Representatives Committee on International Relations to hold a joint hearing of the Subcommittee on Africa, Global Human Rights and International Operations and the Subcommittee on Asia and the Pacific (Human Rights Watch, 2006). Among the parties that provided testimony, views were expressed that US internet companies, including Yahoo, Microsoft and Google, have colluded with the Chinese authorities, undermining their self-proclaimed corporate values, as well as the human right to freedom of expression and information. Subsequently, all three companies have in one way or another participated in the practice of censorship in China.

For example, Yahoo has provided the Chinese authorities with private and confidential information about its users. This included personal data that has been used to convict at least two journalists, considered by Amnesty International to be prisoners of conscience (Amnesty International, 2006). Microsoft has admitted to shutting down a blog on the basis of a government request (Amnesty International, 2006). Google has launched a censored version of its international search engine in China (Amnesty International, 2006). These three intermediaries have demonstrated a disregard

---

<sup>25</sup> Yahoo, Microsoft and Google are American multinational technology companies which provide Web services, develop and sell computer software and specialize in internet-related services and products which include online advertising technologies and a search engine.

for their own internally driven and proclaimed policies. They have made promises to themselves, their employees, their customers and their investors which they failed to uphold in the face of business opportunities and pressure from the Chinese government. This raises doubts about which statements made by these organizations can be trusted and which ones are public relations gestures.

Out of these three companies, Google has come closest to admitting publicly that its practices are in conflict with its principles, and to making a commitment to increase transparency by informing users in China when a web search has been filtered. Although there are many other transparency options that the company should consider, these are important first steps (Amnesty International, 2006).

While each of Yahoo, Microsoft and Google may be considered to be complicit in the Chinese government's denial of freedom of information, Yahoo's actions have, in particular, assisted the suppression of dissent with severe consequences for those affected. The company allowed its Chinese partner to pass evidence to the authorities that was subsequently used to convict individuals, at least two of whom received long prison sentences for peacefully exercising their legitimate right to freedom of expression. Thus, Yahoo appears to have failed to honor its responsibility to ensure that its own operations and those of its partners are not complicit in human rights abuses. This is in breach of widely recognized international human rights principles for companies<sup>26</sup> (Amnesty International, 2006).

---

<sup>26</sup> Avoiding complicity is one of 10 Human Rights principles set down in the UN Global Compact, an initiative of the UN Secretary General involving some 2000 companies and institutions.

### *Human Rights responsibilities of companies*

Understanding the scope of the human rights responsibilities of business is evolving and developing, as seen in the 2005 recommendations of the UN High Commissioner for Human Rights to the UN Human Rights Commission (OHCHR, 2005). While the primary responsibility for respecting and protecting human rights, such as freedom of expression, rests with governments, companies also have human rights responsibilities within their spheres of activity and influence. These responsibilities can be drawn from the UDHR, as well as from international treaties and national legislation, developed earlier in the study. They are reflected in codes of conduct for business developed by inter- governmental bodies, as well as by business associations and individual companies (UN General Assembly, 1948).

Additionally, international law and standards already extend human rights obligations beyond states to individuals, armed groups, international organizations and other private actors. The UN Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights (UN Norms), and their Commentary, adopted by the UN Sub-Commission for the Protection and Promotion of Human Rights in 2003, are the most comprehensive attempt at articulating business responsibilities for human rights (OHCHR, 2005). Although the UN Norms themselves are not legally binding, they constitute a benchmark by which governments and corporations can assess the compatibility of corporate activities with relevant human rights standards.

In other words, four situations explain where an allegation of complicity might arise against a company. First, when the company actively assists, directly or indirectly, in human rights violations committed by others; second, when the company is in a partnership with a government

and could reasonably foresee, or subsequently obtains knowledge, that the government is likely to commit abuses in carrying out the agreement; third, when the company benefits from human rights violations even if it does not positively assist or cause them; and fourth, when the company is silent or inactive in the face of violations (International Council on Human Rights Policy, 2002).

*The case of Shi Tao, a journalist imprisoned for 10 years for sending an email*

A Chinese journalist by the name of Shi Tao, has served a 10-year prison sentence in China for sending an email on 20 April 2004. The content of his text was a summary of a Chinese Central Propaganda Department communiqué orally transmitted to editorial staff at the newspaper where Shi worked. He sent the email using his Yahoo account to the editor of a Chinese pro- democracy website based in the US. On the basis of this email, the Chinese authorities accused Shi Tao of ‘illegally providing state secrets to foreign entities’. He was detained on 24 November 2004 and officially arrested on 14 December 2004. He was sentenced to 10 years’ imprisonment on 27 April 2005 (Amnesty International , 2006)

Therefore, the vaguely worded legal definition of what constitutes a ‘state secret’ gives the Chinese authorities broad discretion to detain those engaged in the peaceful exercise of their right to free expression. According to the transcript of the Changsha Intermediate People’s Court of Hunan Province, Yahoo Holdings in Hong Kong, the US-based internet company, provided account holder information that was used as evidence in the case against the journalist, which resulted in his 10-year prison sentence (Amnesty International , 2006).

Moreover, a representative of Shi Tao's family has filed a privacy complaint with Hong Kong's office for the Privacy Commissioner for Personal Data against Yahoo's Hong Kong subsidiary for its role in the case.

During his detention in Chishan prison<sup>27</sup>, Shi Tao has reportedly been forced to work under harsh conditions. His family has been harassed by the authorities. His wife underwent daily questioning by public security bureau officials and was persistently pressured by her work unit to divorce him, which she eventually did. Tao's uncle and brother have also been under surveillance and harassed both at work and at home, and his mother is also reportedly being closely monitored and harassed as she petitions for his release (Amnesty International , 2006).

Amnesty International considers Shi a prisoner of conscience<sup>28</sup>, imprisoned for peacefully exercising his right to freedom of expression, a right entrenched in international law and the Chinese Constitution.

## Section B. Data Protection and the Right to Privacy

### *The future of privacy is here*

Privacy is an important issue. Imagine living in a world where every move a person makes is recorded. When driving the car to work, the choice of road to take, the choice of music, and the speed while driving to be recorded and stored in databases, which later might be sold to third parties for advertising purposes. Moreover, and while driving, the mobile phone is receiving

---

<sup>27</sup> Chishan Prison houses a number of political prisoners and prisoners of conscience in China's Hunan province. The prison practices reform through labor with prisoners being forced to work in for profit prison industries.

<sup>28</sup> A prisoner of conscience is a person who has been put in prison for holding political or religious views that are not tolerated in the state in which they live.



advertising messages from stores and restaurants nearby with special offers. When arriving to work, the computer system at the office is down due to a denial of service attack. As the system turns back up, the incoming mail is cluttered with unsolicited bulk email, some of it directly connected to the companies that have passed on the way to work. Other data was also stored in a database such as the actual time of entering the office, the document which was operating on the computer and every site visited on the internet as well as the time for the breaks that were taken throughout the day.

In other words, and to some extent, the future is already here, and the privacy is almost damaged. The threats towards privacy in these days have their roots in free market and capitalism. Without the usage of marketing reports and buying patterns the work economy would be affected negatively. The driving force in a capitalistic society is characterized on earning money and that is one of the reasons to why our privacy is violated. In other kinds of societies, the privacy is violated for other reasons. Technology and exchange of electronic information are other reasons to why people's privacy is threatened. The fact that personal information can be stored in databases and that the databases could be cross-correlated is a risk towards privacy. And the fact is that our personal information is a pawn in the companies' profiting games.

### *Online Privacy as a Human Right*

Many people are not concerned about their privacy and most of them feel that they have nothing to hide. But privacy is not just about hiding things, and this is where it becomes a problem. Privacy is about self-possession, independence and integrity. The concept does not give us the right to lock ourselves in and engage ourselves in illegal activities. Instead it gives us the right to decide which

details of our personal lives that are private, and which are public. In that manner, Ross Anderson defines the concept as follows:

*“privacy is the ability and/or the right to protect your personal secrets, it extends to the ability and/or right to prevent invasions of your personal space. Privacy can extend to families but not to legal persons such as corporations”.* (Anderson, 2001)

Furthermore, privacy is one of the most important civil rights in the computerized world. People must have the right to control what information about their lives stay inside their own home and what is spread outside. It is primarily about the power of the individual and the personal privacy is unquestionably under attack. Although it is very important to address these problems, the issue is that we don't know how to fight back.

Therefore, the matter of privacy is extremely debated because people might argue that, in order to enjoy the benefits of modern society, we must give away some degree of privacy. For example, if people want to keep having the advantage of paying for a meal by credit card, then they must accept the routine collection of their purchases in a large database over which they have no control. And this is not new, however it is very similar to the environmental which the society faced back in the 1950's and 1960s where big business advocates said that poisoned rivers and lakes were the necessary costs of economic development, jobs and improved standard of living (Garfinkel, 2001). Today people know that sustainable economic development depends on preserving the environment and it is a prerequisite to the survivability of the human race. Likewise, in order to obtain the benefits of technology, it is more important to use technology to protect personal freedom.

Lastly, invasion of privacy does not emerge out of emptiness because technology itself exists at an intersection between science, the market and society. People create technology to fill specific needs and it is regulated as people and society see fit.

Some engineers set out to build systems designed to destroy privacy and autonomy, and some businesses or consumers would willingly use or purchase these systems if they understood the consequences. What happens often is that the privacy implications of a new technology go unnoticed, and if they are considered, they are misinterpreted. In practice, just a few mistakes can turn a system designed to protect personal information into one that destroys people's secrets (Garfinkel, 2001).

*The role of the government in data protection: Emphasis on the case of the European Union*

One way of keeping technology and the free market from killing individual's privacy is being careful and informed consumers. Equally important, the federal government has a fundamental role to play and could be the best hope for privacy protection.

Accordingly, The European Parliament has introduced the General Data Protection Regulation (GDPR) to regulate the data processing of European citizens. It replaced the 1995 directive (95/46/EC) on the protection of individuals with regard to data processing of personal information. This new regulation requires organizations to reassess the way they handle personal information. The new regulation creates more rights for data subjects and puts more emphasis on what data is collected and processed. Companies are therefore required to change their data processing

activities, update their processing agreements with external parties and renew their governance to fit the requirements of the GDPR (Serdeen, 2017).

As a result, to protect the privacy of data subjects, privacy has been a topic in regulations (Papakonstantinou & de Hert, 2012). These regulations put consequences on company behavior that neglects the privacy of their data subjects. To avoid penalties, companies aim to be compliant to regulations. In other words, compliance can be defined as ensuring that business processes, operations and practice are in accordance with a set of norms, which is the GDPR in this case, and the companies aim to adapt their organizational and information systems to these regulations (Lu, Sadiq, & Governatori, 2007).

Hence, we summarize the legislation of the GDPR with the most significant changes compared to the old directive by starting with the change of scope. By that token, the GDPR proposed a change to the territorial and material scope which are documented in its articles 2 and 3 (The European Parliament, 2016). In general, the GDPR will be applicable to organizations that process personal data in the context of activities of an establishment in the EU, regardless of the processing taking place in the EU or not. Establishments outside the EU who process data concerning EU residents that is related to the offering of goods or services, are also included in the scope of the GDPR.

Moreover, the GDPR describes how data breaches must be notified to data controllers. According to the articles of the European Parliament in 2016, data breach incident is described in the GDPR as being: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”. The data processor is obliged under the GDPR to notify the data controller with undue delay after becoming aware of it (The European Parliament, 2016).

Additionally, the GDPR introduces a Data Protection Officer who is responsible to ensure that he is involved in all issues related to the protection of personal data and considered to be a GDPR specialist. The Data Protection Officer is supported by the data controller and processor in doing his job and he acts as contact point for data subjects concerning issues related to the processing of personal data and to the exercise of data subject rights under the GDPR. Also, a Data Protection Officer is mandatory when data processing is carried out by a public authority or body. The role is obligatory when the core activities of the company consist of large scale processing of sensitive data or regular and systematic monitoring of data subjects on a large scale and he therefore cannot be prevented to perform his duties (Serdeen, 2017).

The GDPR also has Data Protection Impact Assessments which purpose is to identify high risks to the privacy rights of data subjects when their data is being processed. The assessment consists of a description of the processing activities and the actual assessment of these activities. It therefore explains that organizations can respond to these risks by formulating measure to address them: examples of high risk processing are large scale processing of sensitive data and monitoring of behavior (Serdeen, 2017). For instance, corporations might monitor an employee's browsing habits to make sure they aren't using the internet for illicit purposes, and they can also install video surveillance in offices to keep an eye on their whereabouts.

A positive aspect of the GDPR is that a data controller needs to be able to prove that consent to gather and use data has been given by the data subject; and taking consent away must require the same effort as giving the consent (The European Parliament, 2016). With the withdrawal of consent, the subject can revoke access to their personal data and the controller has to remove it, and this is called "The Right to be Forgotten". In this scenario, the controller has to delete personal

data in the following cases: the data subject withdraws consent and there is no legal ground for processing; the personal data is no longer necessary for the purposes for which they were collected; the data subject object to personal data used for direct marketing purposes and there is no overriding legitimate ground for processing; the personal data has been unlawfully processed; the personal data has to be erased to comply with the legal obligations of the Member State and if the personal data concerns a minor (Hall, 2018). However, there are some exceptions to the subjects right to have his or her data removed. This can be the case for reasons of public health and public interest, such as scientific, historical or statistical purposes. The controller, after being notified of the request to erase the data, has to take reasonable steps to ensure that all controllers of the subject's data are informed of this fact (Hall, 2018).

Another additional point is that the new regulation of the GDPR requires companies to prove to have taken privacy into account when designing a new information and this is a key action point discussed in the study. This so-called privacy by design describes how businesses should solely collect data that is necessary for their business goals and not invade people's privacy for other matters. Non-compliance with these regulations can lead to fines which can go up to 20 million euros or 4% of the global turnover of the company (which can be even higher) (The European Parliament, 2016).

In some special cases, such as the rights of children online, they have different rights than regular data subjects. In fact, children are seen as vulnerable individuals in the GDPR, and deserve specific protections, just like in any international law. An example is the new requirements for parents to give consent for their children in specific situations. Another example is the need for notices to be

child-friendly when addressed to children. Although the maximum age of children is not described in the GDPR itself, some rules apply to 16 year olds and younger (The European Parliament, 2016).

### *Data Protection & Human Rights in Germany: Case Study*

At the beginning of the process of the Right to be Forgotten, even as a developer on issue of personal data protection, the German government went against the proposed Right to be Forgotten. German Interior Minister Friedrich argued that the current German law has already offered an excellent model for this, he does not want the proposed EU Regulation to apply to data processing which carried on by governmental authorities. He declared that he supported the individuals self-regulate, trying to avoid the negative effect on themselves as much as possible. He thought the idea of the proposed right is mainly interested in expanding the European Commission's power (SPIEGEL, 2012).

As media start to bring a number of data to online environment, the way in which individuals intend to control over the information has become diverse and contradictory. Therefore, we take a look at how developments of a Right to be Forgotten in Germany affected other countries to carry on the data protection.

In Germany, individuals who have committed crimes, served their sentence and paid their debt, and have the right to get protection of their privacy; while the internet may record their crimes, indicate their identities, and show their offense. In addition, the media has the right to freedom of expression and the public has the right to know. However, as time passes by, the online publisher

who releases the information related to individuals should delete such information; in other words, the individuals obtain a right to be forgotten (Siry, 2012).

In the past years, German Courts have dealt with some cases about criminal offenders after being published, they sued the data controller to take down their information from internet and delete their full name that were mentioned in the online archives. The most famous case is Wolfgang Werlé and Manfred Lauber (Larsen, 2013). They are two half-brothers who were convicted of robbery and murdering Walter Sedlmayr, who is a famous actor in 1993. But the two defendants denied the accusations, afterwards, in 1999, they sued a constitutional complaint to Constitutional Court against their convictions and wanted to overturn the situations. The Constitutional Court held their objection and reviewed that their complaint was not admissible. Then further applications for re-litigation was also unsuccessful. This case caused more public attention in the late 90s.

The offenders were known widely in Germany, and the news broadcast referred to the accused and always mentioned their full names which made the Wolfgang Werlé and Manfred Lauber more notable. With the development of the internet, the news broadcasts were spreading into the online platforms. As the offenders were released on parole, they were worried about the news broadcast to have a side effect on their lives. For that reason, and in order to prevent for them to be stigmatized, they filed a lawsuit in 2007 against website providers, requesting to remove their full names from all articles which somehow connected them to the crimes that they had already served for in prison. After a long time of trials and hearings, the full names of two murders were deleted from news broadcast in German websites. German Wikipedia also removed their full names from



the articles referring to victim Sedlmayr. Nevertheless, the two half-brothers also trying to remove their names from English-language version of Wikipedia was at question.

Correspondingly, many legal professionals in the US think that the action of Wikipedia is protected under the US constitution and the judgement of German Federal Court of Justice has no jurisdiction on US. Thus, they rejected to delete the murderers' names (Larsen, 2013).

From the German case, it indicates that it is difficult to decide whose judgement has priority in US or EU countries. As the world is becoming smaller in the internet environment, the interests are not only direct against domestic areas, but also against non-domestic areas. It will become more interconnected and universal, and more cooperation are needed. In that case, from the German standpoint, the Right to be Forgotten has been applied in society. This is evidence to emphasize the Right to be Forgotten is an important way to protect individuals' privacy.

### Section C. Mass Surveillance and Human Rights

#### *The Businesses behind surveillance*

*"We don't monetize the things we create, we monetize users"* Andy Rubin, co-founder of Android, 2013

The internet has revolutionized our world on a scale not seen since the invention of electricity. Over half of the world's population now relies on the web to read the news, message a loved one, find a job, or seek answers to an urgent question. It has opened social and economic opportunities at a scale and speed that few imagined fifty years ago (Amnesty International, 2019).

Every time people interact with the online world, they leave behind a data trace, a digital record of their activity. When they send an email, the content of the message, the time it was sent, who it was sent to, from where, and a bulk of other information, are recorded and stored in servers and data centers (Levy, 2013). A similar process happens when individuals browse the internet, use an app on their phone, or buy something with a credit card. As more and more aspects of their lives are carried out online, and more and more devices, services and infrastructure are connected to the internet - from cars to toasters to factories, the volume of data monitored is continuing to grow exponentially (Levy, 2013).

Accordingly, the creation of these data trails is simply a by-product of the functioning of computational technology, which relies on processing digital information. But technology companies have long since known the importance of data, finding it an extremely valuable source of information, “the new oil” (Marr, 2018). Respectively, big tech firms such as Microsoft, Apple and Amazon ranked in the top 5 world’s largest companies with a market capitalization of 1.25 US billion dollars in 2020 alone, following Saudi Arabian Oil company, ranking first at 1.6 US billion dollars (Statista, 2020). Thus, the mass harvesting and monetization of data, has meant that surveillance has become the “business model of the internet” (Schneier, 2014).

### *Facebook and Google: Surveillance Businesses*

The services provided by Google and Facebook originate income from the accumulation and analysis of data about people. Instead of charging a fee for their products or services, these businesses require anyone who wishes to use them to give up their personal data instead (Amnesty International, 2019). They are multinational corporations, and as such their operations vary significantly across a wide array of businesses, products and services. However, both companies

share the same core business model, specifically to develop digital products and services that people find useful and then collect extensive data about individuals who use or interact with these platforms (Zuckerberg, 2018). They also use algorithmic systems to analyze vast amount of aggregated data and assign detailed profiles to individuals and groups, to predict people's interests and behaviors. Plus, they aim at selling access to the information to anyone who wishes to target a defined group of people, mainly for advertising and marketing purposes (Zuckerberg, 2018).

Therefore, the rise of data and continuous tracking of people's lives online has created a golden opportunity of surveillance for states, providing authorities access to detailed information on people's activities that would have been unthinkable in the era before the digital age. Likewise, the surveillance based business model of Google and Facebook has succeeded from the approach of not having direct control to the regulation of the industry of technology in key countries such as the United States, and the companies' home states (Schneier, 2015).

Nevertheless, Google and Facebook have exceptional power over people's lives online through having established control over the primary channels that most of the world relies on to engage with the internet. Both companies alongside YouTube and WhatsApp, facilitate the ways people seek and share information, participate in debate, and contribute in society. The businesses' platforms have become fundamental to the modern world and how people interact with each other.

Still, there are some exceptions across different countries, most notably the first country mentioned in the study, China. The Chinese government operates an internet firewall- which is a technical set of controls that determine what applications Chinese users can access and which websites they can see- that sets it apart from the wider internet economy, and that allows the government to maintain a repressive internet censorship and surveillance regime (Amnesty International , 2017/2018). This

implicates that China has a largely separate network of Chinese internet services, with WeChat and Weibo serving almost as the same functions of Facebook, and Baidu serving as the leading search engine in place of Google.

As for the countries other than China, the dominance of Google and Facebook is sharply evident in areas such as 1) social media, where Facebook dominates with 2.45 billion active users each month (StatCounter, 2019), 2) messaging, where WhatsApp (an application owned by Facebook) accounts for 75% market share in mobile messaging outside of China (Statista, 2019), 3) search, where Google dominates search engines with over 90% of all internet searches conducted on its platform (Visual Capitalist, 2018), 4) video, where YouTube (a platform owned by Google) acts as the second biggest search engine in the world (Mushroom Networks, 2018), 5) web browsing, with Google Chrome being the world's dominant browser, making Google the gateway to the entire web (Statista, 2019), 6) mobile platforms, with Android (Google's biggest operating system) having 2.5 billion active Android devices per month (StatCounter, 2019). This makes Google a constant presence on the single most revealing object in a modern person's life, the smartphone. 7) advertising, with both Google and Facebook accounting for more than 60% of online ad revenues worldwide as well as 90% of growth in the digital ad market (AdExchanger, 2018).

Before we conclude, it is also fundamental to mention the governance of states during the coronavirus (Covid-19) pandemic in 2019, 2020 in relation to human rights. States across the world employed far-reaching measures to handle the Covid-19 outbreak. Time and resources were limited, and there was immense pressure to introduce effective measures and to scale them back at the appropriate time. When making these decisions, many states strived to uphold acceptable governance standards. Several countries including South Korea, Singapore and Israel made an

effort to gain better overview by instigating location and tracing confirmed cases with the use of intelligence tracking tools, mobile phone locations, CCTV footage and/or credit card transactions (Morely, 2020).

On one hand, intimidating details about people's lives and whereabouts have been potentially revealed in the process, raising privacy concerns (Zastrow, 2020). On the other hand, several states have been hesitant to employ such measures, leading to a lack of disease outbreak data and lack of contact notification.

Recognizing the need, private companies such as Google and Apple have developed an interface to support such apps (Morely, 2020). Geolocation data are notoriously difficult to anonymize, and there is a risk that individuals may be identified, as some were in South Korea (Zastrow, 2020).

Universal human rights provide limits for the exercise of state authority. The human rights framework is complex and not readily accessible to anyone not specialized in human rights law. However, it is paramount that human rights would be respected during the pandemic as well.

To summarize, the power of Google, Facebook and Apple over the core platforms of the internet poses unique risks for human rights, as explained in the subsequent sections. As the statistics above show, for most people it is simply not feasible to use the internet while avoiding all services of Google and Facebook (Hill, 2019). The dominant internet platforms are no longer optional in many societies and using them is a necessary part of participating in modern life.

*Indirect Manipulation of People's Political Opinions: Cambridge Analytica*

The businesses based on models of surveillance have created a design that has not only significantly minimized and restricted the scope of privacy, but at the same time isolated people from one another, as each individual engages with their own highly personalized experience of the internet, uniquely tailored to them based on algorithmically-driven inferences and profiling (Web Foundation, 2018). As a result, this leaves the door wide open to abuse by manipulating people at large.

Most importantly, the most evident and visible example of how Google and Facebook's capabilities to target people at a detailed level can be misused is in the context of political campaigning, the most high-profile case being the Cambridge Analytica scandal that we explore in details in the next section. Correspondingly, this event provided the same mechanisms and tools of persuasion used for the purposes of advertising and were arranged to influence and manipulate people's political opinions (Tactical Tech, 2018). Accordingly, the use of micro-targeting for political messaging can also limit people's freedom of expression by creating an organized and selected worldview unwelcoming to pluralistic political discourse (Kaye, 2018).

Thus, the use of micro-targeting for political campaigning is particularly problematic because of a lack of transparency or oversight over the messages that are sent and their sender. This leaves open the ability for campaigns to use dark political ads, in which people receive highly tailored messages that are only visible to them, and where it may not be clear what organization or individual is behind them, or what information other people are seeing and receiving.

One of the most popular scandals was Cambridge Analytica, a political data analytics firm that claimed the ability to influence target populations by creating uniquely detailed personality profiles and then tailoring political messaging based on these profiles, otherwise known as a

technique named psychographic targeting<sup>29</sup> (Halprem, 2018). Cambridge Analytica's own marketing stated that the company had profiles on up to 240 million Americans, and that it had 4,000 to 5,000 data points on each voter (BBC News, 2019). Moreover, in 2014, the firm gained access to Facebook profile data that was obtained via an app called "this is your digital life", created by Dr. Aleksander Kogan, a psychology professor at Cambridge University. When Facebook users downloaded the app, they consented for the app to access their personal information (Facebook, 2018). Dr. Kogan's company entered into a contract with a Cambridge Analytica partner, presumed on collecting Facebook data (Cadwalldr, 2018).

At that time, the applications under Facebook's policies could access data not only about users who directly consented, but also personal data from people in those user's social network such as friends (UK House of Commons, 2018). This meant that even though only 270,000 users consented to share their data through Dr. Kogan's app, information from up to 87 million Facebook profiles was afterward improperly shared with Cambridge Analytica, as Facebook later confirmed (Facebook, 2018).

In late 2015, the Guardian reported that Cambridge Analytica was improperly using personal Facebook data for the campaign of US Presidential candidate Ted Cruz (Davies, 2015). The contender had only 40% recognition, but with Cambridge Analytica working for his campaign, he quickly rose to become the national Republican runner-up. The company used psychographics, which referred to as its "magic sauce" to target voters based on personality (Cambridge Analytica, 2018).

---

<sup>29</sup> It is the study of people's attitudes and interests, often studied in conjunction with typical demographic data to build more complete profiles of target market and audiences.

As for 2016, the Donald Trump US presidential campaign hired Cambridge Analytica, which also used psychographic profiles to help the campaign identify target audiences by harvesting more than 50 million Facebook profiles without consent and legal justification. Moreover, the move was not just illegal, but it also affected the result of US election significantly (Unver, 2018).

Data driven elections do not just put democracies at risk, but endangers countries to strengthen the surveillance in future, risking transparency in elections, fair processing, security, accountability and the right to privacy.

### *Terrorism and Mass Surveillance*

Since the 9/11 attacks in New York, the Patriot Act was the first of many changes in the name of national security in the United States. The purpose of this Act was to deter and punish terrorists with surveillance laws that made it easier for the government to spy on ordinary Americans and expand the authority to monitor phone and email communications, collect bank record and track people's activities on the internet (Wyden, 2011). While most Americans thought it was created to catch terrorists, the Patriot Act turned regular citizens into suspects.

Terrorism and the fight against terrorism have become major elements of domestic and international politics. Despite the significance and recurrence of terrorist acts, countries demanded more security. In the last decade, it's become increasingly normal for civil liberties to be eroded and for government agencies to spy on citizens, to collect and store personal information to prevent acts of terrorism however it is fundamental to analyze whether these stored information has actually made states safer.



In the aftermath of 9/11, the US government concluded that the law had not kept pace with technology. It created the Terrorist Surveillance Program, initially to intercept communications to Al-Qaeda (Gaetano, 2009). Officials were confident that if the program had been in place before 9/11, the hijackers could have been stopped (Gaetano, 2009). But soon, the new powers were also used to prove guilt by association. In other words, the FBI used immigration records to identify Arab and Muslim foreign nationals in the US. On this basis, 80,000 individuals were required to register, another 8,000 were called in for FBI interviews, and more than 5,000 locked up in preventive detention. Not one terrorist was in what's been called the most aggressive national campaign of ethnic profiling since World War II (Cole, 2005).

The documents leaked by Snowden in 2013, revealed that US government has been secretly collecting and monitoring billions of electronic communications around the world. Some of these data contained bulk collections of telephone records as well as collections of internet communications inside and outside of the US (Gellman & Soltani, 2013). They showed how the NSA can demand information about users from firms like Microsoft and Google, in addition to their daily collection of data from civilian internet traffic, such as email content and contact lists (Gellman & Soltani, 2013). As a result, instead of focusing on criminals, governments are increasingly turning their attention to everyone.

Nevertheless, if people are looking for a needle in a haystack, adding more hay to the stack isn't going to make it any easier to find the needle<sup>30</sup>. On the contrary, every recent success announced by the NSA, has come from classic target surveillance. Despite high hopes, the NSA surveillance program has not stopped any major terror attack (Makwana, 2020). For instance, one of the Boston

---

<sup>30</sup> An American metaphor indicating that adding more data to the digital systems which if filled with data is not going to have positive outcomes if people were to want to find one specific information.

Marathon bombers was already a target of the FBI (Senate Hearing 113-444, 2014). Hence, what is needed, is not more random data, but better ways to understand and use the information governments have. Spy agencies are also pushing to cripple encryption. In fact, in early 2016, the FBI asked Apple to produce a backdoor program to disable the encryption of a terrorist's iPhone. Apple publicly declined, not only because this tool could be used to permanently weaken the privacy of law-abiding citizens worldwide, but fearing to open the floodgates for states requesting access to a technology used by billions of people; a fear shared by security experts and cryptographers (Cook, 2016). Following that event, the FBI revealed that they had hacked the phone themselves, admitting that they lied to the public about the need for a backdoor. This has questioned the trustworthiness of agencies, especially considering that the NSA, for example, already has the capability to turn on people's iPhone microphones, and activate laptop cameras without owners noticing (Makwana, 2020).

Concerns about this are often met with the argument stated earlier in the study "if you have nothing to hide, you have nothing to fear" (Makwana, 2020). But this reasoning only creates a climate of oppression. In that manner, wanting to keep certain parts of people's life private, doesn't mean they are doing anything wrong instead it means they are expected to live in a democracy. in the United States, protection of privacy has been an objective of public policy for at least a century, and people living there believe that the right to privacy is an important democratic right (Lever, 2006).

Besides, imagining the damage the wrong person could do with all these data and such having easy access to all digital devices is worrying. Anti-terrorism laws allow the authorities to investigate and punish non-terrorism related crimes more aggressively. If law enforcement were given these

powerful tools, the concerned people in power would use them unconditionally. And this is why democratic oversight is very important to human dignity and human rights at the digital age, because if these laws are not used today, they might be used tomorrow.

Moving forward, following the November 2015 Paris attacks which entailed a series of coordinated terrorist offenses, France expanded its already extensive anti-terrorism laws by giving law enforcement greater powers to conduct house raids and place people under house arrest (Human Rights Watch, 2016). Within weeks from these developments, evidence emerged that these powers were being used for unintended purposes, such as suppressing climate change protests. Furthermore, the governments of Spain, Hungary and Poland have introduced more restrictive laws on the freedom of assembly and speech. Freedom of expression and the press in Turkey has been also seriously undermined in the last years, with people sentence to prison by criticizing the government (a similar act seen in the section about the Freedom of Expression in China) (Makwana, 2020).

None of this is effectively helped countries fight terrorism but on the contrary. By letting elected governments limit people's personal freedom, we only led terrorists into winning and into achieving their motives. More dangerously, if states are not careful, they might slowly move towards a surveillance state. Therefore, the data is clear, and the erosion of rights along with mass surveillance, hasn't led to significant successes to date, but it has surely changed the nature of society. Terrorism is a complicated problem without simple solutions: no security devices can prevent criminals from building a bomb in the basement and a principle of proportionality<sup>31</sup> should be kept in mind. Creating master keys to enter millions of phones is not similar as searching a

---

<sup>31</sup> The principle of proportional justice is to describe the idea that the punishment of a certain crime should be in proportion to the severity of the crime itself and should be used as a criterion of fairness.

single house. In most countries, the law already permits a wide range of actions, including targeted surveillance. To take full advantage of the existing potential, countries need better international cooperation and more effective security and foreign policies, better application of present laws instead of new and stricter ones that undermine freedom. It is important that states do not, out of fear, destroy democracy and fundamental rights and liberties.

## **Chapter 5 – Findings of the Study**

We have seen in the structure of this thesis how the expansion and the development of the internet have been great opportunities to consolidate democracy, by putting information within everyone's reach, including individuals who did not have access to mainstream media before, and by allowing everyone to share any type of content online. The public sphere has been significantly enlarged and civil participation increasingly encouraged.

However, the study also showed that the democratic potential of the internet has been challenged by several factors. The first important one is the growing role of private actors in the protection of human rights. These actors, previously referred to as internet intermediaries, can be powerful mediators based on their capacity in the protection of the following rights, in particular, the right to freedom of expression, the right to the protection of personal data and the right to privacy (mass surveillance).

With respect to freedom of expression online, the outcome of content created and published by users on their networks is under private entities' control. When they decide to restrict content online, both the freedom of speech of the creator or publisher of the content and the right to access information of the public are affected. Thus, the guarantees attaching to freedom of expression

under international human rights standards, specifically under the ICCPR and the ECHR, should always be respected. Conversely, we have found that this is often not the case, especially because the decisions restricting content lack transparency, appropriate solutions are lacking, or the judiciary is being excluded from the decision-making process.

As for the protection of personal data, internet intermediaries are in ownership of countless data on their users. These data are a valuable tool both for intermediaries and states. Certainly, they are of great commercial value for the former and an essential part of law enforcement for the latter, in particular for the investigation and prosecution of serious crimes. Yet, the retention and the processing of these data constitutes an interference in the private life of individuals and need to be compatible with international norms on data protection rights.

Regarding mass surveillance and the right to privacy, some companies (such as Facebook and Cambridge Analytica) have publicly reported the requests they receive from governments to remove or include content for specific interests as well as to retain data and provide them to authorities, and these firms have complied without any transparency and with insufficient safeguards against abuses. More importantly, in the context of the fight against terrorism, most users do not even know that governments are monitoring people's activities, and mass surveillance seemed to become the norm more than an exceptional measure.

Therefore, if internet mediators unquestionably have a large influence on the protection of these rights, it became evident as we went along with our analysis that states remain the lead actors in their protection and the main responsible, whether directly or indirectly, of the violations of these rights that occur online. Undeniably, on the one hand, when digital companies want to offer their services on the territory of a state, they have to comply with the domestic laws. If they do not abide

by these national laws, they face sanctions, and at last resort, they can be excluded from the national market by the withdrawal of their license, or when they do not physically operate within this territory. On the other hand, governments have progressively forced intermediaries to control content online that they consider illegal or harmful on their behalf or to hand over data to national authorities.

Consequently, the level of protection of these rights is, therefore, mainly left to the hands of states, whereas the roles of intermediaries, although important, remains limited. To ensure human rights protection online, states have to abstain from adopting legislations that oblige or encourage digital intermediaries to act in a way not consistent with human rights standards. Most of the time it will even be possible to hold regimes liable for violations happening online. In this regard, traditional human rights instruments<sup>32</sup> have not lost their importance and continue to be relevant to protect individuals against human rights violations in a globalized world.

Furthermore, a state can be internationally held responsible for human rights violation only if it is part of human rights treaties. We have analyzed the case of China and its regime of broad censorship, but the state is not part of any human rights binding agreements and can therefore not be held accountable for human rights violations in regard of these instruments. Moreover, the study shows that treaties have been developed to prevent private actors from being complicit of gross human rights violations by making the liable for it. However, the impact of such instruments is limited. Surely, these instruments are not legally binding and rest on the voluntary commitment of

---

<sup>32</sup> International human rights law lays down obligations of governments to act in certain ways or to refrain from certain acts in order to promote and protect human rights and fundamental freedoms of all individuals or groups.

the corporations. Compliance of the latter with the principles laid down on them depends to a large extent on the willingness of the corporations.

In addition, the power of the internet to bring about social change in authoritarian regimes, where human rights are poorly protected, can be limited with enough states' determination. Internet in a globalized world is an influential democratic tool that some authors have seen as a threat for authoritarian regimes, because it is a platform where information is easily spread, and this could have a political impact on the country. And, truly, internet has played a key role in the overthrow of undemocratic regimes in the Arab Spring<sup>33</sup>. Nonetheless, some states, such as China, have so far succeeded in keeping exercising total political control on the internet. Hence, although internet intermediaries are powerful, they are still not powerful enough to bring change in all undemocratic regimes and, despite globalization and internet, states that are sufficiently powerful, stable and determined can remain fully sovereign on their territory. In this context, human rights protection continues to be largely dependent on states.

## **Chapter 6- Recommendations and the Way Forward**

### Section A. Recommendations on Freedom of Expression at the Digital Age in China

Based on the analysis and findings in the previous chapter, showcasing the violations of freedom of expression online, we conclude that China is home to one of the largest and most complex media and information systems in the world. It is a system that often suppresses free expression but also

---

<sup>33</sup> For example, Tunisia, being one of the six countries that experienced major anti-government protests during the 2011 Arab Spring, had the most successful transition because the protests led to both the end of President Zine El Abidine Ben Ali's authoritarian rule and the establishment of a new democratic regime. Tunisian activities mainly used the internet to organize the protests and overcome censorship.

provides opportunities for domestic and international actors to help protect and expand the basic rights of millions of people.

We therefore suggest some of the policy recommendations, particularly to the Chinese government and Communist party, to the technology firms and to the educators and university administrators.

Beginning with the Chinese government and the Communist Party, we propose to publically commit to honoring the freedom of expression provision in the Chinese constitution and lobby for the release of all journalists, bloggers and religious believers who were imprisoned for peacefully and legitimately exercising the right to free speech, and ensure that they are given access to proper medical treatment. To also order officials at local levels to refrain from engaging in harassment or physical violence against journalists or their sources, and instead investigate reported incidents to punish those responsible. Moreover, it is advised to end online censorship that blocks Chinese users' access to global social media platforms and websites that provide news and information regarding political, social, religious and human rights topics. Likewise, to end the practice of requiring social media providers to delete user posts or accounts on topics of public interest by being transparent about the filtering process and make public what words and phrases are filtered and how these words are selected. From the legal perspective, it is recommended to implement international standards from UN bodies and experts regarding freedom of expression, encryption, and surveillance by abolishing the provisions in their national legislation such as the Cybersecurity Law that undermines the freedom of expression and privacy or otherwise violate international standards.

Moving forward with the recommendations for technology firms, we propose they would refrain as much as possible from complying with Chinese government requests, that inhibit freedom of



expression or might compromise the privacy or safety of users. It is thus suggested to establish comprehensive policies to guide employees on how to respond to official request and develop an explicit human rights policy that states the company's support for the Universal Declaration of Human Rights. Additionally, when dealing with Chinese government requests for user information or removal of content, firms are ought to comply with the UN guiding Principles on Business and Human Rights<sup>34</sup> and the Global Network Initiative's Principles<sup>35</sup> on Free Expression.

To apply some of the best practices, it is advised to conduct regular assessments to determine the impact of the company's products and actions on user freedom of expression and privacy. Similarly, firms should refuse to participate in China's World Internet Conference unless it acknowledges respect for international standards and reject any vision of internet governance that is inconsistent with those standards. Regarding transparency, technology companies shall inform users of policies and processes for handling Chinese government requests, whether to remove content, restrict mobile phone applications, or hand over personal information, in a clear and accessible way such as transparency reports for the volume and legal basis of requests and company responses.

More importantly, firms should push back against arbitrary requests for censorship or user information, including through Chinese courts, and note down information related to problem that might affect the rights of those using the company's services. In the same manner, digital businesses should support civil society groups and those who develop technological solutions for avoiding censorship or protecting user information; and cooperate with them to monitor internet

---

<sup>34</sup> An instrument consisting of 31 principles implementing the UN "Protect, Respect and Remedy" framework on the issue of human rights and transnational corporations and other business enterprises.

<sup>35</sup> These Principles provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of these human rights globally.

freedom developments in China to maximize users' opportunities to access blocked social media platforms. Also, companies can ensure that any restrictions on information that are imposed as a result of Chinese legal enforcement do not affect other markets or restrict access to information or freedom of expression for people in other countries, including Chinese speakers.

Finally, when teaching about China in schools or University, curriculums should include a unit on its internet system, which is critically important to the country's economic and political development. By that, it is proposed to offer readings, resources and accounts that inform students about the nature of restrictions on free expression. For example, in international relations courses, provide content on the Chinese Communist Party's influence outside of China, specifically the use of economic power and incentives to achieve political censorship goals.

As for the University leaders, it is recommended they gather regularly to discuss concrete cooperation and the development of common procedures and best practices standards to address the various challenges the government can pose to free expression on campuses. Topics to consider include protecting academic freedom, responding to bullying of lecturers or students who express views contrary to the party line, Chinese government surveillance or intimidation of overseas Chinese students.

### Section B. Recommendations on Data Protection at the Digital Age in EU

As seen in previous sections, we confirm that data protection laws are essential for protecting human rights, most notably the right to privacy, but also many related freedoms that depend on the ability to make choices about how and with whom people share information about themselves.

Therefore, the EU's GDPR continues to be one of the strongest and most comprehensive attempts globally to regulate the collection and use of personal data, by both governments and the private sector. Moreover, if its provisions have been well implemented and enforced across EU's 28 member states since its launch in 2016, it should have inevitably strengthened privacy protections in Europe and potentially far beyond.

Furthermore, scandals involving Facebook and Cambridge Analytica, previously elaborated in the study, have driven for greater controls over how personal data is collected and used; which proves the GDPR's safeguards to be particularly important for human rights in the digital age.

As these regulations provide new ways for people to protect revealing data about their private lives, they also give individuals more control and require businesses, governments and other organizations to disclose more about their data practices and regulate the way they collect, process and store people's data.

However, the GDPR, like any new rule, will become clearer over time as companies challenge practices and interpretations of its requirements. For example, member states of the EU have a certain amount of flexibility in deciding how to apply the law and reflect it in their own national data protection regime. One area in which some variation is expected is the age at which children can themselves consent to the processing of their data without a parent or a guardian. Another type of uncertainty is when the regulation permits organizations to obtain and process a person's data without consent, if the entity's legitimate interests outweigh a person's rights and freedoms. Some of the legitimate interests that corporations can rely on include fraud prevention, information security or possible criminal acts. But direct marketing is also a legitimate interest, raising a potentially much broader category against which the individual's rights would be weighed. Thus,

depending on how the legitimate interests' provision is interpreted, it could create a major loophole allowing data collectors to avoid seeking consent. Fortunately, one safeguard is that the EU member states will still need to apply and enforce the regulation in a way that ensures respect for people's human rights found in the Charter of Fundamental Rights in the European Union.

Moreover, the EU regulation will not reduce mass government surveillance as it allows for government agencies to process personal data without consent if there is a national security, defense or public security concern, which are terms that the regulation does not define. This however does not provide a green light for countries to do whatever they like, but International and regional human rights laws still apply to limit the surveillance and data processing activities of intelligence and law enforcement agencies.

In that context, the EU regulation is likely to become a de facto global standard, much as the previous European Data Protection Directive did, because it will apply to any organization that collects or processes the data of EU citizens, regardless of where the organization is based or where the EU data is processed. It is also possible that non-European countries will copy some of its protections as they modernize or establish data protection laws. For example, Microsoft, Apple and Twitter announced that they could extend at least some of the regulations' protections to their customers worldwide, with varying degrees of detail about which provisions would be applied (Human Rights Watch, 2018).

Based on the analysis of the GDPR, it is therefore recommended that all countries adopt comprehensive data protection laws that place individuals' human rights at their center. The EU regulation is not perfect but still is the strongest data protection regime in force anywhere in the

world. Governments should regulate their private sector's treatment of personal data with clear laws and limit companies' collection and use of people's data to safeguard rights.

Likewise, we see in section B of Chapter 4, how the regulations provide for a "right to be forgotten" to individuals who may ask companies to erase personal data in specific circumstances like if the data is no longer necessary for the purposes for which it was collected, if the individual withdraws consent of objects and there is no justification for keeping it, or if the data was unlawfully processed in breach of the GDPR. This right also applies if the personal data has been made public (refer to the case of convicts in Chapter 4 - section B), raising considerable implementation difficulties given the ease with which online information can be copied and shared across multiple websites in various jurisdictions.

Similarly, the rules provide exceptions, including whether the data processing is necessary for the exercise of freedom of expression and information or for archival or research purposes. However, these exceptions are not well defined in the GDPR, and are left for national legislation to elaborate. Because private platforms risk penalty for non-compliance, the provision may tend to encourage unnecessary or excessive take-downs of content, infringing freedom of expression. In addition, leaving determinations about when processing is necessary for freedom of expression to the decision of companies, rather than impartial tribunals, means there is little procedural alternative for those who wish to continue to have access to information that is removed.

Hence, the GDPR is a key step toward stronger privacy protections, but it will not be effective without interpretation, implementation and enforcement. National authorities will need to respond to complaints, investigate breached and enforce provisions. Also, some data protection authorities might not have enough resources, compared to larger companies, to enforce protections which

could be resolved by allocating convenient financial and human resources to authorities from other member states.

### Section C. Recommendations on Mass Surveillance at the Digital Age in The United States

Arguments over surveillance will remain serious for the foreseeable future. There is no prospect either of mass internet surveillance being accepted by all or being abandoned by the authorities in any modern state. That makes the debate over how that surveillance should happen, what limits should be placed upon it, how it should be overseen and the legislation under which it operates a crucial one.

The Snowden files have shown the need to establish a more precise legal framework for surveillance activities, within and outside national borders. We discuss some possible solutions to minimize negative consequences of mass surveillance as the following.

It is fundamental to review national legislation with a view to adapting the protection of privacy to the challenges posed by technological advances enabling mass surveillance. National law should allow the collection and analysis of personal data, only with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity. Likewise, unlawful data collection and treatment should be penalized and the creation of any other technique that weakens security measures or exploit their existing weaknesses should be strictly prohibited. Moreover, given the particularly strong role played by private businesses in the collection and treatment of personal data, all private institutions and businesses collecting or holding such data should be held to firm security standards.

Furthermore, the political problems caused by spying on “friendly” countries and the possible collusion between intelligence services for finding a way around national restrictions show the need for States to come up with an accepted official manuscript for intelligence services that would put an end to uncontrolled mass surveillance and confine surveillance practices to what is strictly needed for legitimate security purposes. Such manuscript would lay down precisely what is allowed and what is prohibited between allies and partners as well as it could clarify what intelligence agencies can do, how they can cooperate and how “friends” should refrain from spying on each other. Therefore, any form of mutual political or economic espionage must be prohibited without exception because wiretapping allies undermines trust among friendly nations with a price that outweighs any benefits.

Additionally, any intelligence activity on the territory of another member state may only be carried out with that state’s approval within a statutory framework such as for the specific goal of preventing terrorism or other serious criminal acts. However, in no event may mass data be tracked, analyzed or stored, especially if it is data from non-suspected individuals but only information concerning legitimately targeted individuals may be collected on an exceptional basis for specific individual purposes. Any data on individual citizens or economic data that is stored but is not needed for this clearly defined purpose must be deleted or destroyed without delay. And finally, telecommunications and internet companies cannot be forced by intelligence services to grant them unrestricted access to their massive databases of personal data; this should only be possible on the basis of a court order.

Another effective solution would be pervasive encryption<sup>36</sup> to strengthen privacy because mass encryption could be an answer to mass surveillance. And by taking this suggestion a step further, it is recommended to decentralize the internet by encouraging each user to set up his or her own well protected server. This would exclude any form of mass surveillance. Therefore, legitimate targets such as terrorist and organized criminals would have to be court ordered to renounce their encryption, which leads us back to traditional targeted forms of surveillance which were authorized by specific court orders and based on concrete grounds for suspicion.

Consequently, improving the protection of whistle-blowers should remain fundamental. Snowden's revelations have been essential for the public to become aware of intelligence agencies' mass surveillance programs and have produced the much-needed discussion about the extent to which the public's civil rights and privacy should be sacrificed in the name of national security. Also, the activities of secret services are by nature difficult to scrutinize by any of the usual judicial means. Therefore, whistle-blowers may constitute the most powerful deterrent against serious violations of the legal limits under surveillance and shall be protected.

In summary, the study has shown the extent of the threat mass surveillance represents on people's privacy and other human rights whose effective exercise depends on privacy, such as freedom of expression and information, even freedom of religion, the right to a fair trial and the right to equal treatment. No one is safe from being inspected by their own countries and even from foreign intelligence unless the generalizing of the use of secure technologies is successful. Before the ever-growing industry of mass surveillance drives completely out of control, people act, in order to subject surveillance to the rule of law. This will require a thorough review of the relevant national

---

<sup>36</sup> The process of turning data and private information into codes.



legislation in most. In addition, in order to be credible, the national and international legal framework must be enforced by reliable control mechanisms including the protection of whistle-blowers who disclose any violations.

As we have seen in the thesis, mass surveillance is not an effective tool in the fight against terrorism and organized crime, compared to traditional surveillance. Similarly, some aspects of mass surveillance, such as the deliberate weakening of encryption and other internet safety standards for the purposes of facilitating data collection, present a serious danger for national security. Such weaknesses can be detected and exploited by rogue States, terrorists, cyberterrorists and ordinary criminals to inflict enormous damage on our societies. It follows that there is no contradiction between the protection of privacy and of national security, on the contrary: data protection and internet security are necessary for our safety.

## **Chapter 7 – Conclusion**

It is vital that States and the UN human rights mechanisms of which they are members and subjects, recognize the importance of protecting and promoting the right to privacy, both as an essential end in itself, and as a fundamental prerequisite to free expression, thought and information. With each new piece of technology, a dangerous game emerges, while increased connectivity also leads to a greater chance of a breach of confidentiality. That is why the Special Rapporteur calls upon the UN human rights mechanisms to update their conceptualizations of the right to privacy in the context of new technologies. Without this, existing protections will not just become outdated. Rather, delay to re-conceptualize how people's privacy is protected will leave the door wide open

for States to abuse new technology, violating rights in the process, all because those with the power to do so refused to act.

Correspondingly, any State that is serious about promoting the right to free expression must get serious about promoting the right to privacy. A free and open press is nothing if the journalists writing for the papers are at risk of surveillance; if the individuals who read the online news sources are being tracked and their data recorded. Just as security cannot be used to justify the suppression of minority opinions, so too it must not be used to justify the monitoring, profiling, tracking and general unwarranted interference with individuals' lives, autonomy, and the development of their personalities. Privacy is the fundamental barrier that stands in the way of complete State control and domination. Without it, the social contract is broken, and individuals cannot recognize their democratic rights to participate, build, grow and think. A community unable to form or communicate private thoughts without the interference of the State will not only be deprived of their right to privacy, they will be deprived of their human dignity. For the ability to freely think and impart ideas is essential to who we are as human beings.

## Bibliography

- AccessNow. (2019). *#KeptOn: What is an internet shutdown?*
- AdExchanger. (2018, May). Digital Ad Market Soars To \$88 Billion, Facebook And Google Contribute 90% Of Growth.
- Alegre, A., & Siochru, O. (2005). *Communication rights. In A Ambrosi, V Peugeot & D Pimienta (eds.), Word matters. Multicultural perspectives on information societies, C&F editions, Caen.*
- Amnesty International . (2004, January). China: People's Republic of China, Controls tighten as Internet activism grows. *Amnesty International reports on cyber-dissidents.*
- Amnesty International . (2006). Amnesty International's briefing on freedom of expression and the death penalty in China. *EU-China Human Rights Dialogue (25-26 May 2006).*
- Amnesty International . (2017/2018). Annual Report: China Country Profile.
- Amnesty International. (2006, July). Undermining freedom of expression in China.
- Amnesty International. (2019). SURVEILLANCE GIANTS: HOW THE BUSINESS MODEL OF GOOGLE AND FACEBOOK THREATENS HUMAN RIGHTS.
- Anderson, R. (2001). "Security Engineering - A Guide to Building Dependable Distributed Systems".

- Article 19. (2013). *"Defending Freedom of Expression and Information, Internet Intermediaries: Dilemma of Liability"*. Free World Center.
- Article 19. (2015, May 4). Joint Declaration on Freedom of Expression and Responses to Conflict Situation.
- Bachelet, M. (2019, October 17). Human rights in the digital age - Can they make a difference? *UN High Commissioner for Human Rights Japan Society*.
- Baistrochhi, P. (2003, January 1). «Liability of Intermediary Service Providers in the EU directive on Electronic Commerce ». *Santa Clara High Technology Law Journal*, 19(1), 3-112.
- BBC News. (2019, January). Cambridge Analytica parent firm SCL Elections fined over data refusal.
- Best, M. (2004). *Can the Internet be a human right*. (Vol. 1). Human Rights & Human Welfare.
- Brevini, B., Hintz, A., & McCurdy, P. (2013). *Beyond Wikileaks: Implications for the future of Communications*. Palgrave, Basingstoke: Journalism and Society .
- Buni, C., & Chemaly, S. (2016). *"The Secret Rules of the Internet. The Murky History of Moderation, and How it's Shaping the Future of Free Speech."*. (T. Verge, Ed.)
- Burkart, P. (2014). *Pirate Politics. The Information Policy Contests*. Cambridge, MA: MIT Press.
- Cadwalldr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.
- Cambridge Analytica. (2018, October 27). The Power of Big Data and Psychographics.
- Castets-Renard, C. (2012). *"Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet"*. Recueil Dallo.
- Cerf, V. (2012). *Internet Access is not a human right* (Vol. 4). New York Times.
- CJEU. (2013, February 26). Åklagaren v.Hans Åkerberg Fransson.
- Cole, D. (2005, May 10). TESTIMONY OF PROFESSOR DAVID COLE BEFORE THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY ON THE USA PATRIOT ACT.
- Cook, T. (2016, February 16). A Message to Our Customers.
- Council of Europe. (1981). Handbook on European Data Protection Law. 16.
- Council of Europe. (1981, January 28). The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- Council of Europe. (2015). "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet". 14-16.
- Council of Europe. (2017, June 4). Chart of signatures and ratifications of Treaty 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
- Dahlberg, L. (2011). *'Re-constructing digital democracy: An outline of four "positions"'* (Vol. 13). New media & society.
- D'Arcy, J. (1983). *An ascending progression. The right to communicate: A new human right*. Dublin: Boole Press.
- Davies, H. (2015, December 11). Ted Cruz using firm that harvested data on millions of unwitting Facebook users.
- Deva, S., & Bilchitz, D. (2017). *Building a Treaty on Business and Human Rights: Context and Contours*. (C. U. Press., Ed.) Cambridge , UK.
- Dickerson, N. (2009). *What makes the Internet so special? And why, where, how and by whom should its content be regulated?* (Vol. 1). Houston Law Review.

- Drake, W., & Jorgensen, R. (2006). *'Introduction', in Human Rights in the Global Information Society*. Cambridge, MA: MIT Press.
- ECHR. (1998). Article 10: Freedom of Expression. *European Convention for the Protection of Human Rights*.
- ECHR. (2008, December 4). *S. and Marper v. The United Kingdom*.
- ECHR. (2018). Article 8. *Respect for your private and family life*.
- E-Commerce Directive. (2000, July 17). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
- E-Commerce Directive. (2000, June 8). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). *Directive 2000/31/EC of the European Parliament and of the Council*.
- European Commission. (2015, May 6). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market for Europe.
- European Commission. (2017, June 5). "Reform of EU data protection rules".
- European Convention on Human Rights. (2007). Article 11. *Official Journal of the European Union C 303/17 - 14.12.2007*.
- European Union. (2000, December 18). Charter of Fundamental Rights of the European Union.
- Facebook. (2018, April 4). An Update on Our Plans to Restrict Data Access on Facebook.
- Facebook. (2018, March). Suspending Cambridge Analytica and SCL Group From Facebook.
- FRA. (2007). Article 8. *Protection of personal data*.
- Gaetano, J. (2009). The 9/11 Attacks—A Study of Al Qaeda's Use of Intelligence and Counterintelligence, *Studies in Conflict & Terrorism*. 32(2), 171-187.
- Garfinkel, S. (2001). "Database Nation - The Death of Privacy in the 21st Century".
- Gellman, B., & Soltani, A. (2013, October 30). NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say.
- Goldsmith, J., & Wu, T. (2006). Who controls the internet? Illusions of a borderless World. *Oxford University Press*.
- Griffin, J. (2009). *On Human Rights*. Oxford University Press.
- Hall, H. (2018). "Restoring Dignity and Harmony to United States- European Union Data Protection Regulation." *Communication Law and Policy*, 23(2), 125-157.
- Halprem, S. (2018, March 30). Cambridge Analytica and the Perils of Psychographics.
- Haugen, H. (2014). *Is Internet Access a Human Right for Everyone, or only for Persons with Disabilities?* (Vol. 1). Kritisk juss.
- Hill, K. (2019, January). Goodbye Big Five.
- Horten, M. (2016). "Content 'responsability' : The Looming Cloud of Uncertainty for Internet Intermediaries". Center for Democracy and Technology.
- Human Rights Committee. (2011, September 12). General Comment No 34.
- Human Rights Council. (2011, April 8). Resolution 16/4. *Freedom of opinion and expression: mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*.

- Human Rights Watch. (2006, August 10). Race to the Bottom: Corporate Complicity in Chinese Internet Censorship. *C1808*.
- Human Rights Watch. (2016, February 3). France: Abuses Under State of Emergency.
- Human Rights Watch. (2018, June 2018). The EU General Data Protection Regulation.
- IACHR. (2013). *Freedom of Expression and the Internet*. Washington D.C: Office of the Special Rapporteur for Freedom of Expression Inter-American Commission on Human Rights.
- ICCPR. (1976, March ). *Article 19*.
- ICCPR. (1976). *Article 19, Paragraph 3*.
- ICCPR. (1976). Article 17.
- ICCPR. (2011). General comment No. 34: Article 19: Freedoms of opinion and expression.
- International Council on Human Rights Policy. (2002, February ). Beyond Voluntarism: Human rights and the developing international legal obligations of companies. 125-136.
- ITU. (2019). *Measuring digital development Facts and figures*. ITU Publications.
- Joint Declaration on Freedom of Expression and the Internet. (2011, June 1). The UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR.
- Jorgensen, R. (2013). *Framing the Net. Human Rights and the Internet*. Cheltenham: Edgar Elgar.
- Joyce, D. (2015). *Internet Freedom and Human Rights* (Vol. 2). European Journal of International Law.
- Karen, N. (2005). *Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet*. (Vol. 2). University of Ottawa Law and Technology Journal.
- Kaye, D. (2018, August 29). *Promotion and protection of the right to freedom of opinion and expression*.
- Kleine, D. (2014). *Technologies of Choice? ICTs, Development, and the Capabilities Approach*. Cambridge: MIT Press.
- Larsen, K. (2013). Europe's "Right To Be Forgotten" Regulation May Restrict Free Speech, 17 FIRST AMENDMENT & MEDIA LITIG. 1-13.
- Lever, A. (2006). Privacy Rights and Democracy: A Contradiction in Terms? *Contemporary Political Theory*.
- Levy, S. (2013, January 8). The Inside Story of the Moto X: The Reason Google Bought Motorola. *Wired*.
- Lu, R., Sadiq, S., & Governatori, G. (2007). Compliance Aware Business Process Design. In 3rd International Workshop on Business Process Design.
- Mackinnon, R., Hickok, E., Bar, A., & Lim, H.-i. (2015). *Fostering freedom online: the role of Internet intermediaries*. UNESCO.
- Makwana, S. (2020, January 6). Comps, Computer Science, concerning, Cyber security, Data Privacy. *Terrorism and Data Privacy*.
- Marr, B. (2018, March 5). Here's Why Data Is Not The New Oil.
- Mathiesen, K. (2012). *The human right to Internet access: A philosophical defense* (Vol. 18). International Review of Information Ethics.
- Maubernard, C. (2016, July). "La protection des données à caractère personnel en droit européen: de la vie privée à la vie privée numérique". *RUE*, 5.

- McGuire, D. M. (2016). *Into the Web of Profit*. University of Surrey.
- Morely, J. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature* (582), 29-31.
- Mushroom Networks. (2018). YouTube: The 2nd Largest Search Engine.
- Netanel, N. (2000). *Cyberspace self-governance: A skeptical view from liberal democratic theory* (Vol. 2). Calif. Law Rev. .
- OHCHR. (2005). *Business and human rights* . United Nations Human Rights Office Of The High Commissioner.
- OHCHR. (2005). *Special Representative of the Secretary-General on human rights and transnational corporations and other business enterprises*. United Nations Human Rights Office Of The High Commissioner.
- OHCHR. (2014). ARTICLE 19, Global Campaign for Free Expression and the Centre for Law and Democracy. *Joint Declaration on Freedom of Expression and responses to conflict situations*.
- OHCHR. (2014). *Internet Rights and Principles Dynamic Coalition* (4th ed.). UN Internet Governance Forum.
- Oozeer, A. (2014). *Internet and social networks: Freedom of expression in the digital age*. (Vol. 2). Commonwealth Law Bulletin.
- Papakonstantinou, V., & de Hert, P. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*. 28(2), 130-142.
- Reporters Without Borders. (2016, January 25). *List of the 13 Internet enemies*. Retrieved from [rsf.org: https://rsf.org/en/news/list-13-internet-enemies](https://rsf.org/en/news/list-13-internet-enemies)
- Schneier, B. (2014, April). Surveillance is the Business Model of the Internet.
- Schnneier, B. (2015). Data And Goliath. *"governments don't really want to limit their own access to data by crippling the corporate hand that feeds them"*.
- Senate Hearing 113-444. (2014, April 30). LESSONS LEARNED FROM THE BOSTON MARATHON BOMBINGS: IMPROVING INTELLIGENCE AND INFORMATION SHARING.
- Serdeen, X. (2017). Managing the Change: a Multiple Case Study on How Large Organizations are Adapting to the General Data Protection Regulation.
- Siry, L. &. (2012). 'A Right to Be Forgotten?-How Recent Developments in Germany May Affect the Internet Publishers in the US'. *European Journal of Law and Technology*, 3(1), 1-12.
- Sorell, T. (2015). *'Human Rights and Hacktivism. The Cases of Wikileaks and Anonymous'* (Vol. 7). Journal of Human Rights Practice.
- SPIEGEL. (2012, 10 17). "The Right to Be Forgotten" US Lobbyists Face Off with EU on Data Privacy Proposal.
- StatCounter. (2019, October). Mobile Operating System Market Share Worldwide.
- StatCounter. (2019, October). Social Media Stats Worldwide.
- Statista. (2019, September). Global market share held by internet browsers 2012-2019.
- Statista. (2019, July). Most popular global mobile messenger apps 2019.
- Statista. (2020, August 19). Top companies in the world by market capitalization 2020.
- Stecklow, S. (2018). *Inside Facebook's Myanmar operation Hatebook*. Rohingya: Reuters .
- SupremeCourt. (1919). *Abrams v. United States* (250 U.S. 616 (1919)).
- Tactical Tech. (2018, April 20). The Influence Industry: The Global Business of Using Your Data in Elections.

- Tenenbaum, J. M. (2014). *Is There a Protected Right to Access the Internet?* International Journal of Constitutional Law Blog.
- The Council. (2008, November 27). Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.
- The European Parliament. (2016). General Data Protection Regulation. (*Regulation (EU) 2016/679*). *Official Journal of the European Union*, 59, 1-88.
- The European Parliament and the Council . (1995, October 24). Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 31-50.
- The European Parliament and the Council. (2001, May 22). Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society . 10-19.
- The European Parliament and the Council. (2015, November 25). Regulation 2015/2120 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation No 531/2012 on roaming on public mobile communications networks within the Union.
- The European Parliament and the Council. (2016, April 27). Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. 89-131.
- The European Parliament and the Council. (2016, April 27). Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. 1-88.
- The OpenNet Initiative. (2005). *Internet Filtering in China 2004-2005: A Country Study*. [http://www.opennetinitiative.net/studies/china/ONI\\_China\\_Country\\_Study.pdf](http://www.opennetinitiative.net/studies/china/ONI_China_Country_Study.pdf).
- The UN Special Rapporteur on Freedom of Opinion and Expression. (2011, June 1). *Joint Declaration on Freedom of Expression and the Internet*.
- Tirosh, A., & Schejter, N. (2015). *"Seek the meek, seek the just": Social media and social justice'* (Vol. 39). Telecommunications policy.
- Tully, S. (2014). *A Human Right to Access the Internet? Problems and Prospects* (Vol. 2). Human Rights Law Review.
- UDHR. (1948). *Article 12*.
- UK House of Commons. (2018, July). Interim Report into Disinformation and 'fake news', *Digital, Culture, Media and Sports Committee*.
- UN General Assembly . (1966, December 16). International Covenant on Civil and Political Rights.
- UN General Assembly. (1948, December 10). Universal Declaration of Human Rights.
- UN Human Rights Committee. (1988, April 8). General Comment No 16.
- UN Human Rights Council. (2012, July 5). The promotion, protection and enjoyment of human rights on the internet. *UN Doc*.



- UNGA. (1996a). *ICCPR*.
- United Nations, Human Rights Council. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Frank La Rue.
- United Nations, Human Rights Council. (2016). Frank La Rue.
- Unver, A. (2018, April 3). Politics of Digital Surveillance, National Security and Privacy.
- Varden, H. (2010). *A Kantian Conception of Free Speech*. (In: GOLASH, D. ed.). (Springer, Ed.) Dordrecht, Netherlands.
- Visual Capitalist. (2018, April). This Chart Reveals Google's True Dominance Over the Web.
- Wagner, B. (2019). *"Governing Internet Expression: Sketching Out the Borders of a Global Default of Freedom of Expression."* (B. Wagner ed., Vol. 36). (C. Springer, Ed.)
- Web Foundation. (2018). The Invisible Curation of Content. 5.
- Wellman, C. (1999). *The proliferation of rights: moral progress or empty rhetoric*.
- Wyden, R. (2011, May 2011). *Statement of Senator Wyden On Patriot Act Reauthorization*.
- Zalnieriute, M. (2017). *"The Anatomy of Neoliberal Internet Governance: A Queer Critical Political Economy Perspective."* (De. Otto ed., Vol. In Queering International Law). (Routledge, Ed.) New York, USA.
- Zastrow, M. (2020). South Korea is reporting intimate details of COVID-19 cases: has it helped? *Nature* , 18.
- Zuckerberg, M. (2018). Internal Facebook records describe data-sharing deals that benefited more than 150 companies.