University of Montpellier

European Master's Degree in Human Rights and Democratisation
A.Y. 2016/2017

The Role of Internet Intermediaries in the Protection of Freedom of Expression and Personal Data

Human Rights in a Digital Age

Author: Louise Timmermans
Supervisor: Christophe Maubernard

ABSTRACT

The phenomenon of globalization has led to the emergence of powerful private actors on the international scene, capable of competing with the traditional powers of states in all fields, including that of human rights. In the world of internet, these new actors, that we will call internet intermediaries, have increasingly been playing a key role in the protection of freedom of expression and of personal data. On the one hand, they have adopted private rules regarding content restriction on their networks and the processing of data. On the other hand, states have been more and more relying on these actors to carry out their policies, mainly by requiring them to restrict content that they consider illegal or harmful or to hand over data to national authorities. The growing role that private actors play in freedom of expression and data protection raises concerns from a human rights perspective. Indeed, traditional human rights law has been designed to apply to states and not to private actors. However, new ways have emerged to ensure human rights protection online through the extension of the scope of state's traditional responsibilities and the development of new instruments specifically addressed to private actors.

TABLE OF CONTENTS

INTRODUCTION

In the age of globalization, cross-border activities between individuals, governments, businesses and institutions have been steadily growing, going hand in hand with the progressive erasure of national borders and the erosion of the sovereignty of nation-states. The development of the internet has been a decisive factor in the acceleration of this phenomenon. Indeed, the internet in itself has become a global industry but it has also enabled other industries' cross-border expansion by allowing economic and political actors to have an almost instantaneous view of what is happening worldwide.

In this context, transnational corporations have become considerably powerful, competing with the regal powers of the sovereign states in numerous areas. Human rights are not an exception to the rule: global corporations have been playing an increasing role in their protection. In the world of the internet, internet corporations have a decisive impact in particular on the freedom of expression and the right to the protection of personal data, the latter traditionally included in the right to privacy. From a human rights perspective, the development of the internet has both upsides and downsides.

On the one hand, the internet has allowed individuals to share and access information and to communicate in an unprecedented way. The fifteenth century printing revolution has allowed the rise of the book that in turn has enabled the expansion of democratic ideas through the dissemination of information and a new relationship to knowledge. The digital age has marked a new stage in the broadening of the public sphere. Whereas on the one hand, access to knowledge and information has been amplified without limits, on the other hand, individuals have been empowered to participate in public affairs and to enhance their place within society. Hence, the internet has been a powerful egalitarian impulse where the logic of democracy has been led to its peak.[1]

On the other hand, some human rights have been increasingly likely to be subjected to various abuses. This is the case in particular of the freedom of expression and the right to data protection. States are more and more relying on internet intermediaries to carry out their policies by requiring them to restrict content online that they consider illegal or harmful or to

[1] Benjamin LOVELUCK, "Internet, vers la démocratie radicale?", *Gallimard I Le débat, 2008/4 n° 151*, 2008, pp. 156-160.

hand over data on citizens. This is particularly true in the current context of the fight against terrorism. Meanwhile, internet intermediaries have adopted terms of service policies in which they have their own rules with regard to content restriction and data processing. We will see that the handling of content and data by private actors often raises concerns regarding the international standards of freedom of expression and privacy. The internet therefore represents a tremendous opportunity to enhance democracy, but can also constitute a threat for democracy if human rights are not adequately protected online. In this regard, it has to be underscored that freedom of expression is of particular importance in a democracy. The European Court of Human Rights has stated repeatedly that "*freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for each individual's self-fulfilment*"[2].

Since internet corporations have become major actors for human rights protection, there has been a growing awareness of the need for corporate human rights accountability. It should be emphasised that multinational corporations are in a difficult position when it comes to states and international human rights standards: their activities extend to the territory of numerous states and each of the latter except them to comply with their domestic laws which in turn are, to varying extents, in line with international human rights standards.[3]

Consequently, international human rights law appears to be the best option to ensure corporate human rights accountability. However, human rights law has emerged in reaction to state power and is therefore traditionally addressed to state institutions. Indeed, the first human rights texts have been redacted in order to prevent the sovereigns from interfering with the freedoms of their citizens. This can be illustrated by the French Declaration of the Rights of Man and of the Citizen of 1789, adopted after the French revolution and aimed at ending the *Ancien Régime*, characterised by the political system of absolute monarchy and by the privileges of the nobility. Its authors were largely inspired by the ideals of the philosophers of the Enlightenment, such as Montesquieu and its doctrine of separation of powers, or Rousseau and its social contract theory. The first international human rights instrument was the Universal Declaration of Human Rights of 1948, largely inspired by the French Declaration. It was adopted after the Second World War and sought to ensure that the atrocities committed by states during the conflict would never occur again.

[2] See for example: ECtHR, 8 July 1986, *Lingens v. Austria*, app. n° 9815/82..
[3] Rebecca MACKINNON, Elonnai HICKOK, Allon BAR, Hae-in LIM, *Fostering Freedom Online: the Role of Internet Intermediaries,* Unesco and Internet Society, 2014, p. 15.

The state was therefore traditionally seen as the main threat to the enjoyment of rights and freedoms, which is why human rights instruments have been developed to limit its powers. Hence, new instruments had to be developed to take into account the increasing influence of private actors in a further globalized world, considering the threat they could pose for the enjoyment of human rights. We will see that there have been some initiatives in the sense of a greater corporate accountability, but that the legal instruments that have been adopted belong to soft law and therefore have a limited impact.

This thesis will focus on the role that internet intermediaries play in the protection of the freedom of expression and the right to the protection of personal data. In the first part, we will study the international and European legal framework for the protection of these both rights. We will then in the second part analyse the rules on the liability of internet intermediaries, in particular those of the European Union, regarding on the one hand, users generated content on their networks and, on the other hand, the data they process. In the first chapter of the third part, we will see the concerns that liability regimes of internet intermediaries for third party content raise for freedom of expression online. Chapter two will examine how and to what extent states and intermediaries can be held responsible for human rights violations online. Finally, the fourth part will be dedicated to the analysis of the current trends in state practice to reinforce the liability of intermediaries for users generated content and to increasingly require them to provide user data to national authorities in the context of the fight against terrorism and the worries this practice raises from a human rights perspective.

PART 1: LEGAL FRAMEWORK OF PROTECTION OF THE RIGHT TO FREEDOM OF EXPRESSION, THE RIGHT TO PRIVATE LIFE AND THE RIGHT TO DATA PROTECTION

We will study in this first part the international and European legal instruments of protection of the rights to freedom of expression and data protection before looking at how these rights can be affected online.

CHAPTER 1: International legal framework

The UN Human Rights Council, in a resolution of 2012[4], affirmed that "*the same rights that people have offline must also be protected online*". At the international level, freedom of expression is entrenched in the Universal Declaration of Human Rights (UDHR) of 1948[5], which applies to the 193 UN members, and in the International Covenant on Civil and Political Rights (ICCPR) of 1966[6], which is legally binding on its 169 State parties.

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 definiton, 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.

The same principles apply to all forms of expression online. In this regard, the Human Rights Committee in its General Comment No 34 on article 19[7] 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*".

---

[4] UN Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, 5 July 2012, UN Doc. A/HRC/20/L.13.

[5] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948.

[6] UN General Assembly, *International Convenant on Civil and Political Rights*, 16 December 1966.

[7] Human Rights Committee, *General Comment No 34*, 12 September 2011, CCPR/C/GC/34.

The Joint Declaration on Freedom of Expression and the Internet of 2011[8], issued by the four Special Rapporteurs on freedom of expression, draws attention to the fact that "*approaches to regulation developed for 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 developped to deal with illegal content online.

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 reads as follows:

> The exercise of the rights provided for in paragraph 2 of this article carries with it 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 (ordre public), or of public health or morals.

With respect to restrictions, General Comment No 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.

Regarding data protection, no specific mention of this right is found in the UDHR and the ICCPR. However, it is guaranteed through the provisions relating to the right to privacy. It is recognized that the latter includes the core principles of data protection.

[8] 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 Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet*, 1 June 2011.

The UDHR guarantees the right to privacy in its article 12 in the following terms:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 elaborates a bit upon this definition, stating that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> Everyone has the right to the protection of the law against such interference or attacks.

The Human Rights Committee has issued General Comment No 16 relating to article 17[9]. 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. These are its words:

> 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.

[9] UN Human Rights Committee, *General Comment No 16*, 8 April 1988, UN Doc A/43/40, 181–183; UN Doc CCPR/C/21/Add.6; UN Doc HRI/GEN/1/Rev 1, 21–23.

CHAPTER 2: European legal framework

SECTION 1: Council of Europe

Within the Council of Europe, the most important human rights instrument is the European Convention on Human Rights[10] (ECHR) of 1950. The European Court of Human Rights is the international jurisdiction responsible for guaranteeing the respect of the Convention by its 47 Member States.

Freedom of expression is guaranteed under the first paragraph of article 10 of the Convention as follows:

> 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.

Similarly to article 19 of the ICCR, the second paraprah provides a three-step test under which a restriction on the right is lawful, namely a test of legality, legitimacy and proportionality.

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are 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 or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in con dence, or for maintaining the authority and impartiality of the judiciary.

Regarding data protection, there is no specific provision enshrining the right. However, 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*"[11].

Right to private life is guaranteed by article 8, which reads as follows:

---

[10] Council of Europe, *European Convention on Human Rights*, 4 November 1950. Entry into force: 3 September 1953.
[11] ECtHR, 4 December 2008, *S. and Marper v. The United Kingdom*, app. n° 30562/04 and 30566/04, § n° 103.

> 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.

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[12], commonly called Convention 108, that counts 50 State Parties. Accession to the Convention is open to non-member states and Mauritius, Uruguay and Senegal have ratified it[13].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. It also seeks to regulate the cross-border flows of personal data.[14]

SECTION 2: European Union

In 2000, the European Union has proclaimed the Charter of Fundamental Rights of The European Union[15]. However, 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.

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*".

[12] Council of Europe, *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, Entry into force : 01 October 1985.
[13] Council of Europe, *Chart of signatures and ratifications of Treaty 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Status as of 04/06/2017*, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=jFc8VQaU, accessed: 5 June 2017.
[14] Council of Europe, *Handbook on European Data Protection Law*, STCE n° 108, 1981, p. 16.
[15] European Union, *Charter of Fundamental Rights of the European Union*, 18 December 2000, entry into force 1 Decembrer 2009, art. 51

With regard to 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 is enshrined in article 8 of the Charter and the latter in article 7. Article 8 reads as follows:

> 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.

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. Mention must also be made of the limited scope of the Charter: according to article 51, it applies to the EU institutions and to the EU Member States, but to the latter only when they implement EU Law. However, the CJUE has interpreted broadly this provision by ruling that when a national law was falling within the scope of EU Law, the Charter was applicable.[16]

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[17]. 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.

However, the directive 95/46/CE doesn't apply to the police and judicial cooperation in criminal matters. This legal vacuum has been filled in 2008 with the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[18].

---

[16] CJUE, 26 February 2013, *Åklagaren v.Hans Åkerberg Fransson*, case C-617/10.
[17] The European Parliament and the Council, *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*, 24 October 1995, OJ L 281 23/11/1995, pp. 31 to 50.
[18] The Council, *Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, 27 November 2008, OJ L 350, 30/12/2008,

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[19]. The new legal framework of reference in the area will be constituted of a new General Data Protection Regulation[20] completed by a Directive[21] replacing the Council Framework Decision 2008/977/JHA. The Data Protection Regulation will improve the protection regarding the use of data by internet intermediaries operating within the European Union.[22] The Directive entered into force on 5 May 2016 and the Member States have until 6 May 2018 to transpose it into their national laws. The regulation will enter into force on 14 May 2016 and be applicable from 25 May 2018.[23]

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 part will be dedicated to the study of liability regimes of internet intermediaries in respect, on the one hand, to data protection and, on the other hand, to content generated by users.

---

pp. 60 to 71.

[19] Christophe Maubernard, "La protection des données à caractère personnel en droit européen: de la vie privée à la vie privée numérique", *RUE,* July 2016, p 5.

[20] The European Parliament and the Council, *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*, 27 April 2016, OJ L 119/1, 4/5/2016, pp. 1 to 88.

[21] The European Parliament and the Council, *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*, 27 April 2016, OJ L 119, 4/5/2016, pp. 89 to 131.

[22] Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim, *op.cit.,* p. 37.

[23] European Commission, "Reform of EU data protection rules", http://ec.europa.eu/justice/data-protection/reform/index_en.htm, accessed: 5 June 2017.

PART 2: LIABILITY REGIMES OF INTERNET INTERMEDIARIES

We have already said 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. Internet intermediaries have also their own policies regarding content restriction and data processing in their terms of service. Hence, these private actors play an increasing role in the protection of data and expression online.

In this part, we will give an overview of the rules laying down their obligations with regard to content generated on their networks and the processing of personal data. Chapter one will analyse legal regimes of liability of internet intermediaries for third party generated content. With respect to the right to protection of personal data, we will study in chapter two the rules aiming at ensuring the conformity of the collection and the processing of data by internet intermediaries with this right. In chapter three, a new right, the right to delisting, which has implications for both data protection and freedom of expression, will be looked at. Finally, chapter four will consider the question of the scope of application of liability regimes.

Before getting into the crux of our analysis, an important observation has to 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 liable and face penalties under these specific regimes. This type of liability has to be distinguished from the responsability 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 incur responsability, depending on the circumstances. We will study this question more in depth in the third part of this thesis.

CHAPTER 1: Liability of internet intermediaries for third party generated content

As stated 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.[24]

In a majority of states, this goal has been achieved through legal rules of liability, compelling intermediaries to police content on the behalf of the state. If they refuse to do so, they can incur liability 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 insolvency, their anonymity or their location. Hence, the new environnent required new rules, and the internet intermediaries were easier to hold accountable than the authors, due to the fact that they are known and, generally, solvent.[25] 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, up- or downloaded, stored, or distributed on their system*".[26]

We have to bear in mind that each removal or blocking of content online has an impact on freedom of expression. Indeed, both measures affect the right of internet intermediaries to impart informations and ideas created and published by third parties, the right of the creators and publishers to communicate such informations 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§3 of the ICCPR, article 10§2 of the ECHR and article 52 of the EU Charter of Fundamental Rights. Any restriction of content should therefore rest on a clear and accessible

---

[24] Council of Europe, "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet", 2015, pp. 14-16, https://edoc.coe.int/fr/liberte-des-medias/7286-pdf-etude-comparative-sur-le-blocage-le-filtrage-et-le-retrait-de-contenus-illegaux-sur-internet.html, accessed: 5 June 2017.
[25] Céline CASTETS-RENARD, "Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet", *Recueil Dalloz*, 2012, p. 827.
[26] Monica HORTEN, "Content 'responsability' : The Looming Cloud of Uncertainty for Internet Intermediaries", *Center for Democracy and Technology*, 2016, p. 5.

legal basis, pursue a legitimate aim and be necessary and proportionate. We will however see that the application of the legal regimes of liability often lead to restriction of content in a manner inconsistent with these international standards.

SECTION 1: Basic Facts

Some basic defintions and distinctions are needed to apprehend the legal rules of liability regarding content online. Indeed, theses rules are specific to the digital era and call for particular considerations.

A. Types of internet intermediaries

The main categories of internet intermediaries that will be studied in this thesis are internet access providers, web hosting providers, social media platforms and search engines. These intermediaries play different roles. Indeed, 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/or to communicate between them. These intermediaries are often considered hosts for the implementation of liability regimes. 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 database.[27] [28]

It is important to bear in mind that some internet intermediaries have considerably diversified their services and can therefore fall into several categories. For instance, Google is most well known as a search engine but besides this service, it has developed Google + which is a social media platform.[29]

[27] Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim, *op.cit.,* pp. 21-22.
[28] Article 19, "Defending Freedom of Expression and Information, Internet Intermediaries: Dilemna of Liability", *Free Word Centre*, 2013, p. 6.
[29] *Ibidem*.

These differences also impact the business models of the intermediaries. Indeed, internet service providers need to be physically present in the same jurisdiction as their users to be able to offer their services. 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. Hence, states have a particular leverage over this type of intermediaries. Conversely, the three other categories of intermediaries mentioned above do not need to operate within the country of the users to whom they offer their services. A user in Kenya can do research on Google or communicate on Facebook despite the fact that these companies have no equipment or personnel in the country.[30] However, states are increasingly trying to impose their laws on these new international actors.

B. Models of liability for third party generated content

Three general models of liability can be identified:

- The strict liability model: under this regime of liability, internet intermediaries are responsible for all illegal content they carry and have therefore constantly to monitor the internet in order to avoid liability. If they don't comply with these obligations, they face various sanctions that can range from fines to criminal punishments or the revocation of their business licence in the most extreme cases. This model is found for example in Thailand or China.[31]

- The safe harbour model: with respect to this regime of liability, internet intermediaries can escape liability for illegal content processed through their services when several conditions are met. This model is found for instance in the European Union and in the United States but in the latter it applies only to specific content such as copyright. Under this model, internet access providers, who act as 'mere conduits' by merely providing technical services, benefit from almost full immunity. By contrast, with regard to hosting providers, social media platforms and search engines, a notice and take down procedure is at the core of the safe harbour regime. According to this

[30] Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim, *op.cit*., pp. 21-22.
[31] Article 19, *op.cit.,* p.7.

procedure, intermediaries do not incur liability when they take down content upon notice of its illegal character.[32]

- The broad immunity model: according to this model, internet intermediaries benefit from a large immunity for third party generated content. The United States are 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.[33]

C. Categories of restrictions

Different measures aimed at restricting content online can be imposed to internet intermediaries. The first main one is the removal of illegal content. In this case, hosting service providers and social media platforms are ordered to delete certain content on sites or platforms hosted by their services or search engines, or to delete hyperlinks to specific webpages. Such a measure is relatively easy to implement towards intermediaries located in the geograpical jurisdiction of the country seeking to impose its law, but way more difficult when the content is hosted abroad. In this regard, it is important to bear in mind that most of the major multinational internet companies, for instance Facebook, Google or Twitter, are based in the U.S. These are also the companies most targeted by restriction orders.

In this context, another solution for states is to turn to internet access providers located in their jurisdiction to request them to take technical measures to block access to specific content. This is the second main type of restriction. Blocking or filtering is therefore generally applied by internet access providers and aims at blocking access either to entire websites or to particular pages or keywords[34].

Other measures can be taken by intermediaries to restrict access to certain content. For example, social media platforms can block from view content to particular users or deactivate user accounts.[35] Nonetheless, it is the two types of restrictions mentioned above that are particularly relevant for the purposes of this thesis.

[32] *Ibidem.*
[33] *Ibidem.*
[34] Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim, *op.cit*., p. 23.
[35] *Ibid.,* p. 24.

SECTION 2: European Union liability regime of internet intermediaries for illegal content generated by third parties on their networks

The European Union 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 strike a fair balance between the necessity to restrict illegal or harmful content online and the need to support the freedom of enterprise of internet intermediaries and freedom of expression online which are essential to the development of the internet.

The regime of liability for third party generated content is provided mainly by two directives : the E-commerce Directive[36] and the Information Society Directive[37] in some of its provisions.

The Information Society Directive applies to copyright claims and bring one important clarification regarding the general regime of liability laid down in the E-commerce Directive. Indeed, it protects the right of reproduction of copyright holders but provides that "*temporary acts of reproduction*" whose sole purpose is "*to enable a transmission in a network between third parties by an intermediary*" is not a violation of that right[38]. Internet intermediaries can therefore not be held liable for such temporary acts of reproduction on their networks.

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.[39]

The E-Commerce Directive provides a safe harbour for 'information society services' against liability under certain circumstances. According to the Directive, internet access providers,

[36] The European Parliament and The Council, *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),* 8 June 2000, OJ L 178, 17.7.2000, pp. 1 to 16.
[37] The European Parliament and the Council, Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, 22 May 2001, OJ L 167 , 22/06/2001 pp. 0010 to 0019.
[38] Article 5§1 Information Society Directive.
[39] Pablo Baistrochhi, « Liability of Intermediary Service Providers in the EU directive on Electronic Commerce », *Santa Clara High Technology Law Journal*, Volume 19, Issue 1, p. 3, p. 112.

who act as « mere conduits », meaning that they transmit content regardless of what it is, are not liable for the information transmitted, as long as they do not 'initiate the transmission', 'select the receiver' or 'modify the information contained in the transmission'.[40] 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 such knowledge', they 'act experditiously to remove or to disable access' to the illegal material.[41]

The Directive prohibits the imposition of a general obligation to monitor on internet intermediaries.[42] Such an obligation would require intermediaries to constantly watch content posted on their networks and remove or block those that seem illegal independently of any notice. The CJEU has ruled that compelling intermediaries to monitor continuously or to take preventive action is not compatible with EU law. According to *Scarlet Extended* and *Sabam v. Netlog* rulings[43], this prohibiton applies to both categories of intermediaries.[44]

In the *Netlog* case, the CJEU ruled that the prohibition precludes a law that would impose on hosting intermediaries an obligation to "*install a system for filtering information which is stored on its servers by its service 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 electronicles containing musical, cinematographic or audio-visual 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"*.[45]

So called 'stay down injunctions' are likewise incompatible with the prohibition of the general obligation to monitor. Such an injunction means requiring from internet intermediaries that once illegal content has been removed, they have to ensure that this content never reappears again on their platforms. Such stay down injunctions would require a scanning or filtering system. These kinds of systems are onerous and given the numerous files

[40] Art. 12 E-Commerce Directive.
[41] Art. 14 E-Commerce Directive.
[42] Art. 15 E-Commerce Directive
[43] CJEU, 24 November 2011, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10 and CJEU, 16 February 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, Case C-360/10.
[44] Monica HORTEN, *op. cit.,* p. 9.
[45] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, op.cit.,* § n° 53.

at stake, decisions would be made by algorithms rather than by humans. However, 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 down of legal content. The stance regarding take down actions has first been stated by EU national courts and then has been supported by the CJEU in the two cases mentioned above.[46]

Importantly, the Regulation on Open Internet Access[47] entered into force April 30, 2016. The new Regulation, among other things, prohibits internet access providers to voluntary block content. Therefore, 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. Limited exceptions to this prohibition are nonetheless provided.[48] The Regulation has authorized states that already had self-regulation mechanisms to keep them in place until December 31, 2016.

We should also already note that in 2016 the European Commission put forward proposals in the framework of the Single Digital Market Initiative [49] that are targeting internet intermediaries. The reform does not seek to amend the E-commerce directive but seeks to adopt special measures to impose more "responsible behaviour" on internet intermediaries in particularly senstitive areas such as the fight against terrorism and hate speech. These proposals consist of a new Terrorism Directive[50], which was adopted the 15 March 2017, and of an amendment to the Audiovisual Media Services Directive[51] concerning hate speech content online. [52] These initiatives considerably increase the burden of intermediaries for

[46] Monica HORTEN, *op.cit.*, pp. 10 and 11.
[47] The European Parliament and the Council, *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*, 25 November 2015, OJ L 310/1, 26/11/2015.
[48] Art. 3.3 §3 Regulation 2015/2120.
[49] European Commission, *Communication from the Commission to the European Partliamant, the Council , the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market for Europ*e, 6 May 2015, COM(2015) 192 Final.
[50] The European Parliament and the Council, *Directive 2015/0281 on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism*, 15 March 2017.
[51] European Commission, *Proposal for a Directive of the European Parliament and the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, 25 May 2016, COM(2016) 287 final
[52] Monica HORTEN, *op.cit.*, p. 5.

content linked to terrorism or hate speech and raise particular concerns regarding human rights. We will study this particular issue in the fourth part of this thesis.

In the next section, we will analyse a specific case of liability and the case law of the European Court of Human Rights relating to it.

SECTION 3: Liability of an online newspaper for comments generated by its users: the position of the European Court of Human Rights

The first case referred to the European Court concerning the liability of an internet news portal for comments generated by users was the *Delfi AS v. Estonia* case[53]. The facts are the following: Delfi, an estonian internet news portal, had published an article reporting how a ferry company had destroyed territory driving from Estonia's mainland to its islands. The article generated numerous comments among which some were threatening or offensive to one shareholder of the company, L. Delfi had a system of notice and take down that allowed readers to mark a comment as offensive, in which case the news portal would remove the comment. L. sent a request to Delfi to remove the offensive comments and to pay him damages. The latter removed experditiously the comments but refused to pay.

The Estonian authorities ruled that Delfi had to be considered as a publisher because it had integrated the user's comments in its platform, it had encouraged the readers to post comments on it and had an economic interest in the exploitation of the platform including the integrated comments. Consequently, it could not rely on the provisions of the E-commerce Directive granting hosting intermediaries a safe harbour against liability when they remove experditiously an illegal content upon notification.

The European Court admitted that there was an interference with Delfi's right to freedom of expression. Nevertheless, it confirmed the approach of the Estionan authorities and stated that "*the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, even without*

[53] ECtHR, 16 June 2015, *Delfi AS v. Estonia*, app. n° 64569/09.

notice from the alleged victim or from third parties"[54] and concluded that the Estonian authorities' interference with Delfi's freedom of expression was not breaching article 10 of the Convention.

This ruling has been criticized, detractors underlining the adverse impact that such a precedent would have on freedom of speech online. Part of these criticisms is directed at the acceptance of the Court to qualify the news portal as a publisher of the comment generated by its users and not as a hosting provider benefiting from the safe harbour of the E-commerce Directive. They argue that although there is no doubt that Delfi is a content provider and an editor regarding the content tbat it personally adds on its platform, it is doubtful that it can be considered as an editor for the users' comments. This decision to consider Delfi as an 'active intermediary', namely an intermediary which play an active part in the organization and functioning of its readers' comments that cannot be considered a 'neutral' hosting provider has far-reaching consequences. Indeed, the Court seems to consider that imposing on 'active intermediaries' an obligation to monitor the internet in order to escape liability is compatible with freedom of expression. There is therefore a risk that news portals similar to Delfi will restrict readers' comments, in particular the possibility to comment anonymously, and be more reluctant to report on controversial topics, resulting in a considerable chilling effect on freedom of expression. [55]

In a subsequent case, *MTE v. Hungary*[56], the same issue arised. In this case, the European Court ruled that the decision of the Hungarian authorities to hold an Internet news portal liable for comments generated by users was violating article 10 of the Convention. However, the Court accepted once again the qualification of the internet news portal as publisher. The finding of a violation was based on the disproportionality of the national authorties' interference with the freedom of expression of the applicant, taking in particular into account the fact that in this case the content was merely 'offensive and vulgar'[57], contrary to the Delfi case in which the content was clearly illegal. The Court therefore tempered the approach it

[54] *Ibid*, § n° 159.
[55] Maya Hertig RANDALL, "Freedom of Expression in the Internet", *Swiss Review of International and European Law, Vol. 26, Issue 2, 2016*, pp. 235-254, and Dirk Verhoof, "Qualification of news portal as publisher of users' comment may have far-reaching consequences for online freedom of expression: Delfi AS v. Estonia", *Strasbourg Observers*, 2013, https://strasbourgobservers.com/2013/10/25/qualification-of-news-portal-as-publisher-of-users-comment-may-have-far-reaching-consequences-for-online-freedom-of-expression-delfi-as-v-estonia/, accessed: 5 June 2017.
[56] ECtHR, 2 February 2016, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, app. n° 22947/13.
[57] *Ibid*., § n° 64.

had taken in Delfi without however strongly recognizing for intermediaries a safe harbour for comments generated on their platforms.

SECTION 4: National regimes of liability in the United Kingdom, France, the United States and China

A. UK

In the United Kingdom, there is no legal framework specific to the internet. As a result, the country relies on general laws to deal with the removal or blocking of illegal content online.[58] This lack of specific legislation can be explained by the legal traditions of the country, as it is a country of common law which has preferred to encourage voluntary regulation to solve these issues by means of cooperation with the private sector. Indeed, in the UK, the removal and blocking of content online is operated broadly by private regulation: either taking the shape of rules contained in terms of use policies of the internet intermediaries either by the voluntary cooperation of those intermediaries with the national authorities, copyright owners and private regulatory bodies. [59]

Regarding pedopornographic content, there is a partnership between internet intermediaries and the Internet Watch Fondation (IWF), the national industry regulatory body, that strives to work towards the "elimination of child sexual abuse imagery online"[60]. The IWF keeps and updates a blacklist of sites hosted abroad and notifies internet providers who must block them.[61] This list is updated regularly to check if the blocking is still necessary or if the blocked contents have been removed.[62] There is also a possibility for interested parties who would consider that certain blocked content is not illegal to appeal against the correctness of the assessment.[63] On its website the IWF makes a blocking good practice guidance available, "*designed to maintain the principle of transparency and minimise over-blocking and latency*

[58] Council of Europe, "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, 2015", *op.cit.,* p. 3.
[59] *Ibid.,* p 13
[60] IWF, "Why We Exist", https://www.iwf.org.uk/what-we-do/why-we-exist, accessed: 5 June 2017.
[61] Swiss Institute of Comparative Law, "Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content", p. 755.
[62] Council of Europe, "Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet", *op.cit.,* p. 17.
[63] Swiss Institue of Comparative Law, *op.cit*., p. 756

issues".[64] The terms of use of the important internet intermediaries refer and defer to the blacklist established by the IWF and accept the blocking of URLs identified by it.[65] In regard to sites hosted in the UK, the regulatory body has developed a Code of Practice for Notice and Take down. When it assesses that a specific content could be subjeted to criminal prosecutions, it notifies the site hosting the content and orders it to remove the allegedly illegal content. The internet intermediary then must either act expeditiously to remove the content or notify the IWF that it does not agree with the accuracy of the assessment.[66]

There is nonetheless a specific legal framework for particular kinds of content, such as terrorist or defamatory content or content breaching copyright law. With regard to blocking orders, they are given by service polices or the judiciary depending on the type of content in question.

For content inciting to terrorism, the Terrorist Act of 2006 gives the police services the power to issue blocking orders against internet intermediaries.[67] The Counter Terrorism Internet Referral Unit is charged with ensuring the coordination of take down notices. However, in practice, it appears that the blocking of contents is achieved through the informal cooperation between the police services and the internet access providers.[68] In the fields of defamation and copyright, blocking injunctions, meaning that the Court orders the blocking of access to internet or certain sites, are increasingly used against internet intermediaries to block unlawful content generated by third-parties. For example, with respect to defamatory content online, the Copyright, Designs and Patents Act 1988[69] gives the High Court the power to grant such injunctions against an intermediary where the latter has 'actual knowledge' that the content in question is infringing copyright law.[70] An increasing use of blocking injunctions is observed as well in the areas of right to privacy and data protection where, in the absence of specific provisions, the orders are issued on the basis of general statutory provisions. [71]

[64] IWF, "URL Blocking: Good Practice", https://www.iwf.org.uk/become-a-member/services-for-members/url-list/url-blocking-good-practice, accessed: 17 June 2017.
[65] Swiss Institute of Comparative Law, *op.cit.,* p. 755.
[66] *Ibid*, p. 762.
[67] Section 3 Terrorist Act 2006.
[68] Swiss Institue of Comparative Law, *op.cit*., p. 756.
[69] Section 97A of the Copyright, Designs and Patents Act 1988.
[70] Swiss Institute of Comparative Law, *op.cit*., pp. 758-760.
[71] *Ibid.,* p. 753.

Regarding the removal of content, a notice and take down procedure is provided by statutory provisions only for defamatory content or content inciting to terrorism.[72] However, it is reported that intermediaries remove content upon notice in other fields in order to avoid liability despite of the absence of statutory provisions foreseeing such a procedure.[73]

We have to recall that according to the EU Regulation on Open Internet Access, auto-regulation mechanisms had to come to an end at the latest the 31 December 2016. The first national reports on the implementation of the regulation are expected for June 30, 2017.[74]

B. France

Unlike United Kingdom, France has endowed itself with legislation specific to the blocking and removal of content on the internet. The Law for Trust in Digital Economy of the 21 June 2004[75] transposes the E-commerce Directive and provides the general regime of liability of internet intermediaries. This law places several obligations on internet intermediaries: they must keep identification data of their clients[76], communicate them to judicial authorities[77] and put into place a reporting mechanism for odious contents (apology of war crimes and crimes against humanity, incitement to discrimination, hatred or violence and pedopornography)[78] and for activities linked to illegal gambling[79].

The law foresees a notice and take down mechanism, meaning that hosting intermediaries are not liable for illegal content if they had no knowledge of the content or if, as soon as they aquired this knowledge, they took action promptly to remove it or to make it unaccessible.[80] There is a presumption of knowledge of the contentious content when different elements listed by the law are notified to the hosting intermediary, such as the date of the facts, their description and location, the grounds upon which the content has to be removed with mention of the relevant legal rules and the factual considerations.[81] However, the intermediary has a

[72] Terrorist Act 2006, Defamation Act 2013.
[73] Swiss Institute of Comparative Law, *op.cit*., p. 762.
[74] Noerr, "BEREC publishes guidelines for net neutrality implementation", 2016, https://www.noerr.com/en/newsroom/News/berec-publishes-guidelines-for-net-neutrality-implementation.aspx, accessed: 5 June 2017.
[75] Loi n°2004-575 pour la confiance dans l'économie numérique, 21 June 2004.
[76] Art. 6, II and II bis loi pour la confiance dans l'économie numérique.
[77] Art. 6, II.
[78] Art. 6, I, 7, al.3.
[79] Art. 6, I, 7.
[80] Art. 6, I, 2 and 3.
[81] Art. 6,I, 5.

margin of appreciation regarding the illegal character of the content notified. Indeed, the Constitutional Council ruled that the latter could be held liable for having failed to make unaccessible a content on the internet after notification only if the content was manifestly illegal.[82] A removal or blocking order can also be ordered by a judicial authority to hosting intermediaries, and, when not possible, to internet access providers.[83] In this case, the intermedaries do obviously not benefit from such margin of appreciation.

In the area of protection of the right to private life, besides the general regime provided by the law described above, article 9 of the civil code also foresees the possibility for judges to order any measures to prevent or to put to an end a violation of that right.[84] Regarding specifically the right to protection of personal data, the CNIL has jurisdiction to stop the treatment of such data under certain circumstances.[85]

Subsequent laws have strengthened the liability regime by posing new obligations on intermediaries. Concerning copyright law, the laws Hadopi 1 and 2[86] modifying the Code on Intellectual Property and provides that, when there is an infringment of copyright committed online, the persons responsible for the infringement as well as the holders of the internet connection can be convicted by a judge to no longer have access to that service. A filtering will therefore be ordered to internet access providers and they have 15 days to obey[87]

A law of 2011[88] regarding national security and a law of 2014[89] aimed at enhancing the means to fight terrorism put new requirements on internet intermediaries for pedopornographic content and content inciting to or making an apology for terrorism. These laws modify the law for trust in digital economy[90] by creating a process in two phases for such content. During the first phase, the administrative authority requires the removal of contents deemed to be illegal to hosters and simultaneously informs internet access providers of its request. The second

[82] Const., 10 June 2014, n°2004-496 DC.
[83] Art.. 6, I, 8 loi pour la confiance dans l'économie numérique.
[84] Swiss Institute of Comparative Law, *op.cit*., p. 237.
[85] Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 January 1978.
[86] Loi n°2009-669 favorisant la diffusion et la protection de la création sur internet, (Hadopi I) 12 June 2009 and loi n°2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet, (Hadopi 2) 28 October 2009.
[87] Art. L. 335-7 du code de la propriété intellectuelle.
[88] Loi n°2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure, 14 March 2011 (LOPPSI 2).
[89] Loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme, 13 November 2014.
[90] Inserting article 6-1 in the law for trust in digital economy.

phase begins if the content targeted is not removed by the hosters within 24 hours of the request, The administrative authority then notifies the internet access providers of a list of the URL addresses they must prevent access to without delay. The administration can provide the same informatio to search engines, ordering them to ensure the delisting of the contents in question.[91]

The administrative authority must send removal requests and the list of adresses URL whose blocking or delisting is asked to a person appointed within the CNIL who controls the operations. If there is an irregularity, it can make a recommendation to the administrative authority ordering it to put it to an end or, if the latter does not obey, lodge a complaint to an adminstrative tribunal.

We see therefore that, for pedopornographic content and content linked to terrorism, the legal regime is genuinely one of administrative censorship without prior judiciary intervention. Note that for sites offering games of chance or gambling, the system is hybrid: the blocking is ordered by a court at the initiative of an administrative authority.[92] Administrative authorities have considerable power to require the removal of content violating the right to privacy as well, even being allowed in some hypotheses to order the removal or blocking of content without prior judicial order.

C. USA

In the United States, Section 230 of the Communication Decency Act (CDA) of 1996 provides that "*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*." This provision therefore confers a broad immunity to internet intermediaries for third party generated content. Furthermore, it has been subjected to an extensive interpretation by the US Courts. For example, it has been ruled that intermediaries could not be held liable for content even if they were aware of the illegal nature of such content or if they had been notified of this fact by a third party victim of the illegal content in question. Nonetheless, the immunity is not absolute. In sensitive areas such as pedopornography, internet intermediaries have the

[91] Philippe SEGUR "Le terrorisme et les libertés sur l'internet", *AJDA*, 2015. pp. 161-163.
[92] *Ibid,* pp. 164-165.

obligation to collaborate with national authorities.[93] This broad immunity model does however not apply to federal crimes, copyright violations claims and electronic communications privacy law.[94]

Regarding copyright infringments online, it is the Digital Millennium Copyright Act (DMCA) of 1998[95] that applies. The DMCA inserted a new section 215 in the Copyright Act of 1976. The regime of liability is less favourable than the general one foreseen in the CDA. The provision draws a distinction between four types of internet intermediaries in order to establish the safe harbours: access providers, caching providers, hosting providers and search engine providers. Access providers are immune from liability for third party generated content, provided that the transmission is initiated by the user, is "*carried out through an automatic technical process*", without "*selection or modification*" of the material or of the recipient and that no copy of the material is "*maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients*" or to anticipated recipients for longer than necessary.

Section 215 grants hosting providers and search engines providers the same safe harbour, which applies under three cumulative conditions: the providers 1) have no "*actual knowledge*" of the illegal character of the material or are "*not aware of facts or circumstances*" from which such illegal charter is apparent, and "*upon obtaining such knowledge or awareness, act expeditiously to remove, or disable access to, the material*"; 2) they do "*not receive a financial benefit directly attributable to the infringing activity*", when they have the "*right and ability to control such activity*"; 3) upon notification of the illegal character of a material, they "*respond expeditiously to remove, or disable access to*" such material. This third condition is an implementation of the notice and take down procedure that we already mentioned before. The regime applicable to caching providers will not be studied here.

This safe harbour regime became a reference around the world and numerous safe harbour legislations have been built on it.[96] The regime established by the E-commerce Directive of the European Union also drew inspiration from it. Nonetheless, while in the US the safe

[93] Benoît FRYDMAN, Isabelle RORIVE, "Regulating Internet Content through Intermediaries in Europe and the USA", *Zeitschrift für Rechtssoziologie 23*, 2002, p. 51.
[94] Article 19, *op.cit.,*p.7.
[95] Digital Millennium Copyright Act, 105th Congress (1997-1998), H.R.2281.ENR.
[96] Nicolo ZINGALES, "Accountability 2.0 : Towards a Special Responsability of Internet Intermediaries for Human Rights Violations", *Paper submitted for the 8th Symposium of the Global Internet Governance Academic Network*, 2013, p. 4.

habour model applies only to copyright infringements, it is applicable in the EU to breaches of all types of laws.

D. China

China has adopted a very strict liability model. In Chinese law, internet intermediaries are referred to as 'Internet Information Service'. The 'Administrative Measures on Internet Information Service'[97] adopted in 2000 provide nine types of speeches which are deemed to be illegal for online services. These illegal types of content, commonly called the 'nine forbidden content categories', include speech that "*harms the dignity or interest of the State*", or "*disseminate rumours, distrubs social order or disrupts social stability*" or "*sabotages State religious policy or propagates heretical teaching or feudal superstitions*".[98]

Internet intermediaries are required to monitor the content online and when they discover material falling into one of the 'nine forbidden content categories', they have the obligation to "*promptly terminate the distribution and keep relevant records and report to the relevant authorities*".[99] If they fail to do so, liability can incur and a range of different sanctions can be imposed, including criminal charges or the withdrawal of business licences. The Chinese authorities, through their national internet access providers, block access on the territory to services whose efforts to police the forbidden content are not deemed sufficient. It explains why the most important multinational internet companies based in the U.S., such as Facebook, Google or Twitter, are not accessible to users located in China.[100]

[97] People's Republic of China State Council, *Measures on the Administration of Internet Information Services*, 25 September 2000, Decree n° 292.
[98] Art. 15 of the measures and Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in Lim, *op.cit*., p. 32.
[99] Art. 16 of the measures.
[100] Ranking Digital Rights, Chinese Internet Companies Show Room for Improvement, https://rankingdigitalrights.org/index2017/findings/china/, 19 June 2017.

CHAPTER 2: European Union regime of responsibility of internet intermediaries with regard to the processing of personal data

SECTION 1: Responsibility for the protection of personal data under the Data Protection Directive and the new General Data Protection Regulation

The Data Protection Directive of 1995[101] sets out the obligations that private and public entities, among them internet intermediaries, have to meet in order to ensure the protection of the right to protection of personal data. Its provisions apply to the "*processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*". The 'proccessing of personal data' includes all the operations performed on personal data, such as collection, storage, dissemination, blocking or erasure.[102] Personal data has to be understood as any data that allows identifying a person.[103]

It distinguishes two types of actors involved in the processing of data: the processors and the controllers. The distinction serves to establish the extent of their respective obligations. The controllers[104] are the decision-makers: they hold personal data and decide, 'alone or jointly with others', what to do with it. In consequence, they have to comply with burdensome rules. The processors also hold personal data but follow instructions of the controllers regarding their use[105] and are therefore subjected to more limited obligations than the controllers.

Internet access providers will in principle fall outside the scope of the Directive since they confine themselves to the mere transmission of information generated by users over a network. With respect to hosting intermediaries, social media platforms and search engines, the situation is more complex. When they process data generated by third parties on their network for their own purposes, they will be considered as the controllers of that specific processing. However, with regard to data published by users on their platforms, sites or pages,

---

[101] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data , op.cit.*
[102] Article 2 (b) Data Protection Directive.
[103] Article 2 (a) Data Protection Directive.
[104] Article 2 (d) Data Protection Directive.
[105] Article 2 (e) Data Protection Directive.

a case-by-case assessment is needed to decide whether they 'determine the purposes and means of the processing' or not and therefore whether they have to be qualified as controllers or processors.[106]

Internet intermediaries that provide the platforms on which user can share informations, index these informations, enable users to search them and ensure their publication and distribution play an active role which goes beyond the mere transmission or storage of content on behalf of users. In these cases, it seems that they have to be considered as controllers and be subjected to the ensuing burdensome legal regime.[107]

As said above, from this qualification arise different obligations. Indeed, controllers have to comply with many requirements. They are for instance responsible for ensuring that the processing is fair and lawful, that data are collected transparently and for legitimate purposes and that they cannot be further processed for other purposes, that they are adequate, relevant and not excessive in relation to these purposes and that they are accurate and kept up to date. They also have to provide indivuals whose data is collected with different information regarding the collection and the processing of its data. Importantly, data subjects have the right to obtain from controllers the rectification, erasure of blocking of data under certain circumstances and to oppose in certain cases the processing of such data.

The Directive provides however exemptions. It includes one exemption linked to freedom of speech considerations: the processing of data carried out for journalistic purposes. It is important since the internet intermediaries could potentially rely on this exception. Nevertheless, we will see in the next section that the CJEU has adopted a narrow interpretation of this exemption.

The new General Data Protection Regulation places a considerable additional burden on collectors of data. Indeed, it enhances the existing rights of data subjects, namely mainly the right to access of data and the right to object to their processing when there is a legitimate jusitification or when the data are processed for the purposes of direct marketing, and grants

[106] Bart VAN DER SLOOT, "Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe", *JIPITEC, Vol. 6*, 2015, p. 6.
[107] *Ibid*., pp. 2-6.

them new and stronger rights and impose broader obligations on controllers. For instance, it provides data subjects with the right to data portability[108], namely the right to transfer data from a controller to another, the right to objet to the profiling of their data[109] and the 'right to be forgotten'[110]. The new obligations of controllers include obligations such as keeping records of processing activities[111] or undertaking an assesment of the impact of any envisaged processing of data on the protection of personal data[112]. Furthermore, the penalties faced by controllers in case of non-compliance with the Regulation are very high.[113]

Another important issue adressed by the Directive and Regulation concerns cross-border flows of data. Article 25 of the Directive sets out the conditions under which data collected within the EU can be transfered to third countries: such transfer is authorized if the third country ensures an adequate level of protection of data. The same criterion of adequacy has been included in the Regulation.

The CJEU made an important ruling in 2015 in this regard in the *Schrems* case[114]. The Court had to decide whether the transfer of data by Facebook's Irish subsidiary to servers located in the United States was in line with the Data Protection Directive. Indeed, a EU citizen had lodged a complaint to the Irish supervisory authority arguing that following the revelations made by Edwards Snowden in 2013 regarding the activities of the US intelligence services, in particular the NSA, the United States could not be considered as ensuring an adequate level of protection of data. The Irish authority had however rejected the complaint on the ground of a decision of the European Commission of 2000[115], know as the 'safe harbour decision', which recognized the adequacy of this level of protection. 'Safe harbour' in this context referrs to the guarantee that EU citizens' rights to data protection will be protected in the transfer of data outside the EU.

---

[108] Art. 20 General Data Protection Regulation.
[109] Art. 21 General Data Protection Regulation.
[110] Art. 17 General Data Protection Regulation.
[111] Art. 30 General Data Protection Regulation
[112] Art. 35 General Data Protection Regulation.
[113] Art. 83 General Data Protection Regulation.
[114] CJUE, 6 October 2015, *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14.
[115] Commission, *Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 26 July 2000, OJ 2000 L 215, p. 7.

The CJEU ruled that a decision of the Commission could not impede the national supervisory authorities to examine, with complete independence, whether a transfer of personal data to a third country was complying with the provisions of the Directive and the EU Charter. Furthemore, the Court considered that the 'safe harbour decision' was invalid. This finding was based on several reasons: the data protection regime in the US allowed for interferences by the government justified by national security, public interest or law enforcement which were prevailing over data concerns, data subjects lacked legal remedies regarding access to data or to ask for their erasure of rectification and the Commission had no competence to restrict the supervisory authorities' powers.[116]

The next section will pay particular attention to the right recently entrenched in the General Data Protection Regulation that we mentioned above: the right to delisting, most well known as 'the right to be forgotten'.

SECTION 2: "The right to be forgotten" or, more accurately, the right to delisting

Article 17 of the General Data Protection Regulation enshrines the 'right to be forgotten'. However, the first entrenchment of the right dates back to the *Google Spain v. Costeja*[117] ruling of the CJEU in 2014 which was based on the Data Protection Directive of 1995.

The facts of the case are the following: in 1998, the Spanish newspaper *La Vanguardia* published an auction notice mentioning the name of M. Gonzalez linked to proceedings for the recovery of social security debts. In 2010, the latter lodged a complaint to the Spanish Data Protection Agency against the newspaper *La Vanguardia*, *Google Spain* and *Google Inc*. He was claiming that the fact that the results or a search by his name in the search engine *Google Search* were links to the articles mentioned above, was an infringement of his right to data protection since the proceedings have been resolved and that such references to these proceedings were hence irrelevant. The National Agency acceded to its request only concerning *Google Inc*. and *Google Spain*, ordering them to remove the personal data of M. Gonzalez in a way that they would not appear anymore in the results of a search on the

[116] See for more information: Cécile THEARD-JALLU, Jean-Marie JOB, Simon Mintz, "Invalidation de l'accord Safe Harbor par la CJUE: portée, impacts et premier éléments de solution", *Dalloz IP/IT 2016*, 26, 18 January 2016.
[117] CJEU, 13 May 2014, *Google Spain SL, Google Inc. v. Mario Costeja Gonzalez*, case C-131/12.

engines. *Google Inc.* and *Google Spain* lodged an appeal against the decision to the Spanish court Audiencia Nacional, which applied to the CJEU for a preliminary ruling.

The main question was whether article 12(b) and subparagraph (a) of the first paragraph of article 14 of the Data Protection Directive obliged operators of a search engine to remove from their list of results, obtained on the basis of a person's name, links to articles published lawfully but prejudicial to the data subject. The first article guarantees data subjects the right to obtain the erasure of information which are no longer relevant for the purposes of the initial processing of data and the second the right to object such processing when there is a justified objection to it.

In the first place, the CJEU had to determine whether a search engine could be considered as a controller and therefore be subjected to the obligations posed by the two articles. It answered affirmatively, stating that the activity of a search engine "*which consists in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference*"[118] had to be qualified as a 'processing of personal data' and that the search engine was determining 'the purposes and means' of such processing in the framework of that activity.[119]

Subsequently, the CJEU decided that individuals had a right to delisting under certain circumstances. It stated that:

> Even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.[120]

The Court specified that the interference with the rights of the data subject protected under article 7 and article 8 of the EU Charter on Fundamental Rights could not be justified merely by the economic interest of the search engine. It however recognized that the delisting of

[118] *Ibid*, § n° 21.
[119] *Ibid*, § n° 33.
[120] *Ibid*, § n° 93.

information by search engines interfered with the legitimate interest of users to access the informations in question and that a balance had to be struck between the latter and the right to privacy and to data protection of the data subject. In this regard, it stated:

> Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.[121]

Summarizing, it appeared from the ruling that a case-by-case assessment has to be done and that three main criteria are relevant to appreciate the appropriateness to accede a delisting request, namely:

- the lapse of time since the information was published,
- the sensitivity of the information,
- and the interest of the public for the information, which will depend on whether the data subject is a public figure or not.

One have to bear in mind that in this case the newspaper *La Vanguardia* has not been ordered to remove the litigious article. Hence, the search engines were forced to remove links to these articles following a search on the basis of the applicant's name while simultaneously these articles remained on the newspaper's site. In this regard, the CJEU admitted that in certain circumstances a data subject would be able to exercise the rights conferred by articles 12(b) and subparagraph (a) of the first paragraph of article 14 against search engines but not against the publisher of the site. It justified this finding by the fact that the processing of data by a publisher of a website could in some cases fall within the scope of the journalistic exemption that we mentioned above whereas it considered that a search engine could not benefit from this derogation.[122]

Hence, the CJEU does not seem to hold the view that internet intermediaries playing an active role in the organization and functioning of websites can rely on the journalistic exception and more generally on freedom of expression in the framework of EU data protection rules. They

[121] *Ibid*, § n° 81.
[122] *Ibid,* § n° 85.

are therefore subjected to a very strict regime of liability regarding data protection matters since they have to comply with all the rules in order not to face penalties.

One observation has to be made with respect to the terminology: some call the right of a data subject to obtain the delisting of information published lawfully relating to its private life the 'right to be forgotten'. However, I think it is more accurate to talk about a right to delisting as when a search engine delists content, it remains on the site on which it was initially published. The measure therefore allows to limit access to the information at stake but in principle not to grant total oblivion by erasing it completely.

The right to delisting is now enshrined in the General Data Protection Regulation.[123] It brings some clarifications. Importantly, it states henceforth clearly that non-European companies processing data operating within the European Union have to apply European rules whereas this question was not clear in the *Google Spain* ruling.[124]

The analysis of the rules set out in the Data Protection Directive and in the General Data Protection Regulation and of the case law of the CJEU has shown that the qualification of an internet intermediary as a controller has considerable consequences regarding its responsibilities for the processing of personal data. Certainly, an increased protection of individuals against abusive use of their data is to be welcomed. However, a too extensive liability of internet intermediaries for user generated content infringing the rules on the protection of personal data or, more generally, for all illegal or harmful user generated content, raises concerns in regard to freedom of expression. In the next chapter we will study the scope of application of measures restricting material online before examining this issue in part three of this thesis.

[123] European Commission, "Factsheet on the 'Right to be Forgotten' Ruling", http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, accessed: 9 June 2017.
[124] Art. 17 Regulation 2016/679.

CHAPTER 3: Scope of application

The two issues that will be addressed in this chapter relate to the scope of application of the rules laying down the obligations that intermediaries have to fulfil regarding content generated by their users and the protection of personal data. The first one is the question of the jurisdiction of EU national authorities to require internet companies based outside the European Union to comply with their national laws. The second one is the issue of the geographical reach of measures restricting content ordered against intermediaries.

SECTION 1: Jurisdiction over companies based abroad

Most of the major international internet companies are based in the United States. It is for instance the case of Facebook, Twitter and Google. To guarantee the effectiveness of the rules relating to data protection or illegal content, it is essential to ensure that they can be applied to these internet intermediaries based abroad.

Article 4 paragraph 1 (a) of the Data Protection Directive provides that its provisions apply where "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*"[125]. With respect to this provision, the CJEU ruled that the words 'in the context of the activities of an establishment' could not be interpreted restrictively in light of the objective of the Directive, namely to ensure the effective protection of the right to data protection and the right to privacy. It consequently decided that the concept of 'establishment' could not be interpreted as meaning that a company would be established solely in the place where it is registered, especially when internet companies are concerned.[126] It concluded that the Member States had to apply their data protection rules to data collectors whose companies are registered abroad but exercice "*through stable arrangements in the territory of that Member State, a real and effective activity, even a minimal on*e".[127]

[125] Article 4§1 (a) Data Protection Directive.
[126] CJEU, 1 October 2015, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, § n° 25 and § n° 29.
[127] *Ibid*, § n° 41.

The General Data Protection Regulation brings clarification and is unequivocal regarding the application of its provisions to controllers based abroad. Indeed, it states clearly that non-European companies processing data and operating within the European Union have to apply European rules, regardless of whether the processing takes place in the EU.[128]

The E-commerce Directive applies to *'Information Society Services'*, defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".[129] The Directive applies therefore to every internet service offered in the EU regardless of the country in which they are established.

SECTION 2: Geographical reach of measures restricting content online

Traditionally, the reach of a measure ordered by a national authority is limited to the states's jurisdiction.[130] Indeed, according to international public law, the territoriality principle is the primary basis of jurisdiction and is justified by the principle of sovereign equality between states and the principle of non-intervention.[131].

We saw that states and regional organizations have adopted rules allowing national authorities to restrict freedom of expression online in particular by issuing orders to block or remove content directed at internet intermediaries. The ratio legis of these rules is most of the time to protect the rights of third parties or to ensure the application of criminal laws. We saw for example that an infringment of the right to protection of personal data and of the right to privacy will often justify a content restriction. However, the removal or blocking of such content within the specific territory where the law is applicable might not always be sufficient to guarantee the effectiveness of the protection of these rights. It is particularly true in the current digital era because thanks to the internet, individuals belonging to different countries

[128] Art. 3 General Data Protection Regulation.
[129] The European Parliament and the Council, *Direcitve 98/48/EC amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations*, 20 July 1998, JO L 217-18, art. 1 (2).
[130] Dan Jerker B. SVANTESSON, "Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?", *Scripted*, Volume 11, Issue 2, 2014, p. 155.
[131] BRENDAN VAN ALSENOY, MARIEKE KOEKKOEK, "The extra-territorial reach of the EU's 'right to be forgotten"', *CiTiP Working Paper Series*, 2015, p. 9.

are continuously interconnected.[132] In some cases, it might therefore be necessary to give removal or blocking measures an extraterritorial effect.

Heterogeneity of laws in different states is an issue. Content might be unlawful in one country and lawful in another. There is often no consensus on the precise definition of some rights at the international level and no uniform application of the balance of interests that has to be struck between freedom of expression online and other fundamental rights or criminal laws.[133] Hence, if a national authority issues a measure restricting content against an internet intermediary and requires the latter to ensure that the content is disabled everywhere in the world, it will lead to a violation of the right of individuals to access the content and the right of the author to communicate such content in all the states where the latter is lawful.[134]

It is important to mention that several techniques can be used to territorially delineate the reach of blocking/removal measures. One technique for such delineation consists of the use of country code Top-Level Domains. For example, if a Belgian court issues a removal/blocking order of content against Google, the latter could decide to restrict this content only on the www.google.be domain, the content remaining available for the rest of the world.[135] The content will however still be accessible from Belgium: individuals wishing to access it will merely have to search on other domains, for example .com, .fr or .es. The question whether the court will be satisfied with its order's implementation is another problem, which is considered further below.

Another option is to exploit geo-location technologies to determine the location of an internet user, using for example his IP address. Geo-location technologies can be used in different ways to limit the accessibility of content and allows to block access to specific internet content depending on the place where the request is done.[136] It can however be circumvented by softwares that are relatively easy to install, which hides the real location.[137]

---

[132] Olivia TAMBOU, "Protection des données personnelles: les difficultés de la mise en oeuvre du droit européen au déréférencement", *RTD Eur*., 2016, p. 249.
[133] *Ibid.*, p. 251.
[134] Dan Jerker B. SVANTESSON, "Delineating the Reach of Internet Intermediaries' Content Blocking – "ccTLD Blocking", "Strict Geo-location Blocking" or a "Country Lens Approach"?",*op.cit*., p. 156.
[135] *Ibid*, p. 157.
[136] *Ibid*, p. 158.
[137] Olivia TAMBOU, *op.cit.,* p. 253.

We will illustrate the issue of the geographical scope of blocking/removal orders by taking as an example the right to delisting and the difficulties that are encountered in its implementation. As a reminder, this right was first enshrined by the CJEU in the case *Google Spain v. Costeja*[138] in 2014 and then in the General Data Protection Regulation[139] of 2016.

The General Data Protection does not specify accurately how the right to delisting should be implemented and left the responsability to determine it to the data protection authorities at the national and European level.[140] However, the EU's Article 29 Working Party on data protection seems to recommend global blocking to ensure the effective implementation of EU law.[141] The Article 29 Working Party has been established by article 29 of Directive 95/46/EC and is responsible for providing the European Commission with recommendations on data protection issues and for forstering the harmonization of policies related to data protection between the EU Member States.[142] In its Guidelines related to the *Google Spain* case, it states:

> although concrete solutions may vary depending on the internal organization and structure of search engines, de-listing decisions must be implemented in a way that guarantees the effective and complete protection of these rights and that EU law cannot be easily circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.[143]

According to these Guidelines, the effective protection of the right to privacy and to data protection therefore requires that the delisting is implemented on all EU domains and at least on the .com domain. It is however not clear what they mean by 'all relevant domains'. Is the delisting on the .com domain sufficient to ensure the effectiveness of the rights and that EU law is not circumvented or should other non-European countries' domains also be targeted by

---

[138] *Google Spain v. Costeja, op.cit.*
[139] *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, op.cit.*
[140] Olivia TAMBOU, *op.cit*, p. 250.
[141] Dan Jerker B.SVANTESSON, "Limitless Borderless to Forgetfulness? Limiting the Geographical Reach of 'The Right to be Forgotten'", *Oslo Law Review*, 2015, Issue 2, p. 116.
[142] EUROPEAN DATA PROTECTION SUPERVISOR, "Glossary", https://edps.europa.eu/data-protection/data-protection/glossary/a_en, accessed: 10 June 2017.
[143] Art 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" Case C-131/12*, 2014.

the delisting? Since one central concern is non-circumvention, the terms 'all relevant domains' should probably be understood as including domains worldwide since it is really easy to access content delisted on European or .com domains on non-European countries domains on which the content in question has not been delisted.[144]

Google's approach concerning blocking or removal orders emanating from national authorities located within the European Union and linked to the right to delisting consists of delisting only in relation to EU national domains, for example .nl. or .es.[145] This approach however does not come without problems since some EU national authorities do not share Google's view on the geographical reach that should be given to such orders. These contradictory views can be illustrated by the recent conflict that opposed the French Commission nationale de l'informatique et des libertés (CNIL) and Google.inc.

In 2015, the CNIL had ordered the search engine to delist links infringing the right to protection of personal data on all its national domains, but Google publicly refused, challenging the legitimacy of this decision. It argued that the decision was disproportionate and unnecessary, because only 3% of French internet users access the search engine on another domain than the national one .fr. It also pointed out that global blocking risked having a serious chilling effect on the Web, underlining the fact that if the 'right to be forgotten' was a law in Europe, it was not the law globally and that "*if the CNIL's proposed approach were to be embraced as the standard for Internet regulation, we would find ourselves in a race to the bottom. In the end, the Internet would only be as free as the world's least free place*".[146] Google then unilaterally decided in 2016 to geographically block access to restricted content on all its domains when a research takes place within the EU. This progress was however not found relevant by the CNIL which imposed 100 000 euro in penalties to Google. This latter has brought the case before the French Council of State.[147]

The considerations above show that there is a lack of consensus on the geographical scope of the right to delisting. The conflict between the CNIL and Google could be seen as representative of a confrontation between two blocs: one European and one American. It

[144] Dan Jerker B. SVANTESSON, "Limitless Borderless to Forgetfulness? Limiting the Geographical Reach of 'The Right to be Forgotten'",*op.cit.,* p. 120.
[145] *Ibid.,* p. 116.
[146] Peter FLEISCHER, "Implementing a European, not Global, Right to Be Forgotten", 30 July 2015, https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html, 2 July 2017.
[147] Olivia TAMBOU, *op.cit*., p. 250.

would however be a simplified perspective.[148] Indeed, the positions concerning the definition and the geographical scope of the right do not converge within the United States and within the European Union.

In the United States, some developments are noteworthy, standing out from the majority theory to prioritize right to freedom of expression and to criticize the European approach of the right to delisting.[149] This majority theory puts to question the conformity of such right with the very broad American approach of freedom of expression as enshrined in the first amendment of the Constitution.[150] However, recent developments show a tendency to claim a right to delisting applicable on American soil.

For instance, in California, 'the Eraser Law' entered into force in 2015. This law allows minors to take down content posted by themselves on the internet. Such a law shows obvious similarities with the European right to delisting even though there are also some important differences. Indeed, on the one hand, the California law applies only to minors, namely individuals under eighteen, and importantly, only for content put online by themselves, not by third parties. On the other hand, the law applies to a broader range of internet operators than in Europe and allows not only the delisting of the content but the removal of the content itself. It is important to emphasize that this law is controversial and that its efficiency as well as its conformity under constitutional American law have been challenged.[151]

In New York, a bill has been proposed aimed at implementing a 'right to be forgotten'. This bill provides that at the request of an individual, search engines and online speakers should remove content or links relating to the individual which are 'inaccurate', 'excessive', 'irrelevant', or 'inadequate'. The constitutionnality of this proposal is highly disputed as well.[152]

Furthermore, in 2015, a consumer advocacy group, the Consumer Watchdog, lodged a complaint before the Federal Trade Commission against Google, denouncing the fact that

[148] *Ibid*, p. 252.
[149] Ioana GHOERGHE-BADESCU, "Le droit à l'oubli numérique", *Revue de l'Union européenne*, 2017, p. 165.
[150] Olivia TAMBOU, *op.cit*. p. 254.
[151] *Ibid.*, p. 254.
[152] Eugene VOLOCK, "N.Y. bill would require people to remove 'inaccurate', 'irrelevant', 'inadequate' or 'excessive' statements about others", https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others/?utm_term=.5ea3681e7f0c, accessed: 11 June 2017.

American users of the search engine were not able to make a delisting request contrarily to its European users. The group was condemning in particular the absence of equity.[153]

These new developments demonstrate that the need for a right to have personal information online erased in certain circumstances is not purely European but that a social need also exists in the United States. Results of some surveys show that ninety percent of US citizens would be in favor of a 'right to be forgotten',[154] whereas advocates of freedom of expression are still fervently arguing against the constitutionality of such right. The position with respect to the legitimacy of such a right in United States' law is therefore far from unambiguous. Nonetheless, this analysis shows that the argument that any right to delisting would inevitably be contrary to the American conception of freedom of expression has to be put into perspective.[155]

In the European Union, there is no consensus on the geographical reach that should be given to the right to delisting either. As seen above, the CJEU did not decide on the geographical scope of the right. The new General Data Protection Regulation does not bring more clarifications. We also underlined that the Guidelines of the Article 29 Working Party on Data Protection are ambiguous regarding this question and let the door open for different interpretations. Hence, the view of the European Union on whether the right to delisting should have a global reach remains so far undetermined.

The question whether the right to delisting should be geographically implemented in all Member States of the European Union is not unanimously shared either. Delisting on European domains is the solution currently adopted by Google and which has the favors of the Advisory Council to Google on the Right to Be Forgotten, whose purpose is to find the best way to implement the right by striking a fair balance between the right of a person to be forgotten and the right of the public to information. The Council reached this conclusion taking mainly into account the fact that 95% of European Google users do their searches on European national domains and that, although a global delisting would ensure a better protection to data subject's rights, this additional protection was outweighed by the interests of users outside of Europe to access information on their national domains which is legal

[153] Olivia TAMBOU, *op.cit.,* p. 253.
[154] ELECTRONIC PRIVACY INFORMATION CENTER, "Public Opinion on Privacy", https://epic.org/privacy/survey/, accessed: 11 June 2017.
[155] Olivia TAMBOU, *op.cit.,* p. 254.

according to their national laws.[156] However, Luciano Floridi, member of the Advisory Council, has stated that he was rather in favour of delisting on a national scale. Indeed, according to him, a systematic European delisting would always be disproportionate, highlighting that the information that requires delisting most of the time only serves a national interest and that most users access information on their local search engines, for several reasons including linguistic ones.[157]

Global blocking or removal measures should therefore not be the default answer and their reach should depend on the circumstances of each case. Indeed, any restriction of freedom of speech needs to be proportionate in a democratic society to satisfy the European and international standards of protection of that right. A case-by-case assessment would ensure such proportionality. In each case the question whether a global delisting is necessary to ensure the effective protection of the right to be forgotten of an individual or whether a local delisting would be sufficient to do so, should be asked. The interest of the public regarding the information at stake should always be taken into account as well.

Another issue raised with opting for global de-listing as the default standard is that it would be difficult to object to other states following the same approach. One could consider this approach unproblematic when it is implemented by EU states but it would become far more questionable if undemocratic regimes would go that way. For instance, Russia prohibits speech deemed to be 'gay propaganda' and China criminalizes speech that is critical of the government. What if these speeches were not accessible online from Europe following a decision of Russian or Chinese authorities to globally remove it? It would be highly problematic regarding the EU's conception of freedom of speech. Internet would not be internet anymore if it was emptied of content each time such content was unlawful somewhere in the world. It is therefore essential to find a solution that fits all legal systems.[158]

Moreover, it is necessary to make sure that the implementation of the right to delisting is not called into question by states for which the delisting at stake is unlawful. Indeed, a global

[156] The Advisory Council to Google on the Right to Be Forgotten, Final's report, 6 February 2015, https://static.googleusercontent.com/media/archive.google.com/fr//advisorycouncil/advisement/advisory-report.pdf, 2 July 2017

[157] Olivia TAMBOU, *op.cit.,* pp. 254-255 and Luciano Floridi, "Should you Have the Right to Be Forgotten on Google? Nationally, Yes. Globally, No", http://www.huffingtonpost.com/luciano-floridi/google-right-to-be-forgotten_b_6624626.html, 2 July 2017.

[158] Dan Jerker B.SVANTESSON, "Limitless Borderless to Forgetfulness? Limiting the Geographical Reach of 'The Right to be Forgotten'", *op.cit*., pp. 129-130.

implementation of the right to delisting is hard to reconcile with the principle of territoriality of jurisdiction, linked to the sovereignty of states and the principle of non-intervention. The authors Van Alsenoy and Koekkoek have proposed to solve this issue by applying a "*jurisdictional principle of reasonableness*", aimed at striking a balance between this principle of non-intervention and the necessity of effectiveness.[159] 'Reasonableness' means that "*states should weigh the realization of their own policy objectives against the risk of undue interference with the national policies of other states*"[160]. According to this approach, the implementation of the right to delisting would depend on the circumstances of each case and would need to take into account different criteria. The criteria would be the following ones:

- "*the potential interests other states might have with regards to the referenced content*",
- "*the likelihood of adverse impact if delisting is confined to "local" search results*",
- "*harmonization*", namely the extent to which the norm that is to be enforced is shared by other states, and,
- "*the presence of other connecting factors in relation to the territory*" of the state whishing to implement the right.[161]

Svantesson recommends to take into account the type of content at stake in each case. He recommends a Code of Conduct to provide support in the determination of the scope of the right to be forgotten. He suggests that some content could be subjected to global delisting, such as sexual content involving minors or posted without the authorisation of the protagonists, so called "revenge porn".[162]

In conclusion, it appears from the preceding developments that there is a need to adopt a more circumstantial approach by doing a case-by-case assessment.

We have seen in this part on the one hand, the obligations that states put on internet intermediaries regarding on users generated content and the processing of personal data and, on the other hand, the scope of application of the rules laying down these obligations. The

[159] BRENDAN VAN ALSENOY, MARIEKE KOEKKOEK, *op.cit*., p. 23.
[160] *Ibid*, pp. 23-24.
[161] *Ibid*, pp. 25-26.
[162] Dan .Jerker B. SVANTESSON, "The Extraterritoriality of EU Data Privacy Law – Its Theoretical justification and its practical effect on U.S.Businesses", *Standford Journal of International Law,* 2014, p. 17.

next part will be dedicated to the study of the impact that liability regimes for third party content have on freedom of expression and to the responsability of states and intermediaries for human rights violations that occur online.

PART 3: LIABILITY REGIMES IN REGARD OF INTERNATIONAL STANDARDS ON FREEDOM OF EXPRESSION

As we have seen, states have compelled internet intermediaries to police content that they consider illegal or harmful on their behalf through legal rules of liability. At the same time, intermediaries ban certain types of content in their terms of service policies, often outside the scope of international standards of legitimate restriction on freedom of expression. These private rules cannot be seen entirely independent of the action of the state. A good illustration of this assertion is the liability regime in the United Kingdom where the state has abstained from legislating the liability of intermediaries for content published by their users and has encouraged self-regulation and co-regulation. This issue of private bans of content is aggravated by the fact that the procedures under which content can be removed or blocked often lack transparency and that remedies offered to internet users for restriction of content are commonly inappropriate.[163] Furthermore, global internet intermediaries may in some countries face particular challenges with regard to their obligation to respect human rights. Indeed, in order to be able to offer their services in a state, they have to comply with its domestic laws. Serious issues arise when the state in question shows little compliance with human rights standards.

The preceding considerations showed that the internet's regulatory environment is unimaginably complex. In this context, the freedom of expression and of information of internet users is particularly exposed to various abuses.[164] The first chapter will describe, on the one hand, the different ways in which restrictions on content operated through intermediaries raise concerns with respect to the protection of freedom of expression online and, on the other hand, the means by which the situation can be redressed. The second chapter will address the question of accountability for violations of freedom of expression and protection of personal data: who will bear the responsibility: states or internet intermediaries?

[163] Article 19, *op.cit,,* pp. 3-4.
[164] *Ibidem*.

CHAPTER 1: Blocking and removal of content by internet intermediaries under the international standards on freedom of expression

As a reminder, any blocking or removal of content is a restriction of freedom of expression and, according to article 19§3 of the ICCPR, article 10§2 of the ECHR and article 52 of the EU Charter, such restrictions have to meet three conditions to be lawful: it has to rest on a legal basis, pursue a legitimate aim and be necessary in a democratic society, meaning it has to be proportionate. We will examine in section 1 the extent to which blocking measures comply with these conditions and we will do the same in section 2 for removal measures. Section 3 will analyse the concerns that restrictions of content raise regarding the right to a fair trial.

SECTION 1: Impact of blocking of content on the right to freedom of expression

A) A Legal Base

The most problematic hypothesis regarding this requirement is voluntary blocking, that is to say blocking operated by access providers either entirely on their own initiative, or with the encouragements of the national authorities.[165] Indeed, this practice raises serious concerns since access to sites, platforms or content is blocked without any legal basis. Such auto-regulation mechanisms therefore do not seem to meet the legality condition laid down in international human rights instruments in order for an interference with freedom of expression to be lawful.[166]

We have to recall that the E-commerce directive exonerates internet access providers from liability under certain conditions and prohibits laws that would put internet access providers under an obligation to monitor. It however does not prevent states from requiring them to block access to content when such content is illegal under their national laws. However, we saw that the new Regulation on Open Internet Access poses a general prohibition of blocking measures that are not ordered by the judiciary, namely voluntary blocking. This new Regulation however includes exceptions.

---

[165] *Report 2011 of the OSCE on Freedom of Expression on the Internet, op.cit.*
[166] Council of Europe*, Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, op.cit.*, pp. 19-28.

Even when there is a legal basis, the latter still needs to be clear and foreseeable to meet the legality requirement. The European Court of Human Rights recalled it in the case *Yildirim v. Turkey*[167]. In this case, the Turkish authorities had first issued a blocking order against a site hosted by Google Sites for having published content insulting the memory of Atatürk. Due to technical issues, the blocking of access to the entire online platform had subsequently been authorized. The owner of a web site hosted by Google Sites filed a lawsuit before the Court, claiming that the blocking of access to his site was violating his freedom of expression.

The Court looked whether the legal basis of the decision was sufficiently foreseeable. The Turkish law in question authorized a tribunal to order the blocking of access to specific content if there were sufficient reasons to think that such content constituted a criminal offense. The Court ruled that this law did not allow a blanket blocking order against an entire platform, that there was no evidence that Google Sites had been informed that it was hosting the allegedly illegal content or that it had refused to comply with a measure concerning a site subjected to criminal lawsuits and that the law had given extensive power to an administrative organ. It concluded that the law was not foreseeable and did not provide enough safeguards against abuses and therefore that the blocking order was breaching article 10 of the Convention.[168]

B) Legitimate aim and proportionality

Even when there is a valid legal basis for the blocking measures, these have to pursue a legitimate aim and be proportionate to this aim. In this regard, the blocking of domains of sites and platforms such as YouTube and Facebook is highly problematic. Indeed, it is not only the illegal content that is made inaccessible but also the entire site or platform, therefore including legal content. Such measures constitute a far-reaching interference in freedom of expression. It appears to be completely disproportionate and it is doubtful that it could be considered as necessary in a democratic society.[169]

Furthermore, blocking measures targeting entire websites or platforms without time limitation also have the effect to restrict the publication of subsequent articles whose content is not

[167] ECtHR, 18 March 2013, *Ahmet Yildirim v. Turkey*, app. n° 3111/10.
[168] Council of Europe, *Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, op.cit*., pp. 19-28.
[169] *Ibidem.*

known yet.[170] In the *Yildirim* case[171] studied above, judge Pinto de Albuquerque, who agreed with the finding of a violation of article 10 but not with all the reasoning of the judgment, made a concurring opinion in which he underscored that "*blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship*".

Blocking measures have severe implications on freedom of expression. From a human rights perspective, blocking of content should always be subsidiary to removal of measures. In consequence, they should be applied only when it not technically possible to obtain the removal of a content because the hosting provider is located abroad or impossible to reach, for instance because of its anonymity.[172]

SECTION 2: Impact of removal of content on the right to freedom of expression

With respect to liability regimes built on the safe harbour model, an important flaw is that the outlines of the safe harbours offered to hosting intermediaries are often not clear. This source of uncertainty for intermediaries can incite them to be overzealous, namely to unduly block or remove content to avoid any liability.

For example, in the European Union, the E-commerce Directive has undergone a lot of criticism linked to the ambiguity of some of its provisions, in particular article 14. As a reminder, this provision rules that hosting providers are not liable for illegal content hosted on their services when they 'act expeditiously to remove or disable access' to such content upon 'actual knowledge' of its existence. The issue is that it is not clear when exactly a hosting intermediary can be considered as provided with 'actual knowledge' or what 'expeditiously' exactly means in this context. Indeed, the Directive does not specify the information that should be provided in the notice and would give the intermediary actual knowledge, hence depriving it of the safe harbour, nor how much time it has to remove the content upon such knowledge. This lack of clarity is thus likely to lead to a chilling effect on expression, and

[170] *Ibidem.*
[171] *Ahmet Yildirim v. Turkey, op.cit.*
[172] Council of Europe, *Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, op.cit*., pp. 19-28.

lawful content risks being taken down, which would be an unacceptable interference in the freedom of expression.[173]

A second concern is that the directive confines itself to providing that hosting intermediaries are not liable for users generated content if they have no knowledge of it or if they remove the content quickly upon such knowledge. The regime that will apply to the intermediaries in the cases they are provided with such knowledge and do not react expeditiously enough are let to the appreciation of the domestic legislators.[174]

As a consequence, the EU Member States have developed several approaches with respect to the way hosting providers will incur liability. We have seen for instance that in the United Kingdom, it is generally self- and co-regulation mechanisms that have the favour of the authorities. In contrast, France has opted for a notice and take down approach. Regarding self-regulation mechanisms, the comments made above in relation to blocking of content concerning the lack of legal basis can be transposed to the removal of content.

Besides that, removal of content is not *prima facie* as illegitimate and disproportionate as blocking measures. Indeed, on the one hand, only the specific content involved is being taken down, and, on the other hand, it may be necessary sometimes in a democratic society to limit content that is illegal or harmful to protect third parties or public interest. The main problem is linked to the lack of guarantees with regard to the right to a fair trial, prerequisite of the right to freedom of expression. This concern is true both for self-regulation mechanisms and notice and take down procedures.

SECTION 3: Impact of restrictions of content on the right to a fair trial, prerequisite of the right to freedom of expression

With regard to self-regulation mechanisms, intermediaries rely on their terms of services policies to take their decisions on restrictions of content. Therefore, they restrict content without a decision on its lawfulness by a judicial authority or an independent organ. the assessment of legitimacy and proportionality is therefore not made by a judicial authority but

[173] Rebecca Mackinnon, Elonnai Hickok, Allon Bar, Hae-in. Lim, *op.cit*., p. 52.
[174] Council of Europe, *Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, op.cit*., p. 30.

by private actors, which are not in the best place to strike a fair balance between freedom of expression and competing interests. Another issue is the lack of transparency regarding the way decisions aimed at restricting content are taken, and that non-public actors are not being subjected to the same obligations of public scrutiny than national authorities. It can sometimes hide discriminatory practices or pressure from states. Furthermore, the remedies are often not appropriate and publishers of restricted content have little recourse against it.

With respect to notice and take down procedures, concerns regarding the right to a fair trial arise when an intermediary can be responsible for not having restricted content even without an order from a court or an independent organ enjoining it to do so. Under these circumstances, in which the rules are often not clear, we face the same problems then in self-regulation mechanisms: lack of transparency, private assessment of legitimacy and proportionality of the restriction and lack of appropriate remedies. It is aggravated by the fact that since they risk penalties, intermediaries will place themselves on the side of caution and take down content if there is any doubt about its lawfulness.

It is important to point out that these issues regarding freedom of expression protection are obviously exacerbated in the framework of a strict liability regime like the one adopted for instance in China. Indeed, internet intermediaries have the obligation to constantly monitor the internet and can be held liable for any illegal content. In these conditions, the dangerous 'chilling effect' on expression is aggravated just like the problems linked to extrajudicial decisions regarding restrictions of content.

SECTION 4: Preferred Model

It is now clear that holding internet intermediaries liable for third party generated content online poses a dangerous threat to freedom of expression. In consequence, the four Special Rapporteurs on Freedom of Expression recommended, in their Joint Declaration on Freedom of Expression and the Internet of 2011[175], that:

> No one should be liable for content produced by others when providing technical services, such as providing access, searching for, or transmission or caching of information;

[175] *Joint Declaration on Freedom of Expression and the Internet, op.cit.*

> Liability should only be incurred if the intermediary has specifically intervened in the content, which is published online;

The UN Special Rapporteur on freedom of expression has made a similar statement in 2011:

> Censorship measures should never be delegated to a private entity, and [...] no one should be held liable for content on the internet of which they are not the author. Indeed, no State should use or force intermediaries to undertake censorship on its behalf.[176]

Furthermore, he recommended that content should be restricted only after a judicial intervention, that the intermediaries should inform at least the publisher of the content of the procedure followed and give him a forewarning before applying the restriction and that effective remedies should be put in place, including a possibility of appeal before a judicial authority.[177]

Article 19, an organization defending freedom of expression, has elaborated a model for removal of third party content online that would ensure compliance with international standards on freedom of expression. According to it, the best model would be the immunity of hosting providers, social platforms and search engines for third party content when they do not take any part in the content. According to this model, an independent and impartial judicial body would always order any removal.[178]

However, it recognizes that in practice it is not always possible to implement this model because it would be too burdensome and onerous for the courts given the high number of requests for content restriction. In consequence, the best alternative to the notice and take down procedure would be a notice-to-notice procedure for civil claims relating to copyright, privacy, defamation or bullying.[179]

The procedure would be the following: a person harmed by specific content would send a notice to the host, including minimum requirements such as his name, the factual and legal reasons justifying the content removal, the location of the material and the time and date it was published or created, and would have to pay a fee. Then, the host would forward the

[176] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 16 May 2011, A/HRC/17/27, § n° 43
[177] *Ibid*, § n° 47.
[178] Article 19, *op.cit.*, pp. 16-18.
[179] *Ibidem*.

notice within for instance 72 hours to the wrongdoer, namely the creator or publisher of the content, and inform the claimant he forwarded the notice or if he did not, the reasons why it was not possible. A choice would then be offered to the wrongdoer: either removing the content and informing the claimant of the removal either filing a counter-notice within for example 14 days. In this latter case, the host would forward the counter-notice within for instance 72 hours to the claimant who would decide if he wants to bring the matter to a court. If the wrongdoer does not react to the notice within the time limit, intermediaries would then have to remove the content. The liability of intermediaries would in consequence be likely to incur in two instances: when they do not remove the material in case of inaction of the wrongdoer or when they fail to comply with their notice-to-notice obligations.[180]

With respect to serious crimes, such as hate speeches and pedopornography, Article 19 admits that this notice-to-notice procedure would not be the most appropriate. It states that anyone should be able to notify law enforcement of alleged serious crimes online. The latter would then either bring the matter to a court when it is not urgent either order the removal of the material in question when it is. Nonetheless, the law enforcement order would have to be confirmed by a court within a certain amount of time, for instance 48 hours. Anyone should also be able to notify the host about allegedly criminal content. The host would then in turn notify law enforcement of the content when the claim seems to be well founded and would also be able to remove the content as an interim measure when needed, in accordance with their terms of service.[181]

At this stage, we have analysed the liability regimes of internet intermediaries for third party content, the issues they raise in regard to freedom of expression and the model of restriction of content online that should be put in place to solve these issues. We have also studied the obligations incumbent to intermediaries regarding the processing of personal data under European Union Law. However, we have so far left aside the important issue of the accountability of states and internet intermediaries for violations of freedom of expression or of the right to protection of personal data. This question will in consequence be the subject of the next chapter.

[180] *Ibidem*.
[181] *Ibidem*.

CHAPTER 2: Accountability of states and internet intermediaries for violations of the right to freedom of expression and the right to protection of personal data

International human rights instruments are traditionally addressed to states, as is the case with the ICCPR and the ECHR. With regard to the EU Charter of Fundamental Rights, it applies to states and EU institutions. We will however focus in this chapter on the first two instruments.

The ICCPR counts 169 State parties. Each State party has to submit reports about their compliance with the ICCPR every four years to the Human Rights Committee, the monitoring body of the treaty. The latter then examines the reports and addresses its concerns and recommendations (called the 'concluding observations') to states. It also publishes general comments on the provisions of the covenant. A procedure of inter-state complaints is provided by the ICCPR. Furthermore, an optional protocol enables the Committee to examine individual complaints. 116 states have ratified it so far. [182]

With respect to the ECHR, it counts 47 state parties, namely all the members of the Council of Europe. The European Court hears allegations of violations of the Convention on applications of individuals against their state or on inter-state applications.

In consequence, a violation has to be attributable to a State in order for the Human Rights Committee or the European Court of Human Rights to have jurisdiction to examine it. However, human rights violations are increasingly attributable to private actors, for instance in the context of this thesis to internet intermediaries.

Two main palliatives have emerged in order to extend the scope of human rights law to private violations of human rights. The first one is the development of the theory of the horizontal effect of human rights provisions that we will examine it in section 1. The second one is the emergence of international human rights instruments addressed to private actors specifically that will be studied in section 2.

[182] OHCHR, "Human Rights Committee", http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIntro.aspx, 4 July 2017.

SECTION 1: Accountability of states

The European Court of Human Rights was the first to establish the horizontal effect of human rights provisions according to which states can be held responsible for private violations in certain circumstances.

This evolution has to be understood through the distinction made by the Court between positive and negative state obligations. Indeed, initially, state obligations regarding the European Convention were seen essentially as negative, namely as obligations to abstain from interfering in the rights enshrined in the Convention. Nonetheless, the Court has quickly stated that states also have positive obligations, taking into account the need to ensure the effectiveness of the rights guaranteed by the Convention. The duty on states to ensure the full enjoyment of human rights to all persons under their jurisdiction includes therefore the obligation to take reasonable steps to impede violations of the rights by individuals. If the state fails to do so, it can incur responsibility for violations committed between private actors.[183]

Hence, if an individual violates a provision of the ECHR, it will not by itself be sufficient to trigger the responsibility of the state. However, this responsibility can be triggered if the violation is linked to a failure of the state to fulfil its positive obligations. This failure is manifested in a deficiency of the legal order, that is to say in a lack of legal intervention, an insufficient legal intervention or an absence of measures tending to modify existing legal rules not compatible with the ECHR.[184]

In its General Comment no. 3, the Human Rights Committee has also established that in certain cases states can be responsible for violations of the ICCPR by private actors. Its words are the following:

> However the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State, not just against violations of Covenant rights by its agents, but also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities. There may be circumstances in which a failure to ensure Covenant rights as

[183] Jean-François AKANDJI-KOMBE, "Les obligations positives en vertu de la Convention européenne des Droits de l'Homme: Un guide pour la mise en oeuvre de la Convention européenne des Droits de l'Homme", *Conseil de l'Europe, Précis sur les droit de l'homme n°7*, 2006, pp. 10-16.
[184] *Ibidem*.

> required by article 2 would give rise to violations by States Parties of those rights, as a result of States Parties' permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities.[185]

If we apply these considerations to violations of freedom of expression and data protection by internet intermediaries in relation to the implementation of liability regimes in the European Union, it appears that in a majority of cases it will be possible to hold states accountable for these violations. This will be the case for example when they encourage self-regulation mechanisms or abstain from adopting a legal basis for the blocking of content. The violations ensuing are linked to the lack of legal intervention. It is the same for notice and take down procedures: when the procedures are not clear and incite intermediaries to be too cautious, leading to the taking down of legal content, the freedom of expression violations are linked to the failure of the state to provide internet intermediaries with a clear legal framework regarding liability for third party content.

Nonetheless, the pattern described above is applicable to democratic regimes that have a minimum commitment to human rights. The situation is very different in authoritarian regimes such as the Chinese one, where freedoms are highly restricted and censorship well spread. Indeed, on the one hand, China is not part of the ICCPR (although it has signed it) or any other regional human rights instruments and it is therefore way harder to hold it accountable for human rights violations. On the other hand, the human rights violations are particularly severe and it is hence essential to be able to hold internet corporations accountable when they are complicit of such violations by restricting content on behalf of the national authorities or handing over data to the latter in order to allow it to muzzle dissidents.

SECTION 2: Accountability of internet intermediaries

We will first study the role that some major internet intermediaries play or have played in the Chinese internet censorship. We will then present the main international instruments that have developed in the sense of a greater accountability of corporations for human rights violations, with a particular emphasis on the UN Global Compact and the question of its efficiency.

[185] Human Rights Committee, *General Comment no. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add. 1326, 29 March 2004, § n° 8.

A) Internet intermediaries' complicity in Chinese censorship

As stated before, China has adopted a model of strict liability of internet intermediaries. The latter have an obligation to monitor all the internet traffic and are liable for all their user generated content that is illegal under Chinese law. Furthermore, numerous types of speech are illegal under this Chinese law. We have seen in part 2 that there were 'nine forbidden content categories' which include any form of criticism directed at the current regime. It is interesting to note that despite the fact that China disregards most fundamental freedoms, a vast range of them are guaranteed by the Chinese Constitution. The Constitution provides that the "*States respects and preserves human rights*". Its article 35 guarantees "*freedom of speech, of the press, of assembly, of association, of procession and of demonstration*" and article 40 the freedom and privacy of correspondence. It also protects citizens against unlawful arrest and detention and states that each Chinese citizen has a right to "*criticize and make suggestions regarding any State organ of functionary*".[186] There is therefore a huge gap between Chinese well known practices and the guarantees provided by its Constitution.[187]

It has to be recalled that the Chinese government compels its internet access providers to block access to services offered by companies which do not abide by its rules and censor content on its behalf. We saw that for example Facebook, Google and Twitter are not accessible from Chinese territory.

Some leading US internet intermediaries have been accused to be involved in the Chinese internet censorship, in particular Yahoo!, Microsoft, Google and Cisco. Corporate complicity in China can be partly explained by the 'Chinese factor'. Indeed, the Chinese market offers a major commercial opportunity to corporations. In this context, the internet operators have chosen to continue their business as usual and to abide by Chinese rules. It is doubtful that these intermediaries would have adopted the same behaviour in other authoritarian regimes such as Myanmar or Zimbabwe.[188] Here we will analyse the way Yahoo! and Google have been cooperating in Chinese internet censorship.

[186] *Constitution of the People's Republic of China,* 1982, http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm, 6 July 2017.
[187] Surya DEVA, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?", *39 Geo. Wash. Int'l L. Rev. 255*, 2007, pp. 262-265.
[188] *Ibid.*, p. 261.

Yahoo! began to operate in China in 1999. It was one of the first foreign internet corporations to offer its services in the country. From the beginning, Yahoo! China facilitated internet censorship by filtering thousands of words, phrases and web addresses out of search results. From 2003, Yahoo! or its subsidiaries Yahoo! China and Yahoo! Hong Kong handed over data about cyber-dissidents to the Chinese national authorities, which resulted in many arrests and incarcerations. In 2005, Yahoo! merged its subsidiary Yahoo! China with a Chinese corporation, Alibaba.com. One of the major benefits of this merger for Yahoo! was to be able to do business in China without bearing the responsibility for the actions of its subsidiary, in particular for its complicity in internet censorship. One of the justifications advanced by the former vice president of Yahoo!, Michael Callahan, for the facilitator role of the corporation in censorship was the following:

> When we receive a demand from law enforcement authorized under the law of the country in which we are operating, we must comply. Failure to comply in China could have subjected Yahoo! China and its employees to criminal charges, including imprisonment. Ultimately, American companies face a choice: comply with Chinese laws or leave.[189]

It is noteworthy to underscore that while facilitating internet censorship, Yahoo! was doing campaigns such as "Yahoo! For Good" claiming that Yahoo! was "committed to making a difference in the world by empowering its users…with products and services that inspire them to make a positive impact".[190] Nevertheless, Yahoo has in 2015 decided to shut down its services in China.[191]

With regard to Google, it first launched a Chinese version of its search engine in 2000 and then physically established itself in China in 2006. At the beginning, Google was undergoing a 'passive' censorship since its search results were censored by the Chinese government. However, Google became active in this censorship in 2006 with the launch of a censored version of its search engine on the Chinese market, and terms such as "Tiananmen Massacre" were filtered out of the search results. Similarly to Yahoo!, Google claims that "acting ethically" is one of its core values and "an integral part of its business culture". One of the objectives of the search engine operator is "to make the world's information accessible to

[189] *Ibid,* pp. 267-269.
[190] *Ibidem.*
[191] Cnet, "Yahoo Lays out Hundreds as it Shuts Down Operations in China", https://www.cnet.com/au/news/yahoo-to-shut-down-operations-in-china/, 7 July 2017.

everyone, everywhere, all the time", stating however to be "responsive to local conditions".[192] Google finally ended its complicity in internet censorship by withdrawing from the Chinese market in 2010.[193]

As we said before, there have been efforts at the international level to adopt instruments aimed at putting pressure on corporations to respect human rights standards and prevent them from being complicit of human rights violations. We are now going to present the main ones.

B) International instruments for corporate accountability

The most important instrument regarding corporate human rights responsibility is the UN-driven Global Compact Initiative, launched in 2000. It is the "*world's largest corporate sustainability initiative*"[194] and it takes the form of a partnership between the private and the public sector in a way that promotes the voluntary commitment of companies to comply with universally accepted principles relating to human rights, labour, environment and anti-corruption.[195] It consists of ten principles in these fields, which are enjoying a 'universal consensus' and are derived from the Universal Declaration of Human Rights, the International Labour Organization Declaration on Fundamental Principles and Rights at Work, the Rio Declaration on Environment and Development and the UN Convention against Corruption.[196] The first two principles are relating to human rights. They state that "businesses should support and respect the protection of internationally proclaimed human rights; and make sure that they are not complicit in human rights abuses". There are 9000 companies and 4000 non-businesses that joined the initiative to this day.[197]

The Global Compact is however not a regulatory instrument. Indeed, it provides a platform to enable the partners to start a dialogue and to take action in a way that promotes respect for its principles but is not aimed at policing and sanctioning the actions of the companies which joined it.[198] Some limitations of the instruments have been pointed out, such as the lack of

[192] Surya DEVA, *op.cit.,* pp. 271-273.
[193] JYH-AN LEE, CHING-YI LIU, WEIPING LI, "Searching for Internet Freedom in China: a Case Study on Google's China Experience", *Cardozo Arts and Entertainment, Vol. 31:405,* 2013, p. 406.
[194] United Nations Global Compact, https://www.unglobalcompact.org/what-is-gc, 7 July 2017.
[195] Rikke Frank JORGENSEN, "Framing the Net, the Internet and Human Rights", *Edward Elgar Publishing Limited,* 2013, p. 57.
[196] Surya DEVA, op.cit., pp. 290-293.
[197] *United Nations Global Compact*, *op.cit.*
[198] Surya DEVA, op.cit. pp. 290-293.

enforcement mechanisms, the fact that the principles are vague and therefore at the same time hard to implement and easy to circumvent, and the fact that some companies are using the Compact's image as a marketing tool without being truly committed to the Compact principles. For instance, participating companies such as Nike, Shell or Nestle are often under allegation of disregarding human rights and labour principles and have been accused to use the Compact to "bluewash" their image.[199] It is noteworthy that Yahoo and Google have not joined the initiative.

Another important international instrument regarding the human rights responsibility of private companies is the UN Guiding Principles on Business and Human Rights[200] endorsed in 2011 by the UN Human Rights Council[201]. The resolution endorsing these guiding principles was following the consultative process that lasted one year, led by John Ruggie, the former UN Special Representative for Business and Human Rights.[202] The same resolution created a Working Group on Business and Human Rights, composed by five independent experts, charged to work on the implementation of these principles[203] and a global platform for discussions, sharing of ideas and practice: the Forum on Business and Human Rights. The latter is guided by the Working Group and brings together more than 2000 participants from national and international organizations, governments, civil society, the academic world or the media every year.[204]

The Guiding Principles are built on the 'protect, respect and remedy' framework. It states primarily that the duty to protect against human rights violations by businesses rely on states. They have a duty of protection regarding activities of businesses operating on their territory or subjected to their jurisdiction.[205] The Guiding Principles then establishes the private companies' duty to respect human rights.[206] In order to fulfil their obligations to respect human rights, the document requires companies to take the following steps:

---

[199] Ibid, pp. 294-301.
[200] Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", 2011, Geneva, United Nations. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[201] UNHRC Res 17/4 (2011), UN Doc A/HRC/RES/17/4
[202] See the 2008 report by John Ruggie to Human Rights Council at: https://business-humanrights.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf, 7 July 2017.
[203] Rikke Frank JORGENSEN, *op.cit.,* p. 57.
[204] OHCHR, "About the United Nations Forum for Business and Human Rights", http://www.ohchr.org/EN/Issues/Business/Forum/Pages/ForumonBusinessandHumanRights.aspx, 7 July 2017.
[205] *Guiding Principles on Business and Human Rights*, *op.cit.,* pp 3 à 12.
[206] *Ibid*, pp. 13 à 27.

1. Make ‘a policy commitment to meet their responsibility to respect human rights’;
2. Establish ‘a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights’;
3. Develop ‘processes to enable the remediation of any adverse human rights impacts they cause or to which they contribute.’[207]

Importantly, it establishes that the corporate responsibility to respect human rights "*exists independently of States’ abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations*".[208] The Guiding Principles are not based on voluntary commitment from companies but expect them all to comply with them. The instrument is not legally binding but seeks to provide a framework for states and companies to better understand their already existing human rights obligations under international law.[209]

The OECD Guidelines for Multinational Enterprises is another important document regarding the human rights responsibility of businesses. It was developed by states and constitutes the most complete voluntary code of conduct, containing recommendations relating to various areas, including human rights.[210]

Regarding initiatives relating specifically to the ICT sector, one of the first was the Global Network Initiative (GNI), active since 2008 and which consists of a multi-stakeholder partnership between companies, civil society and academics seeking to promote the respect of human rights standards by companies. The initiative was launched in order to bring solutions to states’ pressure on companies to comply with their national laws in a way not always compatible with international human rights standards, in particular regarding right to privacy and freedom of expression.

The GNI has created a voluntary code of conduct that provides companies with principles and guidelines regarding the implementation of human rights standards. Twelve companies have joined the initiative so far, including Yahoo, Microsoft, Google and Facebook.[211] Accountability, policy and learning are among the main focus of the GNI. Regarding

[207] *Ibid.*, p. 16
[208] *Ibid,* p. 13
[209] OHCHR, *Frequently Asked Questions about the Guiding Principles on Business and Human Rights*, 2014.
[210] Rikke Frank JORGENSEN, op.cit, *p. 57.*
[211] *Ibid.*, p. 58.

accountability, the participants have to self-report after one year of membership and the compliance of each company with the rules laid down in the code of conduct is assessed every two years. The Board can place companies that do not comply under review. It is however not a regulatory instrument and relies ultimately on the voluntary commitment and the participating companies' willingness to comply.

Other initiatives have been launched since the GNI, such as the Telecommunications Industry Dialogue on Freedom of Expression and Privacy, launched in 2011 and seeking, similarly to the GNI, to promote ICT companies' compliance with human rights.[212]

Although all these initiatives attempting to improve human rights compliance by businesses are commendable, we have seen that the instruments adopted in their framework belong to soft law and are based on the voluntary commitment of the companies, which means that the level of protection of human right is left to the goodwill of the companies.[213] As a result, at this stage states continue to be the decisive actors regarding human rights protection.

We will study in the next part the means by which freedom of expression and privacy are increasingly endangered by states, partly through the new obligations they put on internet intermediaries, in the framework of the fight against terrorism.

[212] *Ibidem.*
[213] *Ibid.,* p 59

PART 4: WORRYING TRENDS IN THE CONTEXT OF THE FIGHT AGAINST TERRORISM

The terrorist threat has considerably increased in Europe and more generally all across the world over the last years, in particular because of the terrorist group Al-Qaeda and more recently with the rise of the Islamic State for Iraq and Syria (ISIS) that declared its Caliphate in 2014. The latter has made from internet and particularly the social media platforms a central part of its propaganda strategy. In this context, counter-terrorism policies have been implemented by European states. These policies include a considerable strengthening of the liability regimes of internet intermediaries for content linked to terrorism and hate speech online and growing obligations on intermediaries in regard to the conservation and the handing over of personal data to national authorities.

The first chapter will study the developments with regard to the liability of internet intermediaries for third party content linked to terrorism and hate speech online and the second those concerning the processing of personal data.

CHAPTER 1: Reinforced liability for third party content

We saw in the second part of this thesis that the Commission put forward two proposals containing special measures in relation to the responsibility of intermediaries in the fields of terrorism and hate speech. These provisions are highly problematic on several counts.

The terrorism directive[214] has been adopted on the 23 February 2017. Article 4 provides that "*Member States shall take the necessary measures to ensure the prompt removal of online content constituting a public provocation to commit a terrorist offence* (…) *that is hosted in their territory*'" and that they "*shall also endeavour*" for such removal outside their territory. When the removal at the source is not possible, blocking measures can be taken. The last paragraph foresees some guarantees by providing that the measures "*must be set following transparent procedures and provide adequate safeguards, in particular to ensure that those measures are limited to what is necessary and proportionate and that users are informed of*

[214] *Directive 2015/0281 on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism., op.cit.*

the reason for those measures. Safeguards relating to removal or blocking shall also include the possibility of judicial redress".[215]

This provision raises serious issues in different regards. It is not clear which measures can be taken to comply with the 'prompt removal' requirement since several technical measures could be taken. There is also a risk that the incentive on states to 'endeavour to remove content outside their territory' combined with the possibility to issue blocking orders when removal is not possible could lead to the systematic issuing of blocking orders when sources of content are located outside EU jurisdiction. With respect to the guarantees provided, the provision is way to vague to ensure real protection. Indeed, it does not specify what should be the procedural safeguards or under which notice users should be informed, leaving a very wide margin of appreciation to states that could lead to abuses.[216]

With regard to hate speech, the Commission has proposed an amendment to the Audiovisual Media Services Directive on 25 May 2016.[217] The new article 28a of the Directive enjoins Member States to ensure that "*video-sharing platform providers take appropriate measures to (...) protect all citizens from content containing incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin"*. According to the article, appropriate measures include the adoption of a definition of hate speech in the terms of service of internet intermediaries, the establishment of a flagging or reporting system and of an age verification. The provision also states that co-regulation should be encouraged by states.

This drafting is problematic first because it calls for voluntary action by encouraging the adoption of a definition of hate speech in the terms of service of intermediaries. Indeed, private definitions of hate speech could not be compatible with standards of protection of freedom of expression set up by the Council of Europe. It also calls for co-regulation without any further precision. The phrasing of the provision can also suggest that these platforms would have a general obligation to monitor. Indeed, it provides that the measures 'should protect all citizens' which seems to imply to take proactive steps. Furthermore, the Explanatory Memorandum of the proposal advances that since the purpose of these video-

[215] Article 21 terrorism Directive.
[216] Monica HORTEN, *op.cit.,* pp. 12-13.
[217] *Proposal for a Directive of the European Parliament and the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, *op.cit.*

sharing platforms is to 'organize' content, their responsibility would lie into this organization and not in the monitoring of any illegal content generated on the platforms. However, for these intermediaries, mere organisation implies 'cataloguing, indexing and search algorithms'[218] and responsibility for this organization could therefore require them to take actions such as suppressing links or amending search algorithms, which amounts to monitoring.[219]

Furthermore, there is tendency among the EU Member States to grant extensive powers to administrative authorities to issue content restriction orders against internet intermediaries. This is the case as we have seen in France where the recent laws allow the administration to order removal and blocking of content inciting to or making an apology of terrorism without any prior intervention of the judiciary. Intermediaries which fail to comply with their obligations can be fined of 375 000 euros. In the United Kingdom, the police services also have the power to issue such orders and the blocking of content is operated broadly through the informal cooperation between internet access providers and the police services.

Recently, Theresa May has declared that she had agreed with Emmanuel Macron on the necessity to strengthen the liability regime of internet intermediaries for terrorist content in France and in the United Kingdom. She has proposed to criminalize internet operators who 'don't do enough' to take down terrorist content by fining them. Her statement has provoked considerable objections. The Independent Reviewer of Terrorism Legislation has compared her proposal with the regime of censorship and surveillance in China, stating notably that: "*We do not live in China, where the internet simply goes dark for millions when government so decides. Our democratic society cannot be treated that way*".[220] Furthermore, it is not clear what 'not doing enough' means. In Germany, a law has recently been adopted which allows to give internet operators which do not remove terrorist content fast enough fines of up to 50 million euro.[221]

---

[218] Monica HORTEN, *op.cit.*, p. 14.
[219] *Ibid.*, pp. 13-14.
[220] Courrier international, "Royaume-Uni. Pénaliser les géants du web pour lutter contre la menace terroriste, une bonne idée?" 3 July 2017, http://www.courrierinternational.com/article/royaume-uni-penaliser-les-geants-du-web-pour-lutter-contre-la-propagande-terroriste-une, 8 July 2017 and The Telegraph, "Government's anti-terror watchdog criticises Theresa May's plans to fine online companies over extremist material", 3 July 2017, http://www.telegraph.co.uk/news/2017/07/03/governments-anti-terror-watchdog-criticises-theresa-mays-plans/, 8 July 2017.
[221] The Telegraph, "Germany to fine Facebook and YouTube €50m if they fail to delete hate speech", 30 June 2017, http://www.telegraph.co.uk/technology/2017/06/30/germany-fine-facebook-youtube-50m-fail-delete-hate-speech/, 8 July 2017.

These developments show that despite the fact that under EU Law it is prohibited to require from internet intermediaries that they monitor the internet traffic, numerous new legislations are increasingly leading to that result. Indeed, internet operators are more and more criminalized for third party content and the fines that can be imposed on them are rising, extra-judicial procedures are increasingly preferred to a prior review of restrictions by the judiciary and these measures are coupled with the issues we already now in EU Law regarding in particular the lack of clarity of the safe harbours. This will indirectly result in compelling intermediaries to monitor all internet traffic.

CHAPTER 2: Reinforced obligations regarding the retention of data and the granting of access to data to national authorities

In the framework of its counter-terrorism strategy, the EU had adopted a Data Retention Directive[222]. It was stated in its preamble that the recent terrorist attacks had recalled "*the need to adopt common measures on the retention of telecommunications data as soon as possible*". This Directive imposed on providers of electronic communications services the obligation to retain numerous personal data of their users in order to make it available for the investigation and prosecution of serious crimes. It was however invalidated by the CJEU in its *Digital Rights Ireland* ruling[223]. The Court decided that the requirements of the Directive constituted serious interference with the right to data protection and the right to privacy guaranteed in the EU Charter of Fundamental Rights. It admitted that they were justified by an objective of general interest, namely public security.

However, it ruled that they were disproportionate because the broad interference with the fundamental rights of the individuals was not circumscribed enough to ensure that it was limited to what was strictly necessary. The grounds on which the Court based its conclusion

[222] The European Parliament and the Council, *Directive 2006/24/ on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, 15 March 2006, OJ L 105, 13.4.2006, p. 54–63.
[223] CJEU, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland and the Attorney General*, joined cases C-293/12 and C-594/12.

included the fact that the Directive confined itself to mention "serious crimes" without further specification, providing a broad access to personal data to national authorities, that it targeted all traffic data without exception or differentiation, that the retention period compelled the intermediaries to retain the data at least six month without making any distinctions regarding the nature of the data or the persons concerned and that the Directive lacked safeguards and did not require the retaining of data within the EU.[224]

Nonetheless, some Member States had already implemented the Directive in their national laws. After the *Digital Rights Ireland* ruling, two cases[225] were referred to the CJEU for a preliminary ruling on the question of the compatibility with EU Law of the obligation imposed, in the United Kingdom and in Sweden, on providers of electronic communications services to retain data relating to these communications, whose retention was foreseen by the invalidated Directive. The Swedish and English laws were setting out a general obligation to retain all data traffic and provided national authorities access to these data without limiting this access to serious criminality and without prior review by a court or an independent administrative authority.

The CJEU decided that the retention of data traffic and of data location constituted a particularly severe interference in the right to privacy and data protection and that consequently only the fight against serious crime was likely to justify such interference. It ruled that a national law targeting all data traffic without exception or differentiation was not consistent with EU Law because such law did not require a relationship between the retention and the threat for public security and in particular did not foresee a retention of data limited to a period or time and/or a geographic zone and/or a circle of persons likely to be involved in a serious crime. Such law was consequently not limited to what was strictly necessary and therefore not justified in a democratic society.

Conversely, the CJEU stated that a national law imposing a retention targeting specific data and aimed at fighting serious crime was compatible with EU Law, provided that such

[224] Emmanuelle BROUSSY, Hervé CASSAGNABERE, Christian GANSER, "Chronique de jurisprudence de la CJUE", *AJDA 2015. 2257*, 30 November 2015.
[225] CJEU, 21 December 2016, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis*, joined cases C-203/15 and C-698/15.

retention was limited to what was stricly necessary regarding the categories of data, the communication means, the persons and the period concerned. It added that such law had to be clear and specific and provide sufficient guarantees to protect data against risks of abuses. With respect to access of national authorities to the data retained, it confirmed that national laws have to set out substantive and procedural conditions to allow such access in addition of the objectives for which such access is authorized. Furthermore, the Court decided that a prior control by a court or an independent adminstrative authority was essential and that the persons concerned by the data accessed by the national authorities had to be informed. Finally, the Court ruled that the data has to be retained on EU's territory and had to be destroyed at the end of the retention period. [226]

It follows from the two rulings that data retention can be compatible with EU Law only under strict conditions that ensure that the right to privacy and the protection of personal data guaranteed by the EU Charter of Fundamental Rights are safeguarded. However, the efforts of some EU states to align their laws with the requirements set out by CJEU are far from being sufficient. Certain states have shown resistance to the rulings, accusing the Court of undermining their ability to ensure national security. These worrying trends of state surveillance are observed all across the world. We all remember the terrifying disclosures made by Edward Snowden about surveillance in the United States. The OHCHR has warned that governmental mass surveillance was "emerging as a dangerous habit rather than an exceptional measure"[227]. It constitutes therefore a major challenge for human rights protection nowadays.

[226] François-Xavier BRECHOT, "Clap de fin pour la conservation généralisée des données de connexion en Europe ?", *Rev. UE 2017*, *178,* 14 March 2017.
[227] Human Rights Council*, The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, 30 June 2014.

CONCLUSION

We have seen in the framework of this thesis that globalization and the development of the internet have been incredible opportunities to consolidate democracy by putting information within everyone's reach, including within the reach of individuals who did not have access to mainstream media before, and by enabling everyone to share any type of content online. The public sphere has been considerably enlarged and civil participation increasingly fostered.

On the other hand, we have also seen that the democratic potential of the internet has been challenged by several factors. The first major difificulty is the growing role of private actors in the protection of human rights, although they are not targeted by traditional human rights instruments in the protection of human rights. We have called these powerful private actors of the digital age the 'internet intermediaries'. We have focused on their role in the protection of two rights in particular: the right to freedom of expression and the right to the protection of personal data.

With respect to freedom of expression online, the fate of content created and published by users on their networks is at the end of the day under their 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. Hence, the guarantees attaching to freedom of expression under international human rights standards, in particular under the ICCPR and the ECHR, should always be respected. We have however found that this is often not the case, in particular because the decisions restricting content lack transparency, appropriate remedies are lacking or the judiciary is being excluded from the decision-making process.

Regarding the protection of personal data, internet intermediaries are in possession of countless data on their users. These data are a precious tool both for intermediaries and states. Indeed, 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. 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 right to privacy and data protection.

Nevertheless, if internet intermediaries undeniably have a large influence on the protection of these rights, it became apparent as we went along with our analysis that states remain the lead actors in their protection and the main responsibles, whether directly or indirectly, of the violations of these rights that occur online. Indeed, on the one hand, when intermediaries 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, as last resort, they can be excluded from the national market by the withdrawal of their license or, when they do not physically operate within the territory of the state, by the blocking of access to their services to users located within this territory. On the other hand, states have increasingly compelled intermediaries to police content online that they consider illegal or harmful on their behalf or to hand over data to national authortities.

With respect to restriction of third party content, they have made sure they can rely on the cooperation of intermediaries through the setting up of liability regimes, under which intermediaries that do not meet their obligations for the removal or blocking of content face civil or criminal sanctions. We have studied three models of liability. The first one was the broad liability model, under which intermediaries benefit from a near total immunity for third party content. This model is found for instance in the United States. The second one was the safe harbour model, which is the dominant model in the European Union and under which intermediaries are immune to liability under certain circumstances. Thirdly, we saw the broad liability model, under which intermediaries are liable for all content generated on their networks. We saw that the safe harbour model and the broad liability model were problematic because they provoked a chilling effect on expression online. We also saw that under the safe harbour model, some states, such as the United Kingdom, are encouraging self-regulation and co-regulation, namely pushing intermediaries to remove content without setting up clear rules which results to content restriction outside the scope of international standards of protection of freedom of expression. Furthermore, we have seen that there was a tendency to strengthen these regimes in the context of the fight against terrorism and to give increasingly more powers to administrative authorities.

Regarding data, we have seen that states are increasingly seeking to force intermediaries to retain these data and to provide them to national authorties, most of the time with insufficient safeguards against abuses. In particular in the context of the fight against terrorism, mass surveillance seems to become the norm more than an exeptional measure.

The level of protection of these rights is therefore mainly left to the hands of states, whereas the role of intermediaries, although important, remains limited. To ensure human rights protection online, states have to abstain from adopting legislations that compel or encourage internet intermediaries to act in a way not consistent with human rights standards and to legislate to oblige intermediaries to act in a way consistent with these standards. Most of the time it will therefore be possible to hold states responsible for violations occurring online. Consequently, traditional human rights instruments have not lost their importance and continue to be relevant to protect individuals against human rights violations in a globalized world.

Of course, a state can be internationally held responsible for human rights violation only if it is part of human rights instruments. We have analysed the case of China and its regime of broad censorship. We saw that China is not part of any human rights instruments and can therefore not be held responsible for human rights violations in regard of these instruments. We also saw that instruments have been developed to prevent private actors from being complicit of gross human rights violations by making them accountable for it. However, the impact of such instruments is limited. Indeed, these instruments are not legally binding and rest on the voluntary commitment of the corporations. Compliance of the latter with the principles laid down on them depends to a large extent on the willingness of the corporations.

Besides that, it seems that the ability of the internet to bring about social change in authoritarian regimes where human rights are poorly protected can be limited with sufficient state's determination. Internet in a globalized world is a powerful democratic tool that some authors have seen as a threat for authoritarian regimes, because of its potential ability through the dissemination of information to have a political impact anywhere. And, indeed, internet has played a key role in the overthrow of undermocratic regimes in the Arab Spring. Nonetheless, some states, such as China and Cuba, have so far succeeded in keeping to exercise 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.

Democratic states should be careful not to strengthen the responsabilities of intermediaries regarding data handing over and third party content too much at the risk of moving away from our democratic principles and move towards a system of internet censorship such as the Chinese one. Although the aims of content restriction or data providing are sometimes legitimate and necessary, interferences in freedom of expression and privacy that do not come alongside sufficient guarantees are a threat to democracy. In Europe, human rights principles have a constitutional value in most states and are enshrined in two regional instruments: the EU Charter of Fundamental Rights and the European Convention of Human Rights. These principles underlie any true democracy and are a condition for its existence. They should be respected in every circumstance, even in the context of an increasing terrorist threat. National security concerns should not justify the sacrifice of the values on which our democracies have been built and which define who we are.

BIBLIOGRAPHY

ACADEMIC ARTICLES

AKANDJI-KOMBE Jean-François, "Les obligations positives en vertu de la Convention européenne des Droits de l'Homme: Un guide pour la mise en oeuvre de la Convention européenne des Droits de l'Homme", *Conseil de l'Europe, Précis sur les droit de l'homme n°7*, 2006.

ARTICLE 19, "Defending Freedom of Expression and Information, Internet Intermediaries: Dilemna of Liability", *Free Word Centre*, 2013.

BAISTROCCHI Pablo, "Liability of Intermediary Service Providers in the EU directive on Electronic Commerce", *Santa Clara High Technology Law Journal*, Volume 19, Issue I, 2003.

BRECHOT François-Xavier, "Clap de fin pour la conservation généralisée des données de connexion en Europe?", *Revue de l'Union Européenne 2017*, *178,* 14 March 2017.

BROUSSY Emmanuelle, CASSAGNABERE Hervé, GANSER Christian, "Chronique de jurisprudence de la CJUE", *Actualité juridique du droit administratif 2015. 2257*, 30 November 2015.

CASTETS-RENARD CELINE, "Le renouveau de la responsabilité délictuelle des intermédiaires de l'internet", *Recueil Dalloz*, 2012.

DEVA Surya, "Corporate Complicity in Internet Censorship in China: Who Cares for the Global Compact or the Global Online Freedom Act?, *39 Geo. Washington International Law Review. 255*, 2007.

FRYDMAN Benoit, RORIVE Isabelle, "Regulating Internet Content through Intermediaries in Europe and the USA", *Zeitschrift für Rechtssoziologie 23*, 2002.

GHOERGHE-BADESCU Ioana, “Le droit à l’oubli numérique”, *Revue de l’Union européenne*, 2017.

HORTEN MONICA, "Content ‘responsibility’: The Looming Cloud of Uncertainty for Internet Intermediaries", *Center for Democracy and Technology*, 2016.

JORGENSEN Rikke Frank, "Framing the Net, the Internet and Human Rights", *Edward Elgar Publishing Limited,* 2013.

LEE Jyh-An, LIU Ching-Yi, LI Weiping, "Searching for Internet Freedom in China: a Case Study on Google's China Experience", *Cardozo Arts and Entertainment, Vol. 31:405,* 2013.

LOVELUCK Benjamin "Internet, vers la démocratie radicale?", *Gallimard I Le débat, 2008/4 n° 151*, 2008.

MACKINNON Rebecca, HICKOK Elonnai, BAR Allon, LIM Hae-in, "Fostering Freedom Online: the Role of Internet Intermediaries", *UNESCO and Internet Society*, 2014.

MAUBERNARD Christophe, “La protection des données à caractère personnel en droit européen: de la vie privée à la vie privée numérique”, RUE, July 2016.

RANDALL Maya Hertig, "Freedom of Expression in the Internet", *Swiss Review of International and European Law, Vol. 26, Issue 2, 2016*.

SEGUR Philippe, “Le terrorisme et les libertés sur l’internet”, *Actualité juridique du droit administratif*, 2015.

SVANTESSON Dan Jerker B., “Limitless Borderless to Forgetfulness? Limiting the Geographical Reach of ‘The Right to be Forgotten’”, *Oslo Law Review*, 2015, Issue 2.

SVANTESSON Dan Jerker B., "Delineating the Reach of Internet Intermediaries’ Content Blocking – “ccTLD Blocking”, “Strict Geo-location Blocking” or a “Country Lens Approach”?", *Scripted, Volume 11, Issue 2,* 2014.

SVANTESSON Dan Jerker B., "The Extraterritoriality of EU Data Privacy Law – Its Theoretical justification and its practical effect on U.S.Businesses", *Standford Journal of International Law,* 2014.

TAMBOU Olivia, « Protection des données personnelles: les difficultés de la mise en oeuvre du droit européen au déréférencement", *Revue trimestrielle du droit européen*, 2016.

THEARD-JALLU Cécile, Jean-Marie JOB Jean-Marie, Simon MINTZ Simon, "Invalidation de l'accord Safe Harbor par la CJUE: portée, impacts et premier éléments de solution"**,** *Dalloz IP/IT 2016*, 26, 18 January 2016.

VAN ALSENOY Brendan, KOEKKOEK Marieke, "The extra-territorial reach of the EU's 'right to be forgotten'", *CiTiP Working Paper Series*, 2015.

VAN DER SLOOT Bart, "Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe", Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 6*, 2015.

ZINGALES Nicolo, "Accountability 2.0: Towards a Special Responsability of Internet Intermediaries for Human Rights Violations", *Paper submitted for the 8th Symposium of the Global Internet Governance Academic Network*, 2013.

WEBSITES

Cnet, "Yahoo Lays out Hundreds as it Shuts Down Operations in China", https://www.cnet.com/au/news/yahoo-to-shut-down-operations-in-china/, accessed: 7 July 2017.

Council of Europe, *"Chart of signatures and ratifications of Treaty 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Status as of 04/06/2017"*, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=jFc8VQaU5, accessed: 15 June 2017.

Courrier international, "Royaume-Uni. Pénaliser les géants du web pour lutter contre la menace terroriste, une bonne idée?" 3 July 2017, http://www.courrierinternational.com/article/royaume-uni-penaliser-les-geants-du-web-pour-lutter-contre-la-propagande-terroriste-une, accessed: 8 July 2017.

Electronic Privacy Information Centre, "Public Opinion on Privacy", https://epic.org/privacy/survey/, accessed: 11 June 2017.

European Commission, Reform of EU data protection rules, http://ec.europa.eu/justice/data-protection/reform/index_en.htm, accessed: 5 June 2017.

European Commission, "Factsheet on the 'Right to be Forgotten' Ruling", http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, accessed: 9 June 2017.

European Data Protection Supervisor, "Glossary", https://edps.europa.eu/data-protection/data-protection/glossary/a_en, accessed: 10 June 2017.

FLEISCHER Peter, "Implementing a European, not Global, Right to Be Forgotten", 30 July 2015, https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html, accessed: 2 July 2017.

FLORIDI Luciano, "Should you Have the Right to Be Forgotten on Google? Nationally, Yes. Globally, No", http://www.huffingtonpost.com/luciano-floridi/google-right-to-be-forgotten_b_6624626.html, accessed: 2 July 2017.

IWF, "Why We Exist", https://www.iwf.org.uk/what-we-do/why-we-exist, accessed: 5 June 2017.

IWF, "URL Blocking: Good Practice", https://www.iwf.org.uk/become-a-member/services-for-members/url-list/url-blocking-good-practice, accessed: 17 June 2017.

Noerr, "BEREC publishes guidelines for net neutrality implementation", 2016, https://www.noerr.com/en/newsroom/News/berec-publishes-guidelines-for-net-neutrality-implementation.aspx, accessed: 5 June 2017.

Office of the High Commissioner for Human Rights, "Human Rights Committee", http://www.ohchr.org/EN/HRBodies/CCPR/Pages/CCPRIntro.aspx, accessed: 4 July 2017.

Office of the High Commissioner for Human Rights, "About the United Nations Forum for Business and Human Rights", http://www.ohchr.org/EN/Issues/Business/Forum/Pages/ForumonBusinessandHumanRights.aspx, accessed: 7 July 2017.

Ranking Digital Rights, "Chinese Internet Companies Show Room for Improvement", https://rankingdigitalrights.org/index2017/findings/china/, accessed: 19 June 2017.

The Advisory Council to Google on the Right to Be Forgotten, "Final's report", 6 February 2015, https://static.googleusercontent.com/media/archive.google.com/fr//advisorycouncil/advisement/advisory-report.pdf, accessed: 2 July 2017

The Telegraph, "Government's anti-terror watchdog criticises Theresa May's plans to fine online companies over extremist material", 3 July 2017, http://www.telegraph.co.uk/news/2017/07/03/governments-anti-terror-watchdog-criticises-theresa-mays-plans/, accessed: 8 July 2017.

The Telegraph, "Germany to fine Facebook and YouTube €50m if they fail to delete hate speech", 30 June 2017, http://www.telegraph.co.uk/technology/2017/06/30/germany-fine-facebook-youtube-50m-fail-delete-hate-speech/, accessed: 8 July 2017.

VERHOOF Dirk, "Qualification of news portal as publisher of users' comment may have far-reaching consequences for online freedom of expression: Delfi AS v. Estonia", *Strasbourg Observers*, 2013, https://strasbourgobservers.com/2013/10/25/qualification-of-news-portal-as-publisher-of-users-comment-may-have-far-reaching-consequences-for-online-freedom-of-expression-delfi-as-v-estonia/, accessed: 5 June 2017.

VOLOCK Eugene, "N.Y. bill would require people to remove 'inaccurate', 'irrelevant', 'inadequate' or 'excessive' statements about others", https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others/?utm_term=.5ea3681e7f0c, accessed: 11 June 2017.

CASE LAW

European Court of Human Rights

European Court of Human Rights, 2 February 2016, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, application n° 22947/13.

European Court of Human Rights, 16 June 2015, *Delfi AS v. Estonia*, application n° 64569/09.

European Court of Human Rights, 18 March 2013, *Ahmet Yildirim v. Turkey*, application n° 3111/10.

European Court of Human Rights, 4 December 2008, *S. and Marper v. The United Kingdom*, application n° 30562/04 and 30566/04.

European Court of Human Rights, 8 July 1986, *Lingens v. Austria*, application n° 9815/82.

Court of Justice of the European Union

Court of Justice of the European Union, 21 December 2016, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice and Geoffrey Lewis*, joined cases C-203/15 and C-698/15.

Court of Justice of the European Union, 6 October 2015, *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14.

Court of Justice of the European Union, 1 October 2015, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14, § n° 25 and § n° 29.

Court of Justice of the European Union, 13 May 2014, *Google Spain SL, Google Inc. V. Mario Costeja Gonzalez*, case C-131/12.

Court of Justice of the European Union, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others v. Minister for Communications, Marine and Natural Resources, Minister for*

Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland and the Attorney General, joined cases C-293/12 and C-594/12.

Court of Justice of the European Union, 26 February 2013, *Åklagaren v.Hans Åkerberg Fransson*, case C-617/10.

Court of Justice of the European Union, 24 November 2011, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10 and EUCJ, 16 February 2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*, Case C-360/10.

National Case law

French Constitutional Court, 10 June 2014, n°2004-496 DC.

LEGAL TEXTS

United Nations

United Nations Global Compact, https://www.unglobalcompact.org/what-is-gc, 7 July 2017.

Office of the United Nations High Commissioner for Human Rights, Resolution 17/4 ,UN Doc A/HRC/RES/17/4, 2011.

United Nations, Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, accessed: 5 July 2017.

United Nations General Assembly, International Convenant on Civil and Political Rights, 16 December 1966.

United Nations General Assembly, *Universal Declaration of Human Rights*, 10 December 1948.

Council of Europe

Council of Europe, *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, Entry into force : 1 October 1985.

Council of Europe, *European Convention on Human Rights*, 4 November 1950. Entry into force: 3 September 1953.

European Union

The European Parliament and the Council, *Directive 2015/0281 on combating terrorism and replacing Council Framework Decision 2002/475/JHA on combating terrorism*, 15 March 2017.

European Commission, *Proposal for a Directive of the European Parliament and the Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities*, 25 May 2016, COM(2016) 287 final

The European Parliament and the Council, *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*, 27 April 2016, OJ L 119/1, 4/5/2016, pp. 1 to 88.

The European Parliament and the Council, *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*, 27 April 2016, OJ L 119, 4/5/2016, pp. 89 to 131.

The European Parliament and the Council, *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*, 25 November 2015, OJ L 310/1.

European Commission, *Communication from the Commission to the European Partliamant, the Council , the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market for Europ*e, 6 May 2015, COM(2015) 192 Final.

European Union, *Charter of Fundamental Rights of the European Union*, 18 December 2000, entry into force: 1 Decembrer 2009.

The Council, *Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, 27 November 2008, OJ L 350, 30/12/2008, pp. 60 to 71.

The European Parliament and the Council, *Directive 2006/24/ on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, 15 March 2006, OJ L 105, 13.4.2006, p. 54–63.

The European Parliament and the Council, Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, 22 May 2001, OJ L 167 , 22/06/2001 pp. 0010 to 0019.

European Commission, *Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 26 July 2000, OJ 2000 L 215, p. 7.

The European Parliament and The Council, *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'),* 8 June 2000, OJ L 178, 17.7.2000, pp. 1 to 16.

The European Parliament and the Council, *Direcitve 98/48/EC amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations*, 20 July 1998, JO L 217-18.

The European Parliament and the Council, *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*, 24 October 1995, OJ L 281 23/11/1995, pages 31 to 50.

National laws

Loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme, 13 November 2014. (France).

Loi n°2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure, 14 March 2011 (LOPPSI 2). (France).

Loi n°2009-669 favorisant la diffusion et la protection de la création sur internet, (Hadopi I) 12 June 2009 and loi n°2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet, (Hadopi 2) 28 October 2009. (France).

Loi n°2004-575 pour la confiance dans l'économie numérique, 21 June 2004. (France).

People's Republic of China State Council, *Measures on the Administration of Internet Information Services*, 25 September 2000, Decree n° 292. (China)

Digital Millennium Copyright Act, 105th Congress (1997-1998), H.R.2281.ENR. (United States).

Art. L. 335-7 du code de la propriété intellectuelle, 1992. (France).

Constitution of the People's Republic of China, 1982, http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm, accessed: 6 July 2017. (China).

Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, 6 January 1978. (France).

POLICY DOCUMENTS

United Nations

Human Rights Council, *The Right to Privacy in the Digital Age, Report of the Office of the United Nations High Commissioner for Human Rights*, A/HRC/27/37, 30 June 2014.

Office of the High Commissioner for Human Rights, *Frequently Asked Questions about the Guiding Principles on Business and Human Rights*, 2014.

United Nations Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, 5 July 2012, UN Doc. A/HRC/20/L.13.

Human Rights Committee, *General Comment No 34*, 12 September 2011, CCPR/C/GC/34.

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011, A/HRC/17/27.

Human Rights Committee, *General Comment no. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add. 1326, 29 March 2004.

UN Human Rights Committee, *General Comment No 16*, UN Doc A/43/40, 181–183; UN Doc CCPR/C/21/Add.6; UN Doc HRI/GEN/1/Rev 1, 21–23, 8 April 1988.

European Union

Art 29 Data Protection Working Party, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" Case C-131/12*, 2014.

Council of Europe

Council of Europe, Etude Comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, 2015, pp. 14-16, https://edoc.coe.int/fr/liberte-des-medias/7286-pdf-etude-comparative-sur-le-blocage-le-filtrage-et-le-retrait-de-contenus-illegaux-sur-internet.html, 5 June 2017.

Swiss Institute of Comparative Law, "Comparative Study on Blocking, Filtering and Take-down of Illegal Internet Content", 2015.

Council of Europe, *Handbook on European Data Protection Law*, STCE n° 108, 1981.

Other

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 Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet*, 1 June 2011.