International Journal of African and Asian Studies
ISSN 2409-6938 An International Peer-reviewed Journal
Vol.80, 2022

Human Rights in the Digital Era: The Right to Privacy at Stake

Mahir Al Banna, PhD.

Associate Professor of International law, American University in the Emirates, P.O. Box 503000, Dubai United Arab Emirates

E-mail of the corresponding author: mahir.albanna@aue.ae

Abstract

The respect for fundamental human rights, including the right to privacy, is always invoked in opposition to the monitoring and social control techniques, but how rigorous and holistic analysis of the translation of these rights in a largely globalized and computerized world? Internet and new technologies: what remain of one's privacy?

However, data-intensive technologies are helping to create a digital environment in which individuals, governments and commercial enterprises are increasingly able to keep up, to analyze, predict, and even manipulate people's behavior to an unprecedented degree. If effective safeguards are not applied, these technological developments entail very significant risks for human dignity, autonomy, and privacy, as well as for the exercise of human rights in general.

The right to privacy is one of the fundamental pillars of human rights which finds its legal basis in international texts, inter-alia, the 1948 Universal Declaration of Human Rights, the 1966 International Covenant on Civil and Political Rights (ICCPR), and the 1950 European convention of human rights (ECHR).

In accordance with the instructions of the relevant resolutions of the United Nations General Assembly and the Human Rights Council, have organized expert consultations and published reports to explore issues that threaten the right to privacy and other human rights in the digital age. The United Nations General Assembly adopted on December 16, 2020, a resolution in which it "reaffirms fundamental of the right to privacy and renews international commitments to ending all abuses and violation of this right worldwide."

Keywords: Human rights – Right to Privacy - Digital technology – ICCPR – ECHR – Cyberspace

DOI: 10.7176/JAAS/80-08
Publication date: August 31st 2022

1.Introduction

The right of access to the Internet, which is an obvious benefit of information technology, and which reflects freedom of expression, has become a new human right which is not conferred by any State. But this right, if it is not limited, risks to infringe on another human right: the right to privacy. While fundamental rights and human rights are valid in the digital world as well as in the analog world, the progress of digitization does reveal new challenges. First, because most international conventions and catalogues of fundamental rights in national constitutions date from the analogue era, they were not originally drafted to resolve issues related to digital processes. For example, the rise of social networks raises an unprecedented question: does freedom of opinion apply to tweets? It is therefore necessary to adapt strategies for the protection of fundamental rights and human rights to the evolution of society and to reinterpret them so that they also address the problems posed by digitalization.[1]

[1] Sabrina Ghielmini, Christine Kaufmann, Charlotte Post, Tina Büchler, Mara Wehrli et Michèle Amacker, « Droits fondamentaux et droits humains à l'ère numérique », © 2021 – CC-BY-NC-ND (ouvrage), CC-BY-SA (texte) Éditeur : Centre suisse de compétence pour les droits humains (CSDH). P 32.

Amid the technological revolution in which everyone is the willing actor and the potential victim how to avoid being submerged by the digital tsunami? Whenever one order something online, or use a free Wi-Fi service, he gives up some privacy in exchange for something of value.

When opening an application on your smartphone, does a user wonder where his location or consultation data will end up? Facebook, Google are surveillance systems; every time a user uses a free service, he is not a customer but a product. Some are not aware of it, while others admit that they are being watched and say that they are not doing anything illegal, so they have nothing to hide.

Strategies must be adopted to help us free ourselves from the constant technological dependence. We speak of the right of the individual capacity to put an end to the connections that make us dependent from the outside.[1] When does the privacy breach occur? The privacy breach occurs when a third party takes a user's data for storage.

In fact, the data can be collected with the consent of the user who will voluntarily provide certain personal information: first and last name, date of birth, studies, personal situation, musical tastes, sexual orientation. There is a paradigm shift in the relationship that individuals have to the network at a time when they freely concede their data to be monetized by large Internet companies. The "Cambridge Analytica" of April 2018 is the perfect illustration.

The private data analytics company reportedly retrieved data from 37 million Facebook users: "In total, we believe that information about up to 87 million people – mainly in the United States – may have been wrongly shared with Cambridge Analytica."[2] The latter, also specialized in political influence, participated in Donald Trump's campaign in 2016. Mark Zuckerberg, the creator of Facebook, was even forced to explain himself to the US Congress on April 10, 2018.

Faced with very angry elected officials due to the failure of Facebook on data protection, the boss of Facebook made long apologies and acknowledged his failures: It is now clear that we have not done enough to prevent these tools from being used for harmful purposes. This includes fake news, foreign interference, hate speech and privacy. We didn't realize enough about the extent of our responsibility, and it was a big mistake. It was my mistake, and I'm sorry. I created and run Facebook; I am responsible for what happens there."[3]

Nevertheless, his argument was not convincing, and the offensives of the elected representatives multiplied: Would you give us the name of the hotel in which you were last night? (...) And the names of the people you exchanged messages with last week? (…) Your right to privacy. It is about your right and whether you are ready to give it up in order. Everyone should be able to control how their data is used."[4]

This study will focus on human rights protection in the digital age by examining the internet access as a human right and its impact on the right to privacy **(Part I),** and the rules designed to guarantee the legal security of Internet users' cyberspace by international instruments as well as the measures adopted by States and private companies **(Part II).**

[1] Stefano Rodota, "Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives ». La Découvertes, « Mouvements » 2010/2 n0 62 pages 55 à 70. P 64.

[2] 26 LE MONDE, Cambridge Analytica : 87 millions de comptes Facebook concernés. Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptesfacebook-concernes_5280752_4408996.html, [consulté le 16 avril 2018].

[3] 27 LE PARISIEN, Facebook : ce qu'il faut retenir du mea culpa de Mark Zuckerberg devant le Congrès, 10 avril 2018. Disponible à cette adresse : http://www.leparisien.fr/high-tech/facebook-ce-qu-il-faut-retenir-du-mea-culpa-de-mark-zuckerberg-devant-le-congres-10-04-2018-7657422. php, [consulté le 8 mai 2018].

[4] 28 DUNAWAY J., Sen. Dick Durbin Proves Mark Zuckerberg Is As Awkward As the Rest of Us, 10 avril 2018. Disponible à cette adresse : https://slate.com/technology/2018/04/dick-durbins-questionat-the-senate-congressional-hearing.html, [consulté le 8 mai 2018].

2. Is Internet Access a Human Right?

A UN General Assembly human rights council report had examined the questions of whether the access to internet is considered as a human right. It declares access to the internet a basic human right that enables individuals to "exercise their right to freedom of opinion and expression".[1] The report condemned France and the United Kingdom, which have passed laws to remove accused copyright scofflaws from internet. It also protested blocking internet access to quell political unrest. The report considered that disconnecting people from internet a violation to international human rights law, especially paragraph (3) of Article 19 of the ICCPR.[2]

A rapid reaction from Vinton Cerf, the Vice-president of Google, described as the father of internet who, while admitting that the internet access may be a civil right, defined as a right conferred by law, argued that internet access is not a human right. In his editorial in New York Times[3] he claimed: "*The best way to characterize human rights is to identify the outcomes that we are trying to ensure. These include critical freedoms of speech and freedom of access to information and those are not necessarily bound to any particular technology at any particular time. Indeed, even the United Nations report, which was widely hailed as declaring internet access a human right, acknowledged that the internet was valuable as a means to an end, not as an end in itself*".[4] The first limitation to regulating internet can be the human rights respect. The freedom of expression is provided by Article 9 of the UDHR:" everyone *has the right to freedom of opinion; this right includes freedom to hold opinion without interference and to seek, receive and import information and ideas through any media and regardless of frontiers*".[5]

So, the United Nations Organization recognizes that all individuals can express their thoughts and ideas in a wide and unrestricted environment that protect his/her speech once posted in a social media. However, this right is not absolute. The paragraph (2) of Article 29 of the 1948 UDHR states that the exercise of freedom of expression is subject "*to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order, and the general welfare in a democratic society* ".[6] But this article does not clarify when and how speech may be censored. As for the ICCPR, it has a stricter level, under which States parties must prohibit by law 'any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence'.[7]

By asking the States to take internal action, the Pact uses a greater assurance on fighting back harmful speech. In comparison to the UDHR which is an instrument, the ICCPR with 74 signatories and 168 parties possesses a legally binding force.[8] So, finding the right balance between internet governance and freedom of expression is a particularly difficult challenge.[9]

3. Right to Privacy

Privacy as enshrined in article 12 of the 1948 Universal Declaration on Human Rights (UDHR) is an important right to develop human personality and to protect human dignity. It gives us protection from unwarranted intervention in our lives and helps us establish frontiers to limit who has access to our information. But at that time, the drafters of the UDHR could not foresee the outcomes of the digital age technologies and their

[1] A/HRC/27/17
[2] Article 19 provides that;"1. Everyone shall have the right to hold opinions without interference. 2. 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. 3. 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.
[3] Editorial of New York Times, January 4th
[4] Ibid.
[5] Universal Declaration on Human Rights. G.A Res. (III) A, UN Doc. A/ RES/27 (III) art. 19 (Dec., 10 1948).
[6] 9. art, 50 note supra, UD
[7] International Covenant on Civil and Political Rights, Dec. 1966, 16, S, Exec. Rep 999, 23-102 UNTS 171, Art 20.
[8] ,(International Covenant on Civil and Political Rights, United Nations Treaty Collection (Jan. 2015, 5), http:// treaties.un.org/Pages/View Details.
[9] See Maura Conway, "Le Terrorisme et la Gouvernance de l'Internet »,Revue de l'Information et la Sécurité Internationale, 2007, 3 0, p 28.

considerable impact on the concept of privacy. This human right is also set forth in the 1966 ICCPR, article 8 of the ECHR, and in article 8 of the Charter of the Fundamental Rights of the European Union.

The original definition of privacy as "the right to be left alone" has not been abolished, but now fits into a context that has aggregated different elements.[1] The right to privacy is a liberty right related to secrecy, to limiting the knowledge of others about oneself.[2] It protects an individual's choice what to share and with whom. As such, it could be described as the right to keep a sphere of our lives away from government intrusion, and away from the intrusion of others with whom we don't want to share certain aspects of our lives.[3]

The first effective innovation was introduced by Alan Westin - the father of modern data privacy law- who defined privacy as the as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[4] Basically, Westin argued that citizens should retain ultimate control over their personal data, including how much of their personal information is disclosed and to whom, how it should be maintained and how disseminated, therefore creating the groundwork for current understandings of online privacy laws way before the Internet was even a thing.[5]

A question has been raised to know whether people have the right to own their own data and to know what their government or the private actors are doing with their data.[6] In this regard, in May 2014 the European Court of Justice in Luxembourg (ECJ), rules in favor of a Spanish citizen's right to privacy. The Court's judgement upholds "*European citizens' right to be forgotten",* that is, "*their right to have embarrassing and currently misleading information deleted from the internet*".[7]

4.Human Rights Protection in Cyberspace

In this section we will study the international human rights framework in relation to the right to privacy and study challenges the impact raised by modern communication technologies, as well as the involvement of governments and the private sector in this regard.

Efforts to construct a global coordination and policy-making framework for the Internet began in the mid-1990s and to date remain unsuccessful.[8]No State, or international organization in overall charge to ensure compliance with the law in respect of the way the internet works,[9] nor is there a convention applicable to internet, although there are national laws and international treaties that are applicable to activities on the internet.[10] In spite the calls from human rights courts and international organizations condemning mass surveillance, still there is consensus on how to bring those activities in line with human rights law. To ensure the protection of individuals against illegal or arbitrary interference which result from mass surveillance effective national legal framework must be in place. Nonetheless, in many jurisdictions, national legislations are nonexistent, ambiguous, or outdated. With the insufficient existing legal framework, it is challenging to achieve a legally binding treaty.[11]

[1] Stefano Rodota, Nouvelles Technologies et Droits de l'Homme : Faits, Interprétations, Perspectives », La Découvertes, « Mouvements » 2010/2 n0 62 pages 65.
[2] Cavoukian, A. and Tapscott, D., "Who Knows: Safeguarding Your Privacy in a Networked World", McGraw Hill, New York, 1997.
[3] Newell, P. B.," Perspectives on Privacy", Journal of Environment Psychology, vol. 15, ed 2, 1995.
[4] Alan Westin, " Privacy and freedom" , Atheneum, New York 1967.
[5] https://www.osano.com/articles/alan-westin#:~:text=In%20%E2%80%9CPrivacy%20and%20Freedom%2C",was%20revolutionary%20in%20its%20approach
[6] Mellissa E. Hathaway, « Connected Choices: How the internet is challenging sovereign dimensions", American Foreign Policy Vol 36. No 2014/5, p. 310.
[7] European Court of Justice (ECJ), Case C12/131
[8] Milton Mueller, et al. "The Internet and Global Governance: Principles and Norms of a New Regime", (2007) 13 Global Governance.
[9] Council of Europe Commissioner for Human Rights, "The Rule of Law on the Internet and in the Wider Digital World", (2014), 36.
[10] Council of Europe, Convention on Cybercrime (23 November 2011) ETS No 185, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1 October 1985) ETS No 108.
[11] Eliza Watt, "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance", 2017 9th International Conference on Cyber Conflict. Defending the Core. 2017 NATO CCD COE Publications, Talinn. P 2.

Since Snowden's disclosure of mass surveillance in 2013, the United Nations General Assembly and the United Nations Human Rights Council have passed resolutions on privacy protection in the digital age each year. These resolutions have progressively developed international standards on how to ensure the right to privacy on the Internet, including addressing the risks posed by new and emerging technologies. They have asserted that international human rights law applies as much offline as online.[1] In fact, Resolution 69/166 called upon member States to review their practices and legislation on the interception and collection of personal data, including mass surveillance, to ensure the full and effective implementation of their obligation under international human rights law. Resolution 28/16 in 2015 also urged States to provide 'an effective remedy and encouraged the Human Rights Council to identify 'principles, standards, and best practices' for protection of privacy.[2]

In 2017, the UN General Assembly resolution addressed encryption and its importance to human rights. The 2020 version reaffirms the strong recommendations on encryption and anonymity adopted in previous versions of the text, calling on states not to interfere with technical solutions to secure and protect the confidentiality of digital communications, and encourage companies to work towards the adoption of these technologies. This resolution goes even further in implementing policies on encryption and anonymity that "recognize and protect the privacy of individuals' digital communications".

The resolution reaffirms the importance of the right to privacy and renews the international commitment to put an end to all abuses and violations of this vital right worldwide. It highlights the interdependence and indivisibility of the right to privacy with other fundamental human rights, including freedom of expression.

Nevertheless, this resolution missed the opportunity to provide strong and strong recommendations to states on some emerging threats to privacy rights, such as on the face and breach recognition technology. In fact, the 'big data' and artificial intelligence are often used to facilitate State surveillance and threaten key freedoms, including freedoms of movement, expression, association and assembly, and the right to privacy. Linked with this point, the use of facial recognition can lead to human rights violations when and where they are used without the consent of individuals concerned.[3]

The Human Rights Committee has applied this framework in several of its Concluding observations[4] and this practice is also present in the jurisprudence of the European Court of Human Rights. The Court has held that the notion of 'private life' is 'not susceptible to exhaustive definition'[5] and has found on numerous occasions that 'protection of personal data is of fundamental importance to a person's enjoyment of respect for his or her personal data and family life'.[6] Article 8 of the Charter of Fundamental Rights of the European Union explicitly recognizes the right to protection of personal data separately and in addition to the right to privacy under article 7.[7] In this regard, the Court of Justice of the European Union (CJEU) delivered a landmark decision in *Schrems v Data Protection Commissioner*,[8] holding that 'legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental rights guaranteed by article 7 of the Charter'.[9]

The raised question is : can the provisions of ECHR and ICCPR function as data protection in their own right? The issue is particularly significant for citizens in countries that lack domestic data protection laws and not legally or politically bound to introduce such laws pursuant to an international instrument dealing specifically with data protection but are party to the ICCPR and/or ECHR. It is also significant for citizens in States that do have domestic data protection laws and/or are obliged to introduce such laws pursuant to an international instrument dealing specifically with data protection.

[1] UNGA Res 68/167 (n6).
[2] UNGA Res 28/16 (26 March 2015) UN Doc A/HRC/28/16.
[3] https://www.ohchr.org/en/statements/2020/12/glion-human-rights-dialogue-2020-glion-viihuman-rights-digital-age-making
[4] Eliza Watt, p. 5.
[5] *Bensaid v the United Kingdom* (App No 44599/98) (2001) ECHR para 47; *Botta v Italy* (App No 21439/93) (1994) ECHR.
[6] *MK v France* (App No 19522/09) (2013) ECHR; S *and Marper v the United Kingdom* [GC] (App Nos 30542/04) and 30566/04) (2008) ECHR.
[7] Charter of Fundamental Rights of the European Union, arts. 7 and8, 2000/C 364/01 (12 December 2000)/
[8] Maxmilian *Schrems v Data Protection Commissioner* (6 October 2015) Case C- 362/14.
[9] Id, para 94.

It is uncertain to interpret and apply the right to privacy norms under Article 17 of ICCPR in the context of cyberspace. In fact, this international instrument which was adopted more than fifty years ago needs to be more developed to be more relevant and beneficial to the realities of the current digital era. That means to modernizing of the concept of 'right to privacy' necessitates more detailed and universal understanding of its meaning in the 21st century.[1] The definition of privacy must also encompass the idea of autonomy and self-determination, which in some countries such as Germany gives rise to a constitutional right to 'information self-determination'.[2] This idea is also referred to as 'informational privacy' and is concerned with the interest of individuals in exercising control over access to information about themselves.[3] This is reflected in the current general comment to article 17, according to which 'the gathering and holding of personal information on computers, databanks and other devices by public authorities or private individuals or bodies, must be regulated by law'.[4]

Some States suggested the adoption of a new additional Protocol to Article 17 ICCPR for the 'digital sphere'.[5] The subject was suggested in the 35th International Conference of Data Protection and Privacy Commissioners and supported by most of the privacy authorities, except for the United States.[6] For many reasons the additional protocol is not envisaged : the difficulty to arrive to an agreed text, the existing legal standards do not apply to digital communications, and States not ratifying the protocol would remain free to argue they are not bound by the standards elaborated in the protocol. The Special Rapporteur adopted a pragmatic and a realistic approach, expecting that protection of privacy could be increased by incremental growth of international law through the clarification and eventually the extension of existing legal instruments.[7]

For Lee A Bygrave, "*If the right to privacy pursuant to the ICCPR and/or ECHR provides as a higher standard of data protection than is provided by the domestic rules or the international instrument, the citizens may be able to gain some relief in cases where data on them are processed in compliance with domestic laws but not the ICCPR and/or ECHR. Again, the governments of the countries concerned will be under a legal duty to raise the domestic levels of data protection to the level required by either of the two human right treaties*".[8]

It is important to that there were four relevant instruments in this regard: the CoE Convention on data protection, the EC Directive on data protection, (both are legally binding instruments).[9] The third one is the OECD Guidelines Governing Protection of Privacy and Transborder Flows on data[10], and the last instrument is the UN Guidelines Concerning Computerized Personal Data Files[11]

It should be noted that the enforcement mechanisms for the ECHR are more powerful than those for the ICCPR. Unlike the ECHR, the ICCPR lacks proper judicial body to enforce its provisions.[12] Instead, the ICCPR has an oversight and complaints-handling body in the form of the Human Rights Committee.[13] Many cases law has been developed around article 8 of the ECHR and article 17 of the ICCPR which indicates that both instruments embrace core data protection principles.

In its General Comments 16, the Human Rights Committee has stated that article 17 of the ICCPR requires legal implementation of essential data protection guarantees in both public and private sectors:

[1] UNHRC (n22), para 46.
[2] Ibid.
[3] Id, para 25.
[4] Ibid.
[5] Ryan Gallagher, "After Snowden Leaks" Countries Want Digital Privacy Enshrined in Human Rights Treaty", Slate (26 September 2013).
[6] 35th International Conference of Data Protection and Privacy Commissioners, Resolution on Anchoring Data Protection and Privacy in International Law, (23-26 September 2013).
[7] Eliza Watt, "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance", 2017 9th International Conference on Cyber Conflict. Defending the Core. 2017 NATO CCD COE Publications, Talinn. P 4.
[8] Lee A Bygrave, "Data Protection to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, 1998, vol 6, pp. 247-284 p 248.
[9] Ibid.
[10] (Paris: OECD, 1980) adopted on 23.9.1980
[11] (Doc E/CN. 4/1990/72, 20.2.1990/, adopted by the UN General Assembly on 4.12.1990.
[12] The ICJ does not have jurisdiction to hear complaints concerning breaches of the Covenant.
[13] D Mc Goldrich, "The Human Rights Committee: Its Role in the Development of the International Covenant on Civil and Political Rights", Oxford: Clarendon Press, 1991.

"*The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant […] The gathering and holding of personal information on computers, databanks, and other devices, whether by public authorities or private individuals and 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 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 law, every individual should have the right to request rectification or elimination*".[1]

The essential object of article 8 of ECHR has been expressed in terms of protecting 'the individual against arbitrary interference by the public authorities in his private or family life'. But article 8 does not merely oblige a State party to abstain from interfering with private life; it additionally creates 'positive obligations' on the State party to take action to ensure that private life is effectively respected.[2] For example, it has been held that, under certain circumstances, a State party is obliged under article 8 (1) to establish a procedure for independently determining persons' demands for access to information kept on them by a public authority.

4.1 Responsibility of States

States have, under international conventions and their constitutions, an obligation to protect individuals and private companies from any interference by other private persons with their fundamental rights and human rights. To this end, they have, for example, laws on data protection or against personality breaches. However, it is difficult for them to fulfil this obligation in the field of digitization: on the one hand, the development of legislation does not keep pace with technological progress, and on the other hand, digital processes are often cross-border. Thus, for example, social networks unite people from a wide variety of countries, making it difficult to regulate these networks at national level.[3]

While the right to privacy is not absolute, any limitation to it should be provided by law and authorities must justify this limitation by proving that it is connected to the legitimate aim. Thus, when authorities decide to conduct surveillance activities that should be based on balancing the interference with the right to privacy with the legitimate public interests that the authorities want to protect.

For the Human Rights Committee, States' obligations under ICCPR extend not only to a State's territory, but to "anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party".[4] The question to be raised is to which extent this would apply to online communications? To give an answer one should stress the universal nature of human rights: States' negative obligation (not to interfere illegally with the right to privacy) applies without any territorial limitation, while States' positive obligation (to protect right to privacy from unlawful interference by third parties) only applies where a State has territorial control.

4.2 Responsibility of Companies

Another challenge that arises in relation to fundamental and human rights in the digital world is the status of the actors involved. Indeed, technologies are designed almost exclusively by private entities, which have a lot of leeway to decide what will be developed, and what rules to set for the use of their services and technologies. In many respects, the State does not adopt legal provisions or instructions. In addition, it often happens that the

[1] General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181-183; UN Doc CCPR/C/21 Add. 6; UN Doc HRI/GEN/1/Rev 1, 21-23), paras 7 &10.
[2] See Marckx v Belgium (1979) Series A, supra 32, para 31; Airey, supra n 32, para 31.
[3] Sabrina Ghielmini, Christine Kaufmann, Charlotte Post, Tina Büchler, Mara Wehrli et Michèle Amacker, « Droits fondamentaux et droits humains à l'ère numérique », p 33.
[4] General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181-183; UN Doc CCPR/C/21 Add. 6; UN Doc HRI/GEN/1/Rev 1, 21-23), paras 7 &10.

companies in question have more specialized expertise than the public services responsible for a given issue. All this gives the private sector a considerable influence on the digital domain, and often a step ahead of the State.[1]

This situation is problematic because companies are not directly bound by fundamental rights and human rights, which instead create obligations for the State and for private individuals assuming a task of the State. Therefore, persons whose rights are infringed by private companies cannot directly assert fundamental rights and human rights to obtain justice. For this reason, a debate should take place at the national and international levels on the need for a mechanism to bring or compel companies to respect these rights and on its modalities.[2]

It was emphasized that it is the private sector that develops and maintains internet and telecommunications system, and this same private sector is an integral part of both the problem and the solution. In some countries internet and telecommunications companies are obliged to hand over their customers' data, and if they refuse, they may get shut down. In most cases these companies are prevented by law from disclosing that they have received such data access requests.

4.3 Adopted Measures

To integrate human rights into business practices, two important instruments will be examined: the UN Guiding Principles on Business and Human Rights and the General Data Protection Declaration (GDPR).

The importance of the UN Guiding Principles on Business and Human Rights in ensuring that companies are not complicit in human rights abuses was underscored. The Guiding Principles contain standards for businesses to adhere to ensure their activities do not have a negative impact on human rights. So, they should develop policies and constantly monitor their activities to ensure they are meeting these standards. Ensuring that a business respects the Guiding Principles where there is no legislative oversight is a major challenge. It was noted that States have a duty to protect those within their jurisdiction from human rights abuses by private actors, so, long as this does not place an undue burden on the State. Included within this positive obligation is the duty to enact legislation regulating the conduct of business with regard to the right to privacy online. Companies are responsible not to put their employees in a situation where they would be acting illegally.

As for the General Data Protection Declaration (GDPR), it is an important component of EU privacy law and of human rights law. The right to data protection also reflects the right to respect for private life in Article 8 of the ECHR which is different from article 8 (1) of the Charter of Fundamental Rights of European Union. The latter provides:

"*1-Everyone has the right to the protection of personal data concerning him or her.*

2-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.

3-Compliance with these rules shall be subject to control by an independent authority"

It aims to enhance the control of individuals on rights over their personal data and to regulate international business. It is one of the first legal acts to firmly introduce the notion that digital rights need to be integrated into the business operations and strategies of companies.[3] By having strong data protection laws and appropriate safeguards, businesses will be able to operate across international borders. Indeed, the GDPR tends to regulate the activities of Facebook, Google, and consorts on the European scene but also on the international scene. This text is based on the protection of privacy and personal data. To prepare the site for the entry into force of the GDPR, a team of lawyers and experts was requisitioned in Dublin at the platform's European headquarters.

[1] Ibid.
[2] Les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme sont un particulièrement bon exemple de cette démarche. Pour de plus amples explications, voir Kälin et Künzli, Menschenrechtsschutz, 2019, p. 91 ss.
[3] Adriana Minovic', "GDPR: Integrating human rights into business practices", https://www.diplomacy.edu/blog/gdpr-integrating- human-rights-business-practices/ 13 November 2017

Voted on 27 April 2016, the General Regulation on the Protection of Personal Data, known as the GDPR, entered into force on 25 May 2018 and repealed the former European Directive 95/46/EC [30] and a large part of Law No. 78-17 of 6 January 1978 on data processing, to files and freedoms. Some see this as a huge step forward. Rules protecting the integrity of users' identities and privacy breaches are strengthened. For more efficiency, the GDPR is in line with the European directive but presents many changes.[1] The free movement of personal data must be ensured to strengthen the effectiveness of data protection law and the digital single market.

The important aspect of the GDPR is the penalties imposed on violators of data protection laws.[2] The main concern of many companies operating in the European Union was non-compliance with competition law and other areas of trade and internal market relations, due to severe sanctions. The most severe sanction is the well known one of 10% on worldwide turnover for undertakings in breach of EU competition law. It indicates the importance of competition law for the EU and its member States.[3]

The GDPR introduces similar sanctions, which are not so common in the field of human rights. The maximum fine of €20 million, or 4% of the company's total annual turnover, for non-compliance with certain provisions of the GDPR, underlines the importance that the EU also attaches to data protection. In addition, the fact that the EU has opted for a regulation on privacy and data protection (which is directly applicable to Member States) puts more emphasis on human rights and related business.[4]

5.Conclusion

Digital technologies represent a double-edge weapon: it can jeopardize the right to privacy as a fundamental human right, but sometimes it is beneficial to human right's protection. States should review their domestic laws and adopt the necessary legislations that both protects the right to privacy, including internet and telecommunications, and regulates communications surveillance by law enforcement. Those legislations must include anonymity protection for internet and telecommunications. State should also enact data protection law.

Governments representative, human rights lawyers, computers scientists and engineers should adopt legal framework to protect individuals against intrusions by other individuals' companies, and work together "*ensure the continued application of human rights in the way in which States operate in the digital age, and in the way in which they regulate the activities of companies in the digital space*".[5] Digital technologies are not isolated from the general context. They can also be a powerful tool for advancing human progress and contribute greatly to the promotion and protection of human rights.

These technologies can be very beneficial also to protect human rights, particularly in data collection and analysis. By enabling modeling and prediction, new technologies such as artificial intelligence and algorithmic decision - making can help improve public service provision, with positive implications for, inter alia, the right to health and the right to an adequate standard of living[6]

These technologies can also protect human rights in the digital age. Indeed, social media and smartphones allied with big data collection and analysis can constitute a powerful tool for monitoring and reporting human rights violations, including in situations of armed conflict, with important benefits for justice and accountability.[7]

[1] Nadir Ouchene,'La Vie Privee sur Internet', 13 en Droit,Revue de Droit de la Faculte de Droit, science politique et sociales de l'Universite Paris 13. No 3. Juin 2019.
[2] The Court of Justice of the European Union (CJEU) recognized that the right to protection of personal information was a general principle of EU law as early as 1969 in the case of Stauder (Case C- 29/69).
[3] Ibid.
[4] Ibid.
[5] Michelle Bachelet, UN High Commissioner for Human Rights, November 2018
[6] https://www.ohchr.org/en/statements/2020/12/glion-human-rights-dialogue-2020-glion-viihuman-rights-digital-age-making
[7] Ibid.

References

Books

1.Sabrina Ghielmini, Christine Kaufmann, Charlotte Post, Tina Büchler, Mara Wehrli et Michèle Amacker, « Droits fondamentaux et droits humains à l'ère numérique », © 2021 – CC-BY-NC-ND (ouvrage), CC-BY-SA (texte) Éditeur : Centre suisse de compétence pour les droits humains (CSDH).
2.Ryan Gallagher, "After Snowden Leaks" Countries Want Digital Privacy Enshrined in Human Rights Treaty", Slate (26 September 2013).
3. D Mc Goldrich, "The Human Rights Committee: Its Role in the Development of the International Covenant on Civil and Political Rights", Oxford: Clarendon Press, 1991.

4. Alan Westin, " Privacy and freedom" , Atheneum, New York 1967.
5. Cavoukian, A. and Tapscott, D., "Who Knows: Safeguarding Your Privacy in a Networked World", McGraw Hill, New York, 1997.
6.Newell, P. B.," Perspectives on Privacy", Journal of Environment.
7.Milton Mueller, et al. "The Internet and Global Governance: Principles and Norms of a New Regime", (2007) 13 Global Governance.

Articles

1.Nadir Ouchene,'La Vie Privee sur Internet', 13 en Droit,Revue de Droit de la Faculte de Droit, science politique et sociales de l'Universite Paris 13. No 3. Juin 2019.
2.Stefano Rodota, "Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives ». La Découvertes, « Mouvements » 2010/2 n0 62 pages 55 à 70.
3.Maura Conway, "Le Terrorisme et la Gouvernance de l'Internet »,Revue de l'Information et la Sécurité Internationale, 2007.
4.Eliza Watt, "The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance", 2017 9th International Conference on Cyber Conflict. Defending the Core. 2017 NATO CCD COE Publications, Talinn.
5.Lee A Bygrave, "Data Protection to the Right to Privacy in Human Rights Treaties", International Journal of Law and Information Technology, 1998, vol 6, pp. 247-284.
6.Stefano Rodota, Nouvelles Technologies et Droits de l'Homme : Faits, Interprétations, Perspectives », La Découvertes, « Mouvements » 2010/2 n0 62
Psychology, vol. 15, ed 2, 1995.
7.Mellissa E. Hathaway, « Connected Choices: How the internet is challenging sovereign dimensions", American Foreign Policy Vol 36. No 2014/5, p. 310.
Council of Europe Commissioner for Human Rights, "The Rule of Law on the Internet and in the Wider Digital World", (2014), 36.

Websites

1.Adriana Minovic', "GDPR: Integrating human rights into business practices", https://www.diplomacy.edu/blog/gdpr-integrating- human-rights-business-practices/ 13 November 2017

2.Michelle Bachelet, UN High Commissioner for Human Rights, November 2018
https://www.ohchr.org/en/statements/2020/12/glion-human-rights-dialogue-2020-glion-viihuman-rights-digital-age-making

3.LE MONDE, Cambridge Analytica : 87 millions de comptes Facebook concernés. Disponible à cette adresse : http://www.lemonde.fr/pixels/article/2018/04/04/cambridge-analytica-87-millions-de-comptesfacebook-concernes_5280752_4408996.html, [consulté le 16 avril 2018].

4.LE PARISIEN, Facebook : ce qu'il faut retenir du mea culpa de Mark Zuckerberg devant le Congrès, 10 avril 2018. Disponible à cette adresse : http://www.leparisien.fr/high-tech/facebook-ce-qu-il-faut-retenir-du-mea-culpa-de-mark-zuckerberg-devant-le-congres-10-04-2018-7657422. php, [consulté le 8 mai 2018].

5.DUNAWAY J., Sen. Dick Durbin Proves Mark Zuckerberg Is As Awkward As the Rest of Us, 10 avril 2018. Disponible à cette adresse : https://slate.com/technology/2018/04/dick-durbins-questionat-the-senate-congressional-hearing.html, [consulté le 8 mai 2018].

6.https://www.osano.com/articles/alan-westin#:~:text=In%20%E2%80%9CPrivacy%20and%20Freedom%2C",was%20revolutionary%20in%20its%20approach

7.https://www.ohchr.org/en/statements/2020/12/glion-human-rights-dialogue-2020-glion-viihuman-rights-digital-age-making