THE RIGHT TO PRIVACY IN INTERNATIONAL HUMAN RIGHTS LAW

Özgür H. ÇINAR [1*]

ABSTRACT

Everyone has the right to demand respect for their privacy (private life). Hence, this right has been safeguarded in international law. However, in the digital age the boundaries of privacy have widened. Both state bodies and non-state organisations make frequent interventions. In fact, these interventions have to be carried out in line with legislation, with the permission of the authorities and in a proportional manner. In this article the historical origins, definition and scope of this right will be examined. Examples from domestic law will be presented and the approach of international bodies such as the United Nations, European Court of Human Rights and European Union mechanisms such as the Court of Justice of the European Union will be examined in detail.

KEY WORDS: *Right to privacy, private life, personal data, international human rights law, European Court of Human Rights, United Nations, European Union.*

1. INTRODUCTION

From the earliest times human beings, as a social entity have shared public spaces with other human beings, while also having a personal and private life. What is mean by the term private life is the right to privacy. Private life is the term used to define the space which people allot to themselves and into which they allow the persons they want. Private life in fact protects us against arbitrary and unjustified interventions by states and other non-state actors. The control of this space is in the hands of the individual who does not want others to intervene. [1] Human dignity lies at the root of this right, and constitutes the basis of all other human rights. What is important here is to improve a person's rights and their conditions of life, so that they may achieve their personal aims and ambitions. Within the broad scope of this right are things such as physical space, home, family life and correspondence. Hence, this sphere has been safeguarded by international law and by the laws of many countries.

Private life is a fundamental right that should be respected by everyone (state and non-state actors) everywhere. This right received recognition in international law after the Second World War. However, it is necessary to be aware that due to the complexity of this right it is linked to different areas of law, for instance: property rights, health, insurance and financial law.

[1]* corresponding author, Dr. Senior Lecturer, University of Greenwich, School of Law and Criminology, ozgurhevalcinar@gmail.com

However, with technological progress in the 21st century serious restrictions on people's private life are being talked about. For instance, our movements can be monitored through the smartphones or computers we use. Data can also be gathered on individuals from search engines, social media, internet searchers and credit cards. This monitoring is in general carried out by states on security grounds.

In this article, in addition to looking briefly at the historical origins of private life, a close examination will be made of its definition and scope. Additionally, how this right is defined in national and international law will be explored and answers sought to the following questions: In private life how can the delicate balance between the gathering of personal data and security be ensured? What is meant by personal data? In what circumstances may this freedom be restricted?

2. HISTORY, DEFINITION AND SCOPE OF THE RIGHT TO PRIVACY

In fact we even come across the origins of this right in primitive communities. Where there were no dividing walls or screens abstract private areas were created by 'imaginary walls'. For instance, in the northeast of Peru the Yagua people who live in houses without dividing walls or screens will turn to the wall of the house when they want to establish a private space. When they do this they are in fact saying that they do not exist in that area. From the 5th century onwards, with the fall of the Western Roman Empire and the coming to power of tribes, people began to live in more protected houses, and privacy gained importance once again. In this context the inviolability of domicile and right to privacy were partially protected. For example, in 1361 the 'Justices of the Peace Act' foresaw the arrest of those who secretly listened in to or followed others. [2] With industrialisation in the 16th century and increasing urbanisation mechanisms were developed to protect privacy with the press having an influence. In 1710 the opening of letters in England without the permission of official authorities was prohibited. In the United States of America there were debates over respect for private life in the 19th century. International debate on this topic came about after the Second World War. Technological developments in the 21st century have made it apparent that this right needs to be protected in a more serious way. [3]

As regards the definition of private life in the literature there are serious difficulties as to its meaning and uncertainty in determining its boundaries. For instance, Arthur Miller said it was hard to define because of a tiresome vagueness and its tendency to disappear. [4] As for Julie C. Innes, she said: "we turn to the legal and philosophical literature on privacy in the hope of gaining a foothold." [5] Unfortunately, the definition of private life has not been completely outlined in international documents. For instance, in article 8 of the European Convention on Human Rights ('ECHR' and/or 'the Convention') we see there is no definition of private life. In *Niemietz v. Germany* the European Court of Human Rights (ECtHR) stated that a definition of private life was neither possible nor necessary: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings…" [6] The Court maintained the same

stance in *Costello-Roberts v. the United Kingdom*, making reference to *Niemietz v. Germany*, reiterating that the concept of private life was not entirely suitable to be defined. [7]

However, the impossibility of a definition does not imply that this right does not exist or is unimportant. The existence of this right is important for human dignity, freedom and democracy. Hence, this right, which is necessary in a democratic society for a person's creativeness and to ensure we can establish and maintain social relations with others and also to safeguard an autonomous life and physical tranquillity, has been described as the heart of all essential freedoms. [8] According to a report written by the Special Rapporteur to the Human Rights Council in 2016:

> Recognizing that the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association…[9]

It is apparent how this right has been violated by state and non-state actors, particularly now with the advances made in technology. According to the United Nations (UN) Special Rapporteur in 2016 one in ten of citizens in all member states suffered human rights violations relating to their personal data. [10]

3. RIGHT TO PRIVACY IN NATIONAL LAWS

It has been pointed out that in more than 33% of UN countries, that is, more than 70 states, there is no law pertaining to private life. In more than 75% of member states there are no safeguards or remedies relating to this right of citizens not being violated by other states. [11] But in more than 120 countries this right is safeguarded by national laws. [12] Efforts are also being made in many countries to provide Data Protection Authorities (DPAs) or Regulators to protect personal data.

For instance, it has been safeguarded by the 4th Amendment of the American Constitution: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." [13]

In the German Constitution although the right to privacy is not openly expressed, it is evaluated within the framework of article 1(1) relating to human dignity and article 2(1) concerning freedom of personality. In the Chinese Constitution, although the right to privacy is not mentioned, this right is associated with the physical rights mentioned in article 37, human dignity referred to in article 38 and public spaces in article 39. [14]

In the South African Constitution this right is clearly set down in article 14: "everyone has a right to privacy which includes a right not to have one's home, person or property searched, possessions seized and privacy of communications infringed." Article 5 of the Brazilian Constitution states: "personal intimacy, private life, honour and reputation are

inviolable"; Article 10 of the Finnish Constitution states: "Everyone's private life, honour and the sanctity of the home are guaranteed." Article 20 of the Georgian Constitution states: "Everyone's private life … shall be inviolable"; article 20 of the Turkish Constitution states: "Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated. [15] Article 26 of the Romanian Constitution states: "The public authorities shall respect and protect the intimate, family and private life…" [16]

Although in the Constitutions of Canada, the United Kingdom, France, Japan and Indian this right is not mentioned, this freedom has been tacitly accepted as a constitutional right by means of court judgments. For instance, the Indian Supreme Court in 2017 made the following judgment: "Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination." [17] The protection of private life has also been guaranteed by law in these countries. For example, in Canada a law on 'the Protection of Personal Information and Electronic Documentation' was enacted in 2000. A similar law was passed in Japan in 2003. [18] This right was safeguarded in the UK by article 8 of the Human Rights Act of 1998, the Wireless Telegraphy Act of 1949, the Copyright Act of 1956, the British Telecommunications Act of 1981 and the Data Protection Act of 1984. [19]

4. RIGHT TO PRIVACY IN INTERNATIONAL HUMAN RIGHTS LAW

This right is also safeguarded in international law. For instance, article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 8 of the European Convention on Human Rights, articles 7 and 8 of the European Union (EU) Charter of Fundamental Rights, article 5 of the American Declaration of the Rights and Duties of Man and article 11 of the American Convention on Human Rights are the main international provisions of the right to privacy. All these articles answer the question as to why privacy needs to be safeguarded. However, there are no answers as regards when, how and by whom this freedom should be protected. [20] We see the answers to these questions in examples of case law or in resolutions passed on this issue.

4.1. UN Human Rights System

The UN General Assembly passed two important resolutions in 2013 and 2014 calling on member states to respect the right to privacy in their laws and policies in digital communications, and to take the necessary steps to ensure this (Resolution 68/167, December 2013; Resolution A/C.3/69/L.26/Rev.1, November 2014). In 2015 the UN Human Rights Council appointed a Special Rapporteur on the Right to Privacy. This Special Rapporteur was asked in particular to make expert analysis on a human rights law perspective and give guidance as regards the right to privacy in the face of new technological challenges. Hence, in a report published on 1 March 2019 was the following: "As I have emphasised in the past, there is much work to be done to protect the right to privacy, and a defensive posture is not sufficient. We, Member States and institutions of the United Nations, need to actively entrench privacy as a standard in a democratic society." [21]

4.2. European Human Rights System

There are two important mechanisms in Europe. The first of these is the Council of Europe, while the second is the EU. The ECHR and the ECtHR will be examined under the heading of the Council of Europe. Under the EU heading the Global Data Protection Regulation (GDPR) and decisions of the Court of Justice of the EU (CJEU) will be examined.

4.2.1. European Convention on Human Rights

Article 8 of the ECHR states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. 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.

As can be seen in this paragraph, this freedom also protects family life, the home and the confidentiality of correspondence in addition to individual private life. However, this is not a correct approach to only identify article 8 with the concept of private life. Personal identification, honour and reputation, personal data, physical and moral integrity and sexual life are also included in the concept of private life in judgments made by the ECtHR. As for a person's identity, this includes the name, gender identification, ethnic identity and lifestyle and image. We will look closely in particular at the principle of the confidentiality of personal data within the scope of the above. States have the negative obligation to prevent all manner of arbitrary interference in this freedom. States also have positive obligations to ensure that private parties behave in a respectful manner towards each other. [22]

In addition to the positive and negative obligations of states, since this article is a "qualified right" the state or public authorities are legally entitled to interfere with this freedom in certain limited situations. There are three stage test that must be applied for this freedom to be restricted: 1-) Any interference by the state must be in accordance with law; 2-) It must satisfy one of the legitimate aims stated in Article 8(2); 3-) It must be necessary in a democratic society. This last point is very important as the ECtHR's judges the concept of necessary according to whether there is 'pressing social need'. On this point national authorities have a margin of appreciation as regards determining whether there is 'pressing social need'. [23]

4.2.2. European Court of Human Rights' Case Law

The protection of personal data is related to the right to privacy. The Court evaluates the gathering of data on a person's private life and the holding and use of this data within the scope of Article 8. The Court stated in *S. and Marper v. the United Kingdom* that the gathering and holding of personal data, even if it is not used, constitutes a violation of Article 8. [24] The Court also takes into consideration the nature of the information gathered and held, the way it is used and possible consequences. Hence, the Court ruled in *Klass and others v. Germany* that states could not use the grounds of espionage and counter terrorism to monitor individuals as they wish. [25] It was emphasised that

interference with the rights of individuals should be subject to 'an effective control' and that attention should be paid to the principle of proportionality. [26]

The Court constantly refers to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in its judgments. Article 2 of this Convention defines the concept of personal data thus: "any information relating to an identified or identifiable individual…"

The Court also frequently makes reference to Article 6 of this Convention: "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions." In accordance with this article personal data is separated into two: specific data and other data.

Specific data concerns data such as 'racial origin', 'political opinions or religious or other beliefs', 'health or sexual life' or 'criminal convictions' as referred to in Article 6. However, the problem here relates to other data that is not mentioned in the article, but which may indicate a person's identity or be sufficient to do so. In this regard the source that need to be referred to be the jurisprudence of the ECtHR. In the Court judgments a person's profile, photographs, fingerprints, DNA profile, cell samples, information regarding health, voice, security number, home address and personal spending are all within the scope of personal data. [27] The Court also differentiates between data as to whether it is of a personal or public nature. For instance, while a person's picture is of a personal nature, their political activities are of a public nature.

The Court points out that a person's photographs distinguish them from others on account of their unique character. For this reason they are important as regards a person's personal development. This matter is particularly relevant in the case of a well-known person's photographs being publicly shared, leading to a complicated situation. For it is necessary to strike a balance between a person's reputation, as safeguarded by Article 8, with Article 10 that protects freedom of expression. On this point the Court asks the following questions: "how well known is the person concerned and what is the subject of the report?; prior conduct of the person concerned; content, form and consequences of the publication; circumstances in which the photos were taken; and severity of the sanction imposed." [28]

Particularly at the present time we frequently see our personal information used on search engines such as Google. This is an interesting example of conflict between Article 8 and Article 10, for while our personal information is on the internet, on the other hand there is the public's right to information. The case of *M.L. and W.W. v. Germany*was the first case to deal with the issue of press archives on the internet featuring previously reported news (para. 90 and para. 102). In this case the Court rejected the applicants' request for media organisations to be obliged to anonymise on-line archive material relating to their criminal trial and conviction (para. 116). In its judgment the Court stressed that Article 10 of the ECHR protects media archives, and public access to them. Nevertheless, the judgment did confirm the validity of the right to be forgotten enshrined in Article 8 being used against primary publishers in addition to search engines. Hence, it is important to distinguish this case from others in which individuals exercise their data protection rights as regards their personal information which is published on the internet and which may be

obtained through search engines (para. 91) and used for profiling purposes by third parties (para. 97). [29]

On 27 June 2017 the Grand Chamber of the Court found that in the case of *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* there had been no violation of the right to freedom of expression and information. [30] The case in question involved the mass collection, processing and publication of personal taxation data publicly available in Finland. The Court found there had been no violation of Article 10 based on a narrow interpretation of (public interest) journalism and a wide margin of appreciation for the domestic authorities finding. [31]

The Court found that the data that had been collected and published by newspapers, giving details of the tax affairs of many people, evidently related to their private lives, despite the fact that the general public was able to access the data, under domestic law, with certain limitations (para. 138). In such matters domestic law has to provide proper safeguards to prevent the use of personal data that could conflict with the guarantees enshrined in Article 8. It is worthy of note that the Court emphasised that Article 8 provided for the right to a form of self-determination as regards information, in that it permitted individuals to rely on their right to privacy concerning data collected, processed and disseminated en masse and in a way that the Article 8 rights of the individuals in question are ensured (para. 137, see also para. 198).

Additionally, personal information is not only monitored by means of the internet, as our movements can also be monitored in public spaces by CCTV or different technological equipment. At this juncture the question as to what will happen to footage taken by video surveillance of public places comes to mind. The Court primarily evaluates this situation within the scope of Article 8. [32] For instance, in this case a violation of Article 8 was found on account of video footage of the suicide of the applicant being shared without permission in the media. [33] In the same way, it was stated that the sharing of photographs taken of persons in custody by the police or public authorities without permission constitutes a violation of Article 8. [34] However, the sharing of photographs of a suspected terrorist was not found to be in violation of Article 8 as in this instance a state's margin of appreciation was interpreted more broadly. [35]

Moreover, the monitoring by states of communications is one of the most controversial issues of modern times. Although national governments and national authorities are granted a certain margin of appreciation when it comes to assessing the best policy in this sphere, States must carry out unlimited covert surveillance of persons within their jurisdiction. The Court has made clear that States may not use whatever measures they consider legitimate on the pretext of combatting espionage and terrorism; instead, there must be adequate and effective measures adopted to prevent abuse under whatever system of surveillance is utilised. [36] Covert surveillance of citizens is only tolerable when it is absolutely necessary to safeguard democratic institutions. [37] All such measures must be based on concrete and sufficient grounds and be proportionate to the legitimate purpose set forth. [38]

The Court has also included the collection of DNA samples within the scope of the right to privacy. The gathering and holding of cellular material, and the determination and retention of DNA profiles extracted from this material, was found to be an interference with the right to respect for privacy enshrined in Article 8 para. 1 of the ECHR. [39] This

ban does not necessarily include the taking and holding of DNA profiles of convicted criminals for future use in criminal proceedings that may arise. [40] As referred to above, such interference is a violation of Article 8 unless it is considered to be 'in accordance with the law', and can be justified under paragraph 2 of Article 8 as trying to achieve one of the legitimate aims listed, and as being 'necessary in a democratic society' in order to achieve the aim or aims in question. [41]

In summary, the ECtHR, by broadening the scope of Article 8, is making clear that this freedom is not unlimited. However, bearing in mind the negative and positive obligations of states as regards restricting this right, it is necessary to carefully implement the three stage test we mentioned above. Otherwise, there will be a risk of violating the principle of proportionality and consequently violating Article 8.

4.3. European Union Legal System

Apart from the ECtHR, another important mechanism in Europe is the EU. Article 7 of the EU Charter was constructed on Article 8(1) of the ECHR: "Everyone has the right to respect for his or her private and family life, home and communications." However, Article 8 of the Charter for the first time included 'personal data' for the first time in international documents, guaranteeing it protection:

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.

The EU Charter is not a statement of fundamental rights and privileges with a universal scope. Article 51 of the Charter states that it only applies to EU institutions and Member States when they are engaged in the implementation of EU Law. Thus, the Charter has an aim to guide the implementation and interpretation of EU Law, including the GDPR. [42]

In *Digital Rights Ireland* and *Seitlinger and Others* the CJEU stated: 'The retention of data for the purpose of possible access to them by the competent national authorities, as provided for by Directive 2006/24, directly and specifically affects private life and, consequently, the rights guaranteed by Art. 7 of the Charter.' [43] The CJEU found that holding private data violated Art. 7 of the Charter, and that national authorities having access to such data constituted a 'further interference with that fundamental right', referring to ECtHR case law. [44]

The CJEU held in *Google v Spain* that Google is responsible for the processing of the personal data in which it engages, as a data controller established in the EU, and is responsible for this data which appears on web pages published by third parties. Hence, Google has a responsibility to respect EU data protection laws (Arts 7 and 8 of the Charter) and also to comply with requests to remove links to certain personal data, under certain circumstances (the right to be forgotten). [45] In *A, B, C v Staatssecretaris van Veiligheid en Justitie* the national court asked the CJEU whether EU law imposed any restrictions as regards the verification of the sexual orientation of asylum applicants. According to the CJEU, Member States have the right to examine the truth of applicants'

statements regarding his/her sexual orientation. [46] However, the methods used to evaluate the credibility of these statements by national authorities must respect the right to respect for private and family life and other *fundamental rights*. [47]

In summary, the CJEU hands down similar judgments to the ECtHR. However, the EU has gone one step further by accepting the Global Data Protection Regulation (GDPR) 2016/679 and the Data Protection Directive for law enforcement and police area in April 2016. At this time the GDPR is the broadest provision in the world concerning data protection in the digital era. [48]

Article 1 of the GDPR is as follows: "[Regulation] protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data." The Impact Assessment of the European Commission noted that, "individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively." [49] Hence, the GDPR emphasises autonomy and consent while also attaching equal importance to the duties of data controllers, without seeing whether data subjects have acted to enforce those duties. [50]

The EU also established a body called the European Data Protection Supervisor (EDPS) to deal with data protection in 2004. The role of the EDPS is one of independent adviser to EU institutions concerning all matters relating to the processing of personal data, including security initiatives and new data-exchange tools for law enforcement agencies. The EDPS has published many Opinions on initiatives designed to broaden information-sharing for the purpose of law enforcement inside the EU, including the Entry/Exit System and EU PNR - and also beyond Europe, examples being the Umbrella Agreement with the US and PNR agreements with non-EU countries. [51]

In summary, EU rules on the right to privacy in particular present the greatest source for us, as it has provided a very strong mechanism to protect personal data. The GDPR is not only implemented in organisations or institutions founded in the EU, but also in bodies founded outside the EU that are legal entities within the EU. In addition to providing new rights to individuals in the digital environment, new detailed obligations have been introduced for companies and organisations. In this regard it is important not to overlook the fact that the EDPS and CJEU have effective mechanisms.

5. CONCLUSION

It is impossible to define the concept of private life and to set forth exactly what it is. Within this freedom there is not only private life, but also freedom of ideas, expression, religion and conscience in social life. Although it is exceedingly difficult to define the concept of private life and draw its boundaries, this does not mean this right does not exist. This right is one of the most fundamental human rights and is important in the safeguarding of human dignity and autonomy. This right is the right of a person to live their private life without unwanted intrusion. Hence, this freedom protects us against arbitrary and unjustified interference by both state and non-state actors. In this context it is part of a state's negative and positive obligations to develop and implement effective mechanisms to protect this freedom of individuals. These obligations have been clearly set down both in international law and in the domestic law of many countries.

Of course, this right is not unlimited. However, interference in this right must be based on legal grounds and have permission and in accordance with the principle of proportionality. It can be particularly difficult to determine boundaries in the digital world. For this reason UN, ECtHR and EU mechanisms have introduced provisions (e.g. GDPR) recently in order to ensure that people do not suffer arbitrary and unjustified interference in this right. However, when we consider that more than 70 UN member states have still no legal provisions safeguarding this right, it is important that both these countries and international bodies take action as soon as possible.

REFERENCES

[1] Korkmaz, Ali (2014). "Insan Haklari Baglaminda Ozel Hayatin Gizliligi ve Korunmasi" [Right to Privacy and Its Protection in the Context of Human Rights]. KMU Sosyal ve Ekonomik Arastirmalar Dergisi 16, p. 99.

[2] Fejos, Pal (1943). "Ethonology of the Yagua". New York; Moore, Barrington (1984). "Privacy: Studies in Social and Cultural History", New York; Salihpasaoglu, Yasar (2013). "Ozel Hayatin Kapsami: Avrupa Insan Haklari Mahkemesi Ictihatlari Isiginda Bir Degerlendirme" [The Scope of Right to Privacy: An Evaluation in light of European Court of Human Rights' Case Law]. Gazi Universitesi Hukuk Fakultesi Dergisi XVII, pp. 228-229.

[3] Akyurek, Guclu (2011). "Ozel Hayatin Gizliligini Ihlal Suclari, Cesitli Hukuk Dallarinda Ozel Hayatin Gizliliginin Korunmasi" [A Violation of Right to Privacy, The Protection of Right to Privacy in Various Law Branches], Seckin Publication House, pp. 105-108; Korkmaz, p. 100.

[4] Miller, Arthur (1971). "Assault on Privacy: Computers, Data Banks and Dossiers". The University of Michigan Press; Salihpasaoglu, p. 234.

[5] Innes, Julie C. (1992). "Privacy, Intimacy and Isolation". Oxford University Press, p. 3; Salihpasaoglu, p. 234.

[6] Niemietz v. Germany, 13710/88, 16.12.1992, para. 29.

[7] Costello-Roberts v. the United Kingdom, 13134/87, 25.03.1993, para. 36.

[8] Salihpasaoglu, pp. 235-236.

[9] Human Rights Council Resolution, A/HRC/RES/34/7.

[10] Human Rights Council (2018). "Report of the Special Rapporteur on the right to privacy". A/HRC/37/62, p. 14.

[11] Ibid., p. 27.

[12] Privacy International (2015). "The Right to Privacy and Why It Matters". Available online: https://rightsinfo.org/the-right-to-privacy-and-why-it-matters/, Accessed on March 28, 2019.

[13] Cornell, Anna Jonsson. "Oxford Constitutional Law: Right to Privacy". Available online: http://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156, Accessed on March 28, 2019.

[14] Ibid, pp. 5-6.

[15] Salihpasaoglu, p. 231.

[16] In Romania the right to privacy is also safeguarded by the "Personal Data Law"no. 677/2001.

[17] See http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf in the "Report of the Special Rapporteur on the right to privacy", p. 7.

[18] Solove, Daniel J. (2008). "Understanding Privacy". Harvard University Press; Salihpasaoglu, pp. 232.

[19] Sen, Ersan (1990), "Anglo Sakson Hukukunda Ozel Hayatin Gizliligi ve Korunmas Hakki" [Right to Privacy and its Protection in the Anglo-Saxon Law]. Istanbul Universitesi Mukayeseli Hukuk Arastirmalari Dergisi 18, p. 85.

[20] See Korkmaz, p. 102.

[21] "Report of the Special Rapporteur on the right to privacy", p. 2.

[22] Council of Europe (2018). "Guide on Article 8 of the European Convention on Human Rights". Council of Europe: Strasbourg, p. 8.

[23] Ibid, p. 11.

[24] S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, ECHR 2008.

[25] Klass and others v. Germany, Series A no. 28, 06.09.1978.

[26] Salihpasaoglu, footnotes 104, 116, 117, 120.

[27] Ibid, p. 245.

[28] Council of Europe, p. 30.

[29] M.L. and W.W. v. Germany, 60798/10 and 65599/10, 28.01.2018.

[30] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, 931/13, 27.06.2017.

[31] Voorhoof, Dirk (2017). "No journalism exception for massive exposure of personal taxation data". Available online: https://strasbourgobservers.com/2017/07/05/no-journalism-exception-for-massive-exposure-of-personal-taxation-data/#more-3801, Accessed on March 28, 2019.

[32] Peck v the United Kingdom, 44647/98, 28.01.2003, para. 57-63.

[33] Ibid, para. 87.

[34] Council of Europe, p. 30.

[35] Murray v. the United Kingdom, 14310/88, 28.10.1994, para. 93; Segerstedt-Wiberg and others v. Sweden, 62332/00, 06.09.2006, para. 88).

[36] Weber and Saravia v. Germany, 54934/00, 29.06.2006, para. 49-50.

[37] Weber and Saravia v. Germany, para. 42; Rotaru v. Romania [GC], 28341/95, 04.05.2000, para. 47; Weber and Saravia v. Germany, para. 78.

[38] Segerstedt-Wiberg and Others v. Sweden, para. 88.

[39] S. and Marper v. the United Kingdom [GC], 30562/04 and 30566/04, 04.12.2008, para. 71-77; Van der Velden v. the Netherlands (dec.), no. 29514/05, ECHR 2006-XV; W. v. the Netherlands (dec.), no. 20689/08, 20.01.2009.

[40] Peruzzo and Martens v. Germany (dec.), nos. 7841/08 and 57900/12, 04.06.2013, paras. 42 and 49.

[41] Ibid.

[42] Mosterst, Menno (2017). "From Privacy to Data Protection in the EU: Implications for Big Data Health Research". European Journal of Health Law 24, pp. 4-5.

[43] Digital Rights Ireland and Seitlinger and Others, Case C-293/12, Case C-594/12, [2014] OJ C175/6, ECLI:EU:C:2014:238, 08.04.2014.

[44] Cornell, Anna Jonsson. "Oxford Constitutional Law: Right to Privacy". Available online: http://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156, Accessed on March 28, 2019, p. 6.

[45] Google Spain, Google Spain SL and Google Incorporated v Agencia Española de Protección de Datos ('AEPD') and Costeja González, Case C-131/12, ECLI:EU:C:2014:317, ILEC 060 (CJEU 2014), 13.05.2014.

[46] A and ors v Staatssecretaris van Veiligheid en Justitie, Case C 148/13, Case C 149/13, Case C 150/13, ECLI:EU:C:2014:2406, [2015] OJ C46/4, 02.12.2014.

[47] Cornell, Anna Jonsson. "Oxford Constitutional Law: Right to Privacy".

[48] European Data Protection Supervisor "Data Protection". Available online: https://edps.europa.eu/data-protection/data-protection_en, Accessed on March 28, 2019.

[49] European Commission (2012). "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)". Available online: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011, Accessed on March 28, 2019.

[50] McDermott, Yvonne (2017). "Conceptualising the right to data protection in an era of Big Data". Big Data & Society, Available online: https://journals.sagepub.com/doi/full/10.1177/2053951716686994, Accessed on March 28, 2019; Quelle, Claudia (2011). "Not just user control in the General Data Protection Regulation. On controller responsibility and how to evaluate its suitability to achieve fundamental rights protection". Available online: https://pdfs.semanticscholar.org/2eeb/f1efca870fc524b381010c97712f98e89419.pdf, Accessed March 28, 2019.

[51] European Data Protection Supervisor "Data Protection".