DOI 10.5817/MUJLT2022-1-2

THE RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA: EMERGING TRENDS AND IMPLICATIONS FOR DEVELOPMENT IN JURISPRUDENCE OF EUROPEAN COURT OF HUMAN RIGHTS

by

YULIIA KOVALENKO*

The emergence of the right to personal data protection is usually considered in close proximity to the right to private life, however, the two rights despite the sufficient degree of similarity are not identical. The article analyses the main concepts and discussions around the protection of privacy and personal data protection, which primarily was only perceived as another facet of privacy, as well as provides a comprehensive overview of theoretical and practical problems associated with their protection. Provided for the right to data protection is not explicitly mentioned in the ECHR the main concern, therefore, is whether it receives an adequate level of protection within the Convention system. The article argues that given the lack of an explicit criterion for distinguishing the rights to privacy and data protection, it is the jurisprudence of the ECHR, which is of the utmost importance for the development of the right to personal data protection as a fundamental right. Due regard is given to the evolution of the fundamental approaches of the ECHR in this field. It is concluded that the effective enjoyment of the right to data protection, which is not specified in the text of the ECHR or its Protocols, undeniably relies on the ECHR's interpretation of the key data protection standards enlisted in the Convention no. 108, as well as relevant EU legislation.

* yuliiakovalenko108@gmail.com, PhD student of International and Comparative Law Department, Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Kyiv, Ukraine.

KEY WORDS
Privacy, Data protection, The right to private life, The right to personal data protection, ECHR.

1. INTRODUCTION

For a long time, personal data protection has only been considered as an aspect of the right to respect for private life, which is inextricably linked to the protection of other fundamental human rights and freedoms. However, the issue of data protection has drastically gained its importance with the unrestrained development of information technology. Accordingly, the question of determining the right to personal data protection and the standards of its protection becomes a modern challenge.

Since the middle of the XX century, the number of international human rights treaties enshrined the right to respect for private life as one of the fundamental human rights. First and foremost, the right to respect for private life was enshrined in Article 12 of the Universal Declaration of Human Rights of 1948, which set forth the list of fundamental human rights and is considered to be a 'milestone document', but yet is not legally binding. The rights incorporated in the Universal Declaration of Human Rights were further detailed in international treaties and other human rights instruments. The International Covenant on Civil and Political Rights of 1966 provided for the right to private life in Article 17 and the UN Human Rights Committee has been established to oversee its fulfilment and adherence. Furthermore, the right to respect for private life was guaranteed under Article 8 of the European Convention on Human Rights and Fundamental Freedoms of 1950 (hereinafter – the ECHR or the Convention).[1] Despite the fact that the right to respect for private life was already recognized as a fundamental human right, the provisions on the protection of privacy were formulated in such a general way that they did not detail certain aspects of personal data protection. Therefore, the issues related to personal data were considered only as an essential part

[1] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights (2018) *Handbook on European data protection law*. 2018 ed. Luxembourg: Publication Office of the European Union, pp. 18-27; Bygrave A. L. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian studies in law*, pp. 181-183.

of the right to privacy, thus, the scope of personal data protection was sufficiently narrowed.

It was not until the second half of the XX – early XXI century that the active implementation of modern technologies in public and private spheres has led to a change of the approach to the recognition of the right to protection of privacy in connection with the processing of personal data. Due to the active use of cutting-edge technology, and the growing importance of the trans-border flow of personal data, the right to the protection of personal data began to be considered an independent right. Consequently, the UN Human Rights Committee issued General Comment no. 16 concerning the right to privacy providing particular attention to the protection of personal data and specifying that the rights of a person whose data was collected to ascertain what data was collected and to rectify or eliminate the incorrect or unlawfully obtained data. The UN Human Rights Committee also stressed that the right to privacy guaranteed under Article 17 extends both to the interference of the state authorities as well as natural and legal persons, however, originally right to respect for privacy only extended to the vertical relations with a state.[2] Likewise, the right to the protection of personal data was more comprehensively set forth by the Council of Europe in Convention no. 108 On the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Convention no. 108). It is noteworthy that Convention no. 108 is the first international binding treaty that establishes the definition of personal data and outlines key principles of data processing. In order to reinforce and strengthen the data protection with regard to the challenges of the digital age, Convention no. 108 has been modernized by protocol amending its provisions.[3]

It is worth mentioning that within the EU right to personal data protection was detailed in the Directive 95/46/EC of 24 October 1995, the Charter of Fundamental Rights of the EU, which after the entry into force of the Lisbon Treaty recognized the right to protection of personal

[2] UN Human Rights Committee (HRC) (1988). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April. Available from: https://www.refworld.org/docid/453883f922.html [Accessed 11 January 2021].

[3] Council of Europe (2018). *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* 10 October. Available from: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [Accessed 12 January 2021].

data as a fundamental right within the EU legal system, and the most recently adopted Regulation (EU) 2016/679 of 27 April 2016 usually referred to as GDPR.[4]

Nevertheless, public international law considers the status of personal data protection with continuing uncertainty given that: 1) the international human rights treaties ensures protection of private life in a broad manner and do not specify the particularities of data protection rights; 2) other international instruments concerning data protection are either regional or are non-binding; 3) there is a lack of international consensus on the scope of privacy and data protection given the differences in cultural and legal perceptions; 4) the substantial fragmentation on data protection in national and regional legal systems. It is alleged that future developments of data protection in international law could be achieved by either developing a uniform international treaty or using the experience of UNCITRAL to the data protection issues.[5] Currently, the only binding international treaty is Convention no. 108, which was adopted by the Council of Europe, yet it could be acceded by non-European countries. Although, it is argued that Convention no. 108 should be adopted by the UN as a global treaty given that it has already been accessed by countries outside the Council of Europe and therefore has all potential to be adopted as a global data protection treaty.[6]

There is no doubt that the full range of aspects related to the right to data protection and the definition of the principles of data protection are gradually developing through court interpretation. The significant impact both on the development of the right to personal data protection and the improvement of the legal framework governing the protection

---

[4] European Commission (2018) *Data Protection in the EU*. [online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [Accessed 15 January 2021].

[5] Kittichaisaree K., Kuner C. (2015) The Growing Importance of Data Protection in Public International Law. *EJIL:Talk!* 14. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ [Accessed 25 January 2021].

[6] Greenleaf G. (2018) The UN should adopt Data Protection Convention 108 as a global treaty: Submission on 'the right to privacy in the digital age' to the UN High Commission for Human Rights, to the Human Rights Council, and to the Special Rapporteur on the Right to Privacy. Sydney, 8 April 2018. Available from: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf [Accessed 13 January 2021]; Buttarelli G. (2016) Convention 108: from a European Reality to a Global Treaty. *Council of Europe International Conference*, Strasbourg, 17 June. Available from: https://edps.europa.eu/sites/edp/files/publication/16-06-17_speech_strasbourg_coe_en.pdf [Accessed 29 January 2021].

of personal data is made by the European Court of Human Rights (hereinafter – the ECHR or the Court). Moreover, since Convention no. 108 does not envisage the judicial or other controlling body to oversee compliance with its provisions, to some extent, it is the ECHR that may be treated as such a controlling body, which reviews the cases related to an alleged violation of the right to privacy under the Convention and take into account the provisions of the Convention no. 108.[7] That is being so the Court also pay particular attention not only to the domestic law and practice of the state concerned but also to the relevant international legal acts, EU law, as well as jurisprudence in the field of the data protection, including the case-law of the Court of Justice of the EU. Thus, the ECHR practice is of the utmost importance for the consolidation and streamlining of the data protection principles and standards.

2. RIGHT TO PRIVACY AND PERSONAL DATA PROTECTION UNDER THE ECHR: GENERAL ASPECTS

Traditionally privacy extends to the confidentiality of communications, covers the secrecy of telephone conversations, e-mails, and other forms of communication, including personal data on the Internet. At the same time, the category of personal data as information on an identified or identifiable individual covers not only printed textual information such as an individual's name, address, date of birth, identification card number, and phone number, but also photos, videos, and voice samples, even if recorded in public places and may also include confidential personal information about one's family life.[8] Privacy within the European legal framework covers the protection of an individual's 'personal space' that goes beyond data protection, therefore, privacy can be considered as a concept which is both broader than and independent from data protection, though there can be a significant overlap between the two.[9]

Turning to the ECHR, the cases regarding the violation of the right to protection of personal data are examined in terms of Article 8 of the Convention, which ensures the right to respect for private

[7] Rojszczak M. (2020) Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace. *Information & Communications Technology Law*, 29 (1), p. 30.

[8] Pazyuk A. (2016) European Approach to the Data Protection in the Police Sector: Current Status and Trends. *Law Review of Kyiv University of Law*, 4, p. 360.

[9] Kuner C. (2009) An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, 25, p. 313.

life. The protection of privacy under Article 8 originally was focused on protection from interference by public authorities, omitting the possible breaches in the private sphere. Although Article 8 provided for a negative obligation of the state and therefore privacy was originally granting negative freedom to individuals in relation with a state, yet the Court subsequently diverged from the initial focus of the Convention authors by accepting both positive obligations for states and positive freedom to individuals.[10]

The right to personal data protection was not initially incorporated within the text of the ECHR as an independent right. Moreover, the Convention from the outset was not perceived as an instrument for adequate protection of personal data since the latter developed after the adoption of the Convention and a special international treaty to regulate this sphere was further developed. Yet the ECHR contributed significantly to the evolution of the data protection concept by providing a broad interpretation of the right to respect for private life and defining the limits of Article 8 of the Convention.

Being of the multifaceted nature, needless to say, that private life under Article 8 of the Convention "*is a broad term not susceptible to exhaustive definition*".[11] In this regard, for a while, the issue of personal data protection was considered only in a close connection to the right to private life. Hence, the ECHR has been steadily developing the scope of the right to private life and has respectfully interpreted different aspects of personal data protection. However, it was only after the decision in *Tyrer v. the United Kingdom* case in 1978 that the Court had accepted the living instrument doctrine, which implies that "*the Convention is a living instrument which must be interpreted in the light of present-day conditions*".[12] Upon adoption of the *Tyrer* decision, the Court for the first time had recognized that the provisions of the Convention must be interpreted dynamically and reflect the current realities, challenges, and threats of a changing environment. For these reasons, the rights and freedoms listed in the Convention in order to be "*practical and effective, not theoretical and illusory*" should not be deemed as exhausted.[13] The living instrument

[10] Van der Sloot B. (2014) Privacy as Human Flourishing: Could a Shift Towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data? *JIPITEC,* 5(3), pp. 230-231.

[11] *Peck v. the United Kingdom* (2003) No. 44647/98, § 57, ECHR 2003-I.

[12] *Tyrer v. the United Kingdom* (1978) No. 5856/72, § 31, ECHR, Series A no. 26.

[13] *Airey v. Ireland* (1979) No. 6289/73, § 24, ECHR, Series A no. 32.

doctrine primarily has had its effect on the provisions of Article 8 of the ECHR. Having functioned as the main reference when the Court accepts new rights and freedoms under the Convention, Article 8 of the ECHR subsequently extended its scope and guaranteed the right to data protection.[14]

Nonetheless, the right to data protection is related to, yet it differs from the right to private life. While the right to data protection is always connected to the information on the identified or identifiable individual, the right to privacy does not necessarily include it. However, privacy is of a wider perspective that embodies a set of rights and values, including the right to be let alone, intimacy, autonomy, personhood, etc.[15] It is also worth mentioning that the scope of data protection is broader than the scope of privacy since not only does it cover the information on the identified individual but also all information on the identifiable individual, which includes a sufficiently wider variety of the information. Another difference concerns the responsibilities of private parties: while the right to privacy mainly addresses the obligations of public authorities not to interfere and to adopt the laws to secure relations between individuals, the right to data protection imposes quite identical obligations on both the authorities and private parties such as, for instance, employers or service providers.[16] Furthermore, it is also asserted that the right to data protection offers individuals more control over different types of data than the right to privacy. Thus, personal data protection is to be considered as a right that greatly coincides with the right to privacy still ensuring complementary, distinct benefits for individuals. While considering the cases related to personal data protection, the Court gives due importance to whether the individual is identified or identifiable. The latter issue reflects the sphere of application of the data protection legislation with regard to the definitions of 'personal data', which is broader than the concept of 'privacy interference' under Article 8.[17]

---

[14] Van der Sloot B. (2015) Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law*, 31(80), pp. 39 -40.

[15] Tzanou M. (2013) Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right. *International Data Privacy Law,* 3(2), pp. 89-93.

[16] Kokott J., Sobotta C. (2013) The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), pp. 224-226.

The advance of modern technologies makes the collection, storing, processing, and disclosure of personal data a vital part of day-to-day life, leading to the emergence of the right to data protection. Even though not initially foreseen in the text of the Convention, the right to data protection found its rightful place within the Convention system. Currently, the right to data protection, despite being closely connected to the right to privacy, is receiving its growing independence.

3. THE ECHR APPROACHES TOWARDS PROTECTION OF PERSONAL DATA

In order to assess the adequacy of personal data protection under the Convention system, the concepts applied by the Court should be analyzed, inter alia, in the light of the key data protection standards, with due regard to the inexhaustible nature of the 'personal data' and specificity of the sensitive data protection.

The ECHR has been gradually confirming that personal data protection, by and large, comes within the scope of Article 8 of the Convention. In the 1980s, a new doctrine originated in the ECHR case-law requiring that the laws should be accessible and foreseeable. At the outset, the Court hesitantly applied this doctrine to the right to privacy and protection of personal data matters, especially because these principles were difficult to uphold in cases of secret surveillance and special police investigations where secrecy and un-foreseeability are constitutive.[18] Nevertheless, this doctrine undeniably has influenced the path of data protection under the Convention. Hence the Court considers two aspects related to the data protection – the state's compliance with its positive obligations, i.e. guarantees of observance of the law, and negative obligations, i.e. refraining from arbitrary interference (and the sufficient safeguards in this respect). The Court also applies the margin of appreciation doctrine to the issues of data protection, providing a state with discretion in fulfilling its obligations under the Convention and reflecting its subsidiary role.[19]

---

[17] Lynskey O. (2014) Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order. *International and Comparative Law Quarterly,* 63(3), pp. 581-583.

[18] Van der Sloot B. (2020) The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *JIPITEC,* 11(2), p. 232.

[19] Byström N. (2016). The Data Subject and the European Convention on Human Rights: Access to Own Data. *EDILEX,* pp. 209-246.

The Court has been progressively introducing a broad interpretation of the term 'private life' with the equally broad notion of 'personal data' in data protection regulation.[20] Indeed, the scope of personal data is hard to be defined, and it includes not only ordinary personal data, such as name or date of birth but also other information that might lead to the identification of a person, including IP address, GPS data or DNA profile. In that respect, the Court also contributes to the interpretation of the key data protection principles, namely, the lawfulness, fairness and transparency, adequacy, relevance, and accuracy of personal data and the terms of its storage.

Since none of the international data protection documents contains an exhaustive list of what constitutes personal data, it is the Court's role to underline its inexhaustible nature and define whether certain information is personal data in each case. For instance, it did so in *Malone v. the United Kingdom* which related to the interception of communications of the applicant on behalf of the police by the metering of his telephone.[21] An important conclusion was reached that the use of data obtained from metering, including the numbers dialed, constitutes an integral element in the telephone communications and consequently it was stressed that the release of that information to the police without the consent of the subscriber was in violation of Article 8.[22] In this case, not only did the ECHR interpreted the scope of the 'personal data', by enlisting the information on dialled calls as information attributed to the individual, but also it significantly impacted the accessibility and foreseeability doctrine concerning privacy and existent data protection legislation.

Further, in *Benedik v. Slovenia, the* ECHR defined the scope of 'personal data' while dealing with the issue of obtaining data on the subscriber's dynamic IP address by the police. The Court pointed out that unlike the static IP address, which is permanently allocated to the device, a dynamic IP address is assigned temporarily, typically each time the device connects to the Internet. It was emphasized that the subscriber's

[20] de Hert P. and Gutwirth S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth S., Poullet Y., de Hert P., Nouwt J., de Terwangne C. (eds.) *Reinventing Data Protection?* Dordrecht: Springer Science, p. 21.

[21] Metering is a process of registration of the numbers dialed, the time and duration of each call.

[22] *Malone v. the United Kingdom* (1984) No. 8691/79, §§ 83-84, ECHR, Series A no. 82 The ECHR practice on the interception of the telephone communications further developed in *Weber and Saravia v. Germany* (2006) No. 54934/00, ECHR 2006-XI and *Szabó and Vissy v. Hungary* (2016) No. 37138/14, ECHR.

information associated with the dynamic IP, including the address, was not publicly available and allowed the police to identify the home from which the Internet connections had been made and reveal the applicant's identity.[23] Thus, the Court enlisted dynamic IP address to personal data since it could lead to the identification of an individual. Moreover, the Court recognized that GPS information also constitutes personal data and its collecting and processing falls within Article 8 of the Convention, given that it may determine the whereabouts and movements of a person in the public sphere. [24]

It is to note that the Court pays particular attention to the processing of the sensitive personal data – namely, health-related data, data on racial or ethnic origin, political opinions, religious beliefs, genetic and biometric data or information on a person's sex life or sexual orientation – and carefully examines such cases since this data needs a higher level of protection due to its sensitive nature. For instance, the case of *Z. v. Finland* related to the seizure of medical records in the course of criminal proceedings, disclosure of information on HIV status by the press, and publication of the applicant's name and health condition in judgment, while *M.S. v. Sweden* related to the transfer of the applicant's medical records by the clinic to the Social Insurance Office. In both cases, the ECHR stressed that the protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of the right to private life as guaranteed by Article 8. Moreover, disclosure of medical and health data may dramatically affect an individual's private and family life, as well as social and employment situation by exposing that person to opprobrium and the risk of ostracism. Respect for the confidentiality of such data is considered a vital principle, and it is of the utmost importance to provide appropriate safeguards to prevent any communication or disclosure of personal health data that could adversely affect the applicant's rights.[25] Also, landmark conclusions were reached in *P. and S. v. Poland* related to the dissemination by the hospital staff to the press sensitive personal data of the 14-year-old applicant, who

[23] *Benedik v. Slovenia* (2018) No. 62357/14, §§ 109, 113, ECHR.

[24] *Uzun v. Germany* (2010) No. 35623/05, §§51-52, ECHR 2010; On the surveillance and use of the GPS data see *Ben Faiza v. France* (2018) No. 31446/12, ECHR.

[25] *Z. v. Finland* (1997) No. 22009/93, §§ 95-96, ECHR, Reports of Judgments and Decisions 1997-I; *M.S. v. Sweden* (1997) No. 20837/92, § 41, ECHR, Reports of Judgments and Decisions 1997-IV.

became pregnant as a result of rape and decided to have an abortion. Even though the information released to the public did not contain the names or other details on the applicant, the Court noted that this information was detailed enough to establish the whereabouts and contact the applicant.[26] Thus, to fall within Article 8, the information concerning a person, even if published anonymized, must be detailed enough to establish the applicant's identity.

Meanwhile, it is acknowledged that the states enjoy wide discretion in the course of a criminal investigation and are authorized to collect sensitive personal data for relatively long periods. Yet the Court critically assess the data retention periods and requires data to be deleted once it is no longer relevant. It was *S. and Marper v. the United Kingdom* where the Court stated that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are, in fact, used in police investigations. The prolonged storage by the authorities of the applicants' fingerprints, cell samples, and DNA profiles after the completion of the criminal proceedings and the use of this data to determine their ethnic origin had infringed and violated their rights.[27] Moreover, in *Gaughran v. the United Kingdom*, it was stressed that the state failed to strike a fair balance between the public and private interests at stake, given the indefinite retention of biometric data of the previously convicted individual, including his DNA profile, fingerprints, and photos in the absence of any reference to the seriousness of the offence or the continuing need for such unlimited retention and any safeguards to review or delete of such data.[28] Therefore, indefinite retention of personal data, especially storage of sensitive personal data, could lead to a disproportionate interference with the individual's rights and the provisions of domestic law on that matter must be precise and clear to guarantee diligence of the authorities.

Due regard is also given to the states' discretion to collect personal data by secret measures and its storage in the secret state registers, which are

---

[26] *P. and S. v. Poland* (2012) No. 57375/08, § 130, ECHR.

[27] *S. and Marper v. the United Kingdom* (2008) nos. 30562/04, ECHR, and 30566/04, §§ 76, 86, ECHR 2008. The ECHR findings on the storage of fingerprints were further outlined in *M.K. v. France* (2013) No. 19522/09, ECHR.

[28] *Gaughran v. the United Kingdom* (2020) No. 45245/15, §§ 96-97, ECHR. More on the use of data obtained from the video surveillance of public places see *Peck v. the United Kingdom* (2003) No. 44647/98, ECHR 2003-I; on a DNA saliva samples see *Dragan Petrović v. Serbia* (2020) No. 75229/10, ECHR.

highly intrusive and requires sufficient guarantees for the individuals. One of the first cases in this regard was *Leander v. Sweden*, where the Court analyzed the legality of maintaining secret police files with information on the private life of the applicant and assessing the applicant by using that information in the process of employment. Although no violation of Article 8 was found since the national security prevailed over the individual interests, the ECHR noted that the storage and distribution of information about an individual by public authorities along with their refusal to allow the individual to refute this information amounted to an interference with the right to privacy.[29] Consequently, in *Amann v. Switzerland*, which related to the application of the secret surveillance measures, the Court confirmed this approach. Particular attention was given to Convention no. 108 while assessing whether there was the interference of public authorities by collecting and processing of the applicant's personal data, namely interception of telephone conversations, creation, and storage of a file about a person in this regard. It was also stressed that in the context of personal data the term 'private life' must not be interpreted restrictively.[30]

Nonetheless, even public information, if it is systematically collected and stored in files held by the authorities, could fall within the scope of data protection. For instance, in *M.M. v. the United Kingdom*, which related to the criminal data recorded by the authorities, *the* Court concluded: 'the greater the scope of the recording system, and the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data'. The Court another time emphasized that it is the authorities responsible for retaining and disclosing criminal record data that have an obligation to secure respect for private life, which is particularly important given the nature of the data held and the potentially devastating consequences of their disclosure.[31]

The issues related to the right to the destruction of a personal data file, lawfulness of the processing of personal data even collected without the use of secret surveillance and storage of a file containing the applicant's personal data, including information on his public activities, publications,

---

[29] *Leander v. Sweden* (1987) No. 9248/81, § 48, ECHR, Series A no. 116.

[30] *Amann v. Switzerland* (2000) No.27798/95, §§ 61-67, ECHR 2000-II. See also the Court's findings in *Taylor-Sabori v. the United Kingdom* (2002) No. 47114/99, ECHR; *Dumitru Popescu v. Romania (no. 2)* (2007) No. 71525/01, ECHR.

[31] *M.M. v. the United Kingdom* (2012) No. 24029/07, § 200, ECHR.

participation in political organizations, etc., was scrutinized in the case *Rotaru v. Romania*. The ECHR concluded that national law did not specify the circumstances to collect information by the intelligence service, the type of information that may be stored, the categories of persons in respect of whom it may be collected, as well as the collection procedure itself. Besides, the legislation did not mention specific retention periods of such information, the range of persons who have access to the files, the manner in which the data may be used, and the nature of those files. The Court noted that the storage and usage of such information were not accompanied by safeguards against abuse of powers.[32] Given these facts, the Court found that the relevant Romanian legislation was not sufficiently clear and foreseeable.

Undoubtedly, the interests of national security could prevail over individual interests, yet the law must provide sufficient safeguards against arbitrariness. The summary of the data protection principles for information obtained by secret surveillance measures that allowed interception of telephone communication was held in *Roman Zakharov v. Russia*. It its judgement the ECHR has formulated detailed criteria on the data protection: 1) the data should be collected on the basis of law; 2) the provisions of the law meet the requirements of accessibility, clarity and foreseeability; 3) the decision on granting secret surveillance measures should be subject to judicial review or control by other body; 4) such control should provide an opportunity for the person to present his arguments; 5) the court decision must be substantiated to prevent arbitrary interference; 6) the instructions in the court decision as to which data (documents) could be accessed should be as clear as possible; 6) the person in respect of whom the data is collected secretly must have effective means of protection, which would provide for the possibility of challenging the legality and reasonableness of the decision on access to such information, as well as obtaining compensation in the event of a violation; 7) access should only be granted to information necessary for the purposes of the investigation; 8) the information obtained must be properly recorded, stored and protected in order to prevent its modification, illegal destruction and

[32] *Rotaru v. Romania* (2000) No. 28341/95, §§ 53-63, ECHR 2000-V. The Court's opinion on the data collected and stored in public register see also *Gardel v. France* (2009) No.5335/06, ECHR 2009; *Catt v. the United Kingdom* (2019) No. 43514/15, ECHR; on the data held in the secret state register see *Segerstedt-Wiberg and Others v. Sweden* (2006) No. 62332/00, ECHR 2006-VII; *Shimovolos v. Russia* (2011) No. 30194/09, ECHR.

dissemination; 9) the information should be destroyed immediately once there is no need in it.[33] Thus, failure to comply with these rules results in the violation of Article 8 of the Convention.

It is important that the rights of data subjects are widely interpreted by the Court, including the right to access the data file and the right to rectify or destruct such data. For instance, in *Gaskin v. the United Kingdom, the* ECHR considered a positive obligation of a state to ensure the right to access personal data given the restriction of the applicant's access to social services documents on his early childhood and upbringing. It was noted that the applicant's rights were infringed due to the lack of an independent body to deal with requests for access to his personal data file. Moreover, the ECHR stressed the importance of ensuring the confidentiality and protection of third-person data by providing a certain individual with access to his or her data.[34]

Besides, the Court gradually deviated from its standpoint that privacy concerns only the vertical relations and expanded the guarantees of Article 8 to the horizontal relationship between individuals themselves, for instance, in relations between employer and employee. An important aspect that should be considered in that respect is whether the individual could reasonably expect privacy and anonymity of his data. In *Bărbulescu v. Romania*, regarding the monitoring of the employee's e-mails and access to their content, the Court held that it is particularly important to guarantee the employee's reasonable expectation of the privacy of his communication even if made from the employer's computer. In that case, the ECHR defined six critical factors to be regarded by the employer in the case of introduction the monitoring measures over the employees' correspondence: 1) notification of the employee on the possibility of such monitoring; 2) the extent of monitoring by the employer and the degree of interference in the employee's privacy; 3) provision of the legitimate reasons to justify the monitoring and access to the content of communication by the employer; 4) the possibility to use other less

[33] *Roman Zakharov v. Russia* (2015) No. 47143/06, §§ 227-305, ECHR. The provisions on bulk interception of communication were considered in *Centrum För Rättvisa v. Sweden* (2018) No. 35252/08, ECHR, *Big Brother Watch and others v. the United Kingdom* (2018) Nos. 58170/13, 62322/14 and 24960/15, ECHR.

[34] *Gaskin v. the United Kingdom* (1989) No. 10454/83, § 49, ECHR, Series A no. 160. On the access to the file containing personal data were see also *Odièvre v. France* (2003) No. 42326/98, ECHR 2003-III; *K.H. and Others v. Slovakia* (2009) No. 32881/04, ECHR 2009; *Haralambie v. Romania* (2009) No. 21737/03, ECHR.

intrusive monitoring measures; 5) the consequences of monitoring for the employee; 6) adequate safeguards against the abuse for the employee.[35] In *Antovic and Mirkovic v. Montenegro, the* Court examined the issue of video surveillance in the university auditoriums where the applicants held their classes. This case highlights the existent distinction between the right to private life and the right to personal data protection. It was noted that the data collected by the video surveillance in the workplace, both secret and not, is of a considerable intrusion into the employee's private life.[36] Consequently, since data protection covers the processing of all information on an identified or identifiable individual, the video monitoring (and recording), even though it was impersonal to some extent due to the blurred character of the recordings, amounted to the processing of information of the identifiable individual.[37]

Interestingly, the ECHR also decided over the cases related to data protection in respect of the legal entities. While international data protection documents only concern the rights of individuals, it is to notice that within the Convention system legal entities are also entitled to such protection. In *Bernh Larsen Holding AS and Others v. Norway*, the tax authority ordered one of the applicants' companies to provide copies of all data from a computer server shared with the other two applicants-companies. The ECHR acknowledged that requiring such information from the applicants constitutes an interference with their rights under Article 8 of the Convention. Yet the Court stressed that the interference was based on the national law, which was accessible, sufficiently clear and foreseeable, and it was necessary in a democratic society. Moreover, the procedure at issue had been accompanied by effective and adequate safeguards: 1) the applicant was notified in advance about a possible tax audit; 2) the applicants' representatives were present and could immediately object to the interference; 3) the backup copy of the data was sealed and could only be open in the applicants' presence; 4) upon

[35] *Bărbulescu v. Romania* (2017) No. 61496/08, §§ 71-81, 121, ECHR. On contrary, monitoring measures introduced by public company were justified in *Libert v. France* (2018) No. 588/13, §§ 46, 52, ECHR.

[36] *Antović and Mirković v. Montenegro* (2017) No. 70838/13, §§ 55-56. More on secret video surveillance at work see *López Ribalda and Others v. Spain* (2019) Nos. 1874/13 and 8567/13, ECHR.

[37] Ivanišević B. (2018) Distinction Between Privacy and Data Protection in ECtHR's Montenegro Case. *BDK Advokati*. 13 February. Available from: https://bdkadvokati.com/distinction-between-privacy-and-data-protection-in-ecthrs-montenegro-case/ [Accessed 02 February 2021].

the completion of the tax audit all data and traces of its content was to be destroyed.[38] Thus, the Court concluded that a fair balance was struck between the applicants' rights and interest in protecting the privacy and data of employees, on the one hand, and the public interest in ensuring effective tax audits, on the other.

The Court recognized that some issues related to personal data protection might also raise issues under Article 10 of the Convention, which guarantees freedom of expression and access to information. The majority of cases before the Court concerning the relationship between those two rights are related to the publication of the material containing personal data. One of such cases is *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland*, in which the newspaper published tax data on 1.2 million citizens, which amounted to a third of all taxable persons in Finland, most of whom were ordinary taxpayers and only a small part of them – people with high income, public figures or celebrities within the meaning of the Court's case law. The information published by the applicants' companies did not relate to a specific category of persons, such as politicians, public figures, civil servants, or other persons belonging to the public sphere through their activities or profits. However, the applicants relied on the relative anonymity of the published data by referring to the 'blending in' factor – the mass data was published, all in the same manner, so the information concerning a specific person 'blended in' and is anonymized to a certain extent. It was noted, however, that the applicants did not take into account the nature of the tax data since it was collected and published by the authorities for one purpose and by the applicants for a completely different. Though the personal data in question were public and the collection of information is an important preparatory step in journalistic activity and an integral, protected part of freedom of the press, yet the public interest in providing access to and collection of large amounts of tax data does not necessarily or automatically mean that there is also an interest in publishing this raw data without any analytical input.[39] Therefore, a distinction should be made between

[38] *Bernh Larsen Holding AS and Others v. Norway* (2013) No. 24117/08, §§ 106, 126-134, ECHR. Similarly, the search of the law firm's premises and seizure of the computer files and emails did not violate Article 8 in *Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal* (2015) No. 27013/10, ECHR.

[39] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* (2017) No. 931/13, §§ 137, 175-181, ECHR. See also the Court's findings in *Axel Springer AG v. Germany* (2012) No. 39954/08, ECHR and *Annen v. Germany* (2015) No. 3690/10, ECHR.

the processing of information for journalistic purposes and the dissemination of raw data, to which journalists only provide 'privileged' access. In the Court's view, the publication of the data in the manner and to the extent that the applicant companies had done was not contributing to public discussion, nor was it intended to do so.

Another important decision was reached in *Segerstedt-Wiberg and Others v. Sweden* where the Court considered that the storage of personal data related to political opinion, affiliations and activities kept in the state register had been deemed unjustified for the purposes of Article 8 and constituted an unjustified interference with the rights protected by Articles 10 and 11.[40]

Thus, the Court's jurisprudence displays various issues related to data protection, defines the scope of the right to data protection, its categories and which operations constitute data processing. It is the evolutive doctrine that empowers the Court to define the scope of data protection in the light of the rapid technological development and the accessibility and foreseeability doctrine that serve as the basis for judicial interpretation of the rights of the data subjects as well as core principles of data protection. Yet certain consideration arises while balancing the reasonable expectations of privacy and distinct rules for data protection. Even though the rights to privacy and personal data protection significantly overlap, still they should not be deemed virtually the same. It is evident from the recent Court's case-law that the difference between the two rights exists, and it is the Court's role to provide specific, distinct requirements for data protection.

4. CONCLUSION

Data protection from the outset of its emergence has been related to privacy to such an extent that it was complicated to establish precisely not only its notion but also its scope and unprecedented value. The fragmentation of data protection is attributed to the lack of a global international treaty or another relevant instrument in this sphere. In this regard, the main issue is whether the right to data protection receives adequate degree of protection under the Convention system since it is not explicitly mentioned either in the Convention or its Protocols. This article reveals

[40] *Segerstedt-Wiberg and Others v. Sweden* (2000) No. 62332/00, §§ 90-92, 107, ECHR 2006-VII.

the main concepts the Court applies in data protection cases. By applying the data analysis and comparative methods, the conclusion is reached that the ECHR has been contributing to the development of this right by defining the key principles of data protection which correspond to the underlying standards stemming from international legal acts in this sphere, including Convention no.108 and relevant EU data protection legislation. Accordingly, the Court has established that personal data should only be collected in accordance with the law, for specific and legitimate purposes, and it is the obligation of the states to establish adequate, accessible and sufficiently foreseeable data protection legislation. It is also important that a fair balance is struck between the aim of collection, processing, storage, or disclosure of data and the impact it has on the individual's rights.

The ECHR cases examined in the article confirm that the inexhaustible nature of the 'personal data' requires the Court to progressively broaden the scope of the latter in light of new technological developments and present-day conditions. Following the Court's case-law it is certain that the personal data by its definition is broader than the interests safeguarded by the scope of the right to private life. Thus, the right to data protection being emerged from the right to privacy is linked to the latter but is rather distinct. The Court's jurisprudence, hence, serves two key purposes – firstly, it fosters the development of the right to data protection, and secondly, it provides the consistency in interpretation of the key data protection principles and rights of data subject with regard to the modern challenges. Even not directly specified under the Convention system, the right to data protection is safeguarded by the Court and successively increasing its independence and significance as a fundamental right. This article concludes, however, that there is a continuing need to recognize the right to data protection as autonomous within the Convention system, which will provide a sufficiently higher level of protection for the data subject, including the specificities of data protection defined in the relevant international standards and will allow finding its rightful place in the existing human rights framework.

LIST OF REFERENCES

[1] *Airey v. Ireland* (1979) No. 6289/73, ECHR, Series A no. 32.

[2] *Antović and Mirković v. Montenegro* (2017). No. 70838/13, ECHR.

[3] *Amann v. Switzerland* (2000). No. 27798/95, ECHR 2000-II.

[4] *Bărbulescu v. Romania* (2017) No. 61496/08, ECHR.

[5] *Benedik v. Slovenia* (2018) No. 62357/14, ECHR.

[6] *Bernh Larsen Holding AS and Others v. Norway* (2013) No. 24117/08, ECHR.

[7] Buttarelli G. (2016) Convention 108: from a European reality to a global treaty. *Council of Europe International Conference*, Strasbourg, 17 June 2016. Available from: https://edps.europa.eu/sites/edp/files/publication/16-06-17_speech_strasbourg_coe_en.pdf [Accessed 29 January 2021].

[8] Bygrave A. L. (2010). Privacy and Data Protection in an International Perspective. *Scandinavian studies in law,* pp. 181-183.

[9] Byström N. (2016). The Data Subject and the European Convention on Human Rights: Access to Own Data. *EDILEX,* pp. 209-246.

[10] Council of Europe (2018). *Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* 10 October. Available from: https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [Accessed 12 January 2021].

[11] Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights (2018) *Handbook on European data protection law*. 2018 ed. Luxembourg: Publication Office of the European Union, pp. 18-27.

[12] de Hert P. and Gutwirth S. (2009) Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In: Gutwirth S., Poullet Y., de Hert P., Nouwt J., de Terwangne C. (eds.) *Reinventing Data Protection?* Dordrecht: Springer Science, pp. 3-44.

[13] European Commission (2018) *Data Protection in the EU*. [online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [Accessed 15 January 2021].

[14] *Gaskin v. the United Kingdom* (1989). No. 10454/83, ECHR, Series A no 160.

[15] *Gaughran v. the United Kingdom* (2020). No. 45245/15, ECHR.

[16] Greenleaf G. (2018) 'Modernised' data protection Convention 108+ and the GDPR. 154 *Privacy Laws & Business International Report* 22-3. Available from: http://www.ssrn.com/link/UNSW-LEG.html [Accessed 13 January 2021].

[17] Ivanišević B. (2018) Distinction Between Privacy and Data Protection in ECtHR's Montenegro Case. *BDK Advokati*. 13 February. Available from:

https://bdkadvokati.com/distinction-between-privacy-and-data-protection-in-ecthrs-montenegro-case/ [Accessed 02 February 2021].

[18] Kittichaisaree K., Kuner C. (2015) The Growing Importance of Data Protection in Public International Law. *EJIL:Talk!* 14 October. Available from: https://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/ [Accessed 25 January 2021].

[19] Kokott J., Sobotta C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), pp. 222–228.

[20] Kuner C. (2009) An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law & Security Review*, 25, pp. 307-317.

[21] *Leander v. Sweden* (1987) No. 9248/81, ECHR, Series A no. 116.

[22] Lynskey O. (2014) Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. *International and Comparative Law Quarterly,* 63(3), pp. 569-597.

[23] *M.M. v. the United Kingdom* (2012). No. 24029/07, ECHR.

[24] *M.S. v. Sweden* (1997). No. 20837/92, ECHR, Reports of Judgments and Decisions 1997-IV.

[25] *Malone v. the United Kingdom* (1984) No. 8691/79, ECHR, Series A no. 82.

[26] *P. and S. v. Poland* (2012). No. 57375/08, ECHR.

[27] *Panteleyenko v. Ukraine* (2006). No. 11901/02, ECHR.

[28] Pazyuk A. (2016) European Approach to the Data Protection in the Police Sector: Current Status and Trends. *Law Review of Kyiv University of Law*, 4, pp. 360-364.

[29] *Peck v. the United Kingdom* (2003) No. 44647/98., ECHR 2003-I.

[30] Rojszczak M. (2020) Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace. *Information & Communications Technology Law*, 29 (1), pp. 22-44.

[31] *Roman Zakharov v. Russia* (2015). No. 47143/06, ECHR 2015.

[32] *Rotaru v. Romania* (2000) No. 28341/95, ECHR 2000-V.

[33] *S. and Marper v. the United Kingdom* (2008) nos. 30562/04 and 30566/04, ECHR 2008.

[34] *Satakunnan Markkinaporssi Oy and Satamedia Oy v. Finland* (2017). No. 931/13, ECHR.

[35] *Segerstedt-Wiberg and Others v. Sweden* (2000) No. 62332/00, ECHR 2006-VII.

[36] *Tyrer v. the United Kingdom* (1978) No. 5856/72, ECHR, Series A no. 26.

[37] Tzanou M. (2013) Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right. *International Data Privacy Law,* 3(2), pp. 88-99.

[38] UN Human Rights Committee (HRC) (1988) *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 April. Available from: https://www.refworld.org/docid/453883f922.html [Accessed 11 January 2021].

[39] *Uzun v. Germany* (2010) No. 35623/05, ECHR 2010.

[40] Van der Sloot B. (2014) Privacy as Human Flourishing: Could a Shift Towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data? *JIPITEC,* 5(3), pp. 230-244.

[41] Van der Sloot B. (2015) Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data". *Utrecht Journal of International and European Law,* 31(80), pp. 25–50.

[42] Van der Sloot B. (2020) The Quality of Law: How the European Court of Human Rights Gradually Became a European Constitutional Court for Privacy Cases. *JIPITEC,* 11(2), pp. 160-185.

[43] *Z v. Finland* (1997) No. 22009/93, ECHR, Reports of Judgments and Decisions 1997-I.

[44] *Zaichenko v. Ukraine (No.2)* (2015) No. 45797/09, ECHR.