UDK 004.056.53:342.7]:341.645(4-67EU)
Original scientific paper

DATA PROTECTION AND CYBERSECURITY: CASE-LAW OF TWO EUROPEAN COURTS*

Dunja Duić, PhD, Associate Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
dduic@pravos.hr

Tunjica Petrašević, PhD, Full Professor
Josip Juraj Strossmayer University of Osijek, Faculty of Law Osijek
Stjepana Radića 13, 31 000 Osijek, Croatia
tpetrase@pravos.hr

ABSTRACT

Cybersecurity is not easily defined. The 2019 EU Cybersecurity Act defines it as the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.[1] Enduringly, cybersecurity was associated with national security, without consideration of what 'secure' Internet means for individual users. In reality, cybersecurity policy focused by and large on systems rather than users, i.e., people. However, as a policy area concerned with online behavior regulation, its definition and implementation inevitably has profound implications for human rights, especially in regard to data protection and freedom of expression. Unsurprisingly, cybersecurity has become a new human rights battleground.[2] The EU Cybersecurity Act and subsequent legislation represent a normative shift in our conception of data ownership, putting ownership and control of personal information in the hands of the user rather than the service provider. Luckily, there have been positive legislative shifts regarding data protection in the context of the EU cybersecurity policy at EU

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

1 Art. 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151, pp. 15–69.

2 More at: Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights,* OpenDemocracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights/], Accessed 25 November 2022.

level. But are they (or will they be) adopted by European courts? To answer, this paper peers into the relevant case-law of the Court of Justice of the EU as well as of the European Court of Human Rights.

***Keywords**: data protection, cybersecurity, human rights, European Union, Council of Europe, Court of Justice of the EU, European Court of Human Rights*

1. INTRODUCTION

In these times of globalization and all-digitalization, technological advancements are a double-edged sword to human rights and freedoms. The advent of the Internet and its pervasiveness stand as one of key such developments of the past 30 years. The Internet has come to pervade the entire social fabric, from communication and learning, to work and shopping.[3] But with the benefits of digitalization come also new threats.[4] As part and parcel of technological advancements, cybersecurity has become integral to a number of countries' and the EU's political action. Until recently, as part of national policy, cyberspace was tied to digital market, cybersecurity, migration and/or terrorism issues. Over time, due to its importance and security issues, the EU included cyberspace and cybersecurity into the scope of the Common Foreign and Security Policy (CFSP).[5]

For clarity, the paper will first turn to defining data protection and cybersecurity and, next, to explaining their interrelatedness.

Essential in the domain of personal data protection in the EU is the General Data Protection Regulation (GDPR), under which personal data is *any information relating to identified or identifiable natural persons, whereby an identifiable natural person is one who can be identified by a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.[6]

There are a number of ways of defining cybersecurity. Microsoft defines it as *the practice of protecting one's digital information, devices, and assets (digital security),*

---

3 Wiśniewski, A., *The European Court of Human Rights and Internet-Related Cases,* Bialystok Legal Studies, Vol. 26, No. 3, 2021, p. 110.

4 Schünemann, W. J.; Baumann, M-O. (eds.), *Privacy, Data Protection and Cybersecurity in Europe*, Springer, Cham, 2017, pp. 1-2.

5 Duić, D., *The EEAS as a Navigator of EU Defence Aspects in Cyberspace*, European Foreign Affairs Review, Vol. 26, No. 1, 2021, pp. 101-114.

6 Art. 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119, pp. 1–88.

which includes one's personal information, accounts, files, photos, and even money.[7] Per the 2019 EU Cybersecurity Act, *cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*[8] *The* Freedom Online Coalition (FOC) sees it as[9] *the preservation – through law, policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline.*[10]

Internet should be 'free' but also secure. For a long time, cybersecurity was strongly tied to national security, disregarding what 'secure' Internet means for individual users.[11] As a result, cybersecurity policy was angled at systems more than people. However, as a policy area concerned with online behavior regulation, its definition and implementation has profound implications for human rights, especially in regard to data protection and freedom of expression. It is then hardly surprising that – to quote the OpenDemocracy forum – cybersecurity has become a new human rights battleground.[12]

In support of their position, OpenDemocracy underline several important facts. First, that cybersecurity policy was framed exclusively by national security agencies and select private sector interests (e.g. telecommunications operators). Second, that government services, which store a wide range of sensitive data (from taxation to health records), are rapidly migrating online, while (as third) the monopoly-holding tech companies elite's business model relies on the processing, storage, and monetization of the people's personal information. Correspondingly, cybersecurity has become fused with 'national security', leaving by the wayside the

---

7 *What is cybersecurity?*, [https://support.microsoft.com/en-us/topic/what-is-cybersecurity-8b6efd59-41ff-4743-87c8-0850a352a390], Accessed 25 November 2022.

8 Art. 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151, pp. 15–69.

9 The Freedom Online Coalition (FOC) is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide. See more at: Freedom Online Coalition, *Aims and Priorities*, [https://freedomonlinecoalition.com/aims-and-priorities/], Accessed 25 November 2022.

10 See: Freedom Online Coalition, *Why Do We Need a New Definition for Cybersecurity?,* [https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity], Accessed 25 November 2022.

11 Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights*, Open Democracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights], Accessed 25 November 2022.

12 The statement was taken from the OpenDemocracy forum as an independent international media platform. See more: Puddephatt; Kaspar, *op. cit.*, note 2.

interests of individual users and what 'secure' Internet might mean for them. Such understanding of cybersecurity – in which surveillance powers run wild, 'backdoors' undermine encryption and anonymity, and accountability is an anomaly – may easily come to diametrically oppose individual security and individual (human) rights.[13] Per Pavlova, countries should find the right balance between fundamental rights and freedoms of their citizens, with the aim of achieving an appropriate level of national security that ensures respect for fundamental rights. Countries should not be able to hide their failure to do so behind the pretext of human rights vs. national security.[14]

Cybersecurity must begin to be understood as a policy centered on the security and rights of the end user rather than systems, as provided for under the 2019 EU Cybersecurity Act. Would that imply a normative shift in our understanding of data ownership, putting the reins of ownership and control of personal data in the hands of the user instead of the service provider? A democratic society provides cybersecurity that entails the informed consent of the population – in other words, it ensures that parties other than security agencies have a say in the conversation around it that will ultimately result in cybersecurity being understood above all as the protection of persons.[15] Luckily, there have been positive legislative shifts regarding data protection in the context of the EU cybersecurity policy at EU level (to be discussed below). But are they (or will they be) adopted by European courts? To answer this, this paper peers into the relevant case-law of the Court of Justice of the EU (CJEU) as well as of the European Court of Human Rights (ECtHR).

This paper updates the present authors' previous research in data protection in the CJEU and ECtHR case-law given new developments in the area.[16]

---

13 *Ibid*.

14 Pavlova, P., *Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups*, Peace Human Rights Governance, Vol. 4, No. 3, 2020, p. 409.

15 See: Puddephatt, A.; Kaspar, *op. cit.*, note 2; Duić, D., *Common Security and Defence Policy and Cyber Defence*, in: Brill, A.; Misheva, K.; Hadji-Janev, M. (eds.), *Toward Effective Cyber Defense in Accordance with the Rules of Law*, IOS Press, Amsterdam, 2020, pp. 32-42.

16 Petrašević, T.; Duić, D., *Standards of Human Rights Protection in the Domain of Personal Data Protection: Strasbourg vs Luxemburg*, in: Sander, G. G.; Poščić, A; Martinović, A. (eds.), Exploring the Social Dimension of Europe- Essays in Honour of Nada Bodiroga-Vukobrat, Verlag Dr. Kovač, Hamburg, 2021, pp. 215-231.

2. A BRIEF EVOLUTION OF INTERNATIONAL AND EU CYBERSECURITY POLICY

In 'The right to privacy in the digital age',[17] the UN General Assembly, concerned over the negative impact of communications surveillance and interception on human rights, called on all member states to review their legislation, procedures and practice of surveillance of communications, their interception and collection of personal data and ensure full and effective implementation of their obligations in accordance with international human rights standards.[18] In its resolution on the promotion and protection of human rights on the Internet, the UN's Human Rights Council affirmed that the same rights that people have offline must also be protected online, in particular, freedom of expression.[19,20]

The European Convention on Human Rights (Convention) – a vital instrument of the Council of Europe – was adopted in 1950, at a time when the Internet was an unknown to the wider society and its creators could not have foreseen technology's current magnitude. The ECtHR must therefore interpret the Convention as a "living instrument" [21] in light of changes in the social circumstances.[22] The right to personal data protection is not an autonomous right guaranteed by the Convention. Nevertheless, the ECtHR subsumes and protects it primarily under Article 8 of the Convention – the right to private and family life, even though it can also be considered under other articles of the Convention and certain protocols.[23,24] Cybersecurity is also not regulated by the Convention or its protocols, but the ECtHR interprets the Convention considering changes in the social circumstances, taking into account technological progress, and especially the increasingly widespread use of the Internet (to be discussed in more detail below).

---

17 Resolution A/RES/68/167 adopted by the UN General Assembly on 18 December 2013 on the right to privacy in the digital age.

18 United Nations, *General Assembly backs right to privacy in digital age,* [https://news.un.org/en/story/2013/12/458232], Accessed 30 December 2022.

19 United Nations, High Commissioner for Human Rights, Resolution A/HRC/RES/32/13 on the promotion, protection and enjoyment of human rights on the Internet. See also: United Nations, High Commissioner for Human Rights, *The right to privacy in the digital age*, [https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age], Accessed 30 December 2022. See also: Pavlova, *op. cit.*, note 14, p. 398.

20 For more on development of cybersecurity policy at the international level, see: Pavlova, *op. cit.*, note 14, pp. 398-401.

21 *Demir and Baykara v Turkey*, Application No. 34503/97, Judgment, 12 November 2008, par. 146.

22 Wiśniewski, *op.cit.,* note 3, p. 110.

23 See: *Guide to the Case-Law of the European Court of Human Rights: Data protection*, Council of Europe / European Court of Human Rights, 2022 (Updated on 31 August 2022), p. 7.

24 Petrašević; Duić, *op.cit.*, note 16, pp. 223-224.

Apart from the Convention, two other important documents have been adopted under the auspices of the Council of Europe: the Convention on Cybercrime[25] (the Budapest Convention), along with its Protocol on Xenophobia and Racism Committed through Computer Systems, [26] and the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[27]

The EU is spearheading in the category of cybersecurity reinforcement, well aware that – while creating a profusion of new opportunities for the economy and society – the digital era also introduces new challenges. Cyber-incidents and cyber-attacks often bring billions of euros in losses annually. Cybersecurity, trust, and privacy form the backbone of a prosperous European Digital Single Market (EDSM). To shield the EDSM and protect infrastructure, governments, businesses and citizens, the EU has adopted a wide range of measures.[28] But how did it all begin?

In 2013, the EU adopted its first Cybersecurity Strategy on an Open, Safe and Secure Cyberspace, aimed at safeguarding an open and free cyberspace under the same EU norms, principles and values upheld 'offline'.[29] The Directive on Security of Network and Information Systems (NIS Directive), enacted in 2016, was the first tangible piece of EU law aimed at boosting the cybersecurity at EU level overall.[30] The EU Cybersecurity Act of 2019 established an EU framework for cybersecurity certification to enhance cybersecurity of digital products and services in Europe,[31] while strengthening the action of the European Union Agency for Cybersecurity (ENISA). Founded in 2004, ENISA contributes to the EU's cyber policy, improves ICT product, service and procedure reliability through a cybersecurity certification program, cooperates with member states and EU bodies, and

---

25 Convention on Cybercrime (ETS No. 185) [2001].

26 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) [2003].

27 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [1981].

28 European Commission, *Building strong cybersecurity – Brochure*, 2019, [https://digital-strategy.ec.europa.eu/en/node/1500/printable/pdf], Accessed 5 January 2023.

29 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, [2013] JOIN(2013) 1 final, par. 1.1.

30 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194, p. 1–30. In December 2020, the European Commission proposed a revision of Directive (EU) 2016/1148 (NIS2).

31 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (PE/86/2018/REV/1) [2019] OJ L 151, p. 15–69.

helps Europe prepare for future cyber challenges.[32] In 2020, the European Commission adopted the new EU Cybersecurity Strategy for the Digital Decade.[33] To increase the Internet networks and information systems security, in 2021, the Council of the EU adopted the Regulation establishing the European Cybersecurity Competence Centre (ECCC) (based in Bucharest) to aggregate investment in research, technology and industrial development in cybersecurity.[34] In May 2022, the Council extended until May 2025 the framework for restrictive measures against cyberattacks threatening the EU and its member states. The framework[35] was originally established in May 2019 as the EU's joint diplomatic response to malicious cyber activities ('cyber diplomacy toolbox'). The framework enables the EU and member states to apply all CFSP measures, including restrictive measures, where necessary, with the aim of preventing and containing malicious cyber activity aimed at undermining the integrity and security of the EU and its member states, as well as deterring from them and responding to them.[36] Cyberspace has become a matter of geopolitical competition, so the EU must be ready to respond quickly and forcefully to cyberattacks. Guidelines for strengthening the EU's position in the field of cybersecurity are provided in the Strategic Compass – the EU's action plan for strengthening the security and defense policy until 2030.[37,38]

3. RELATION OF THE TWO EUROPEAN COURTS REGARDING HUMAN RIGHTS PROTECTION

To better understand the case-law of the two European courts (the CJEU and the ECtHR) in regard to personal data protection in the context of cybersecurity, their relation in the field of human rights protection must be understood in general. Particularly interesting in that regard is that relation before and after the entry

---

32 ENISA - European Union Agency for Cybersecurity, *About*, [https://www.enisa.europa.eu/about-enisa/about/], Accessed 5 January 2023.

33 Joint communication to the European parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN/2020/18 final.

34 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT [2021] OJ L 202.

35 Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L 129I.

36 Council of the EU, *Cyber-attacks: Council extends sanctions regime until 18 May 2025*, 2022, [https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025], Accessed 5 January 2023.

37 A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security [2022] 7371/22.

38 For more on the development of EU cyber policy, see: Christou, G., *Cybersecurity in the European Union*, Palgrave Macmillan, London, 2016, pp. 87-118.

into force of the Charter of Fundamental Rights of the EU[39] (Charter) that was a turning point in the development of human rights in the EU.[40]

Given that the EU (that is, the European Community as its precursor) was founded primarily for the purpose of economic integration, human rights were reasonably not in its primary focus. Human rights protection was instead entrusted to the Council of Europe as a separate international organization, of which EU member states automatically became members, as well as signatories to the Convention.[41] Below is a brief overview of the two courts' relation, including references to relevant literature, given that the topic was discussed as part of the present authors' previous research.

After being shunned, then accepted by the CJEU only as unwritten rules (general principles of law), and eventually codified in the EU Charter on Fundamental Rights, the protection of fundamental human rights in the EU came into its own only with the EU's accession to the Convention.[42] Even though after the entry into force of the Treaty of Lisbon (2009) there were no formal legal prerequisites for the EU's accession to the Convention, the CJEU still issued the highly criticized negative opinion no. 2/13 of 18 December 2014.[43,44] The consensus in literature

---

39 Charter of Fundamental Rights of the European Union [2012] OJ C 326, pp. 391–407.

40 See: Cherubini, F., *The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View of the Accession*, German Law Journal, Vol. 16, No. 6, 2015, pp. 1375-1386.

41 Petrašević, T.; Duić, D., *Opinion 2/13 on the EU accession to the ECHR*, in: Vinković, M. (ed.), New Developments in the EU Labour, Equality and Human Rights Law, J. J. Strossmayer University of Osijek – Faculty of Law, Osijek, 2015, p. 253. Petrašević, T.; Kovačić Markić, L., *Položaj nacionalnih ustavnih sudova u primjeni mehanizma prethodnog postupka s posebnim osvrtom na Ustavni sud Republike Hrvatske*, in: Bačić, A. (ed.), Pravo i politika EU: stara pitanja, novi odgovori, HAZU, Zagreb, 2020, pp. 144-145.

42 Petrašević; Markić Kovačić, *op. cit.*, note 41, pp. 145-146. Petrašević; Duić, *op. cit.*, note 16, pp. 251-267. Petrašević, T., *The relation of Human Rights and market freedoms in case law of the CJEU*, in: Primorac, Ž.; Bussoli, C.; Recker, N. (eds.), Economic and Social Development: 16th International Scientific Conference on Economic and Social Development "The Legal Challenges of Modern World", Varazdin Development and Entrepreneurship Agency, Varaždin/Split, 2016, pp. 142-145.

43 E.g. Lazowski, A.; Wessel, R.A., *When Caveats Turn into Locks: Opinion 2/13 on Accession of the European Union to the ECHR*, German Law Journal, Vol. 16, No. 1, 2015, pp. 179 – 212. See blog discussions: Peers, S., *The CJEU and the EU's Accession to the ECHR: A Clear and Present Danger to Human Rights Protection*, EU L. ANALYSIS BLOG, 2014, [http://eulawanalysis.blogspot.com.es/2014/12/the-cjeu-and-eus-accession-to-echr.html], Accessed 30 December 2022. Douglas-Scott, S., *Opinion 2/13 on EU Accession to the ECHR: A Christmas Bombshell from the European Court of Justice*, U.K. CONST. L. BLOG, [http://ukconstitutionallaw.org], Accessed 30 December 2022. Gotev, G., *Court of Justice rejects draft agreement of EU accession to ECHR*, Euractiv, 2014, [http://www.euractiv.com/sections/eu-priorities-2020/court-justice-rejects-draft-agreement-eu-accession-echr-310983], Accessed 30 December 2022.

44 For more on Opinion 2/13 on the EU accession to the ECHR, see: Petrašević; Duić, *op. cit.*, note 16, pp. 251-266.

on the exhaustively discussed topic[45] of the formal grounds of said CJEU's opinion is that behind it likely lay a power struggle between the CJEU and the ECtHR. [46] Namely, in case of accession, the decisions of the CJEU in the field of human rights protection would fall under the supervision of the ECtHR. Consequently, the ECtHR would *de facto* become superior to the CJEU.

Namely, even though the Convention is still not formally part of the EU legal order, by virtue of the provision of Art. 52(3) of the EU Charter of Fundamental Rights, the standards set by the ECtHR are binding on the CJEU. Specifically, to the extent to which the EU Charter contains rights corresponding to those guaranteed by the ECHR, the meaning and scope of application of those rights are equal to those of the Convention. Apart from the obligation to consider relevant issues, i.e., to avoid contradictions in relation to the ECtHR's case-law on relevant issues, this also includes the implementation of its awards, with a view to achieving a uniform interpretation of fundamental and human rights. The CJEU's consistency in this regard after entry into force of the Treaty of Lisbon, i.e., of the EU Charter, evidences itself best from its judgements.[47]

In the field of human rights protection today, the two courts increasingly frequently take opposing positions on the protection of the same fundamental human right or freedom guaranteed both by the Convention and the Charter. National, and particularly constitutional courts are often faced with the dilemma of whether to prioritize the views of the Strasbourg or Luxembourg court.[48]

Having come a long way, human rights protection in the EU today occupies a central place and stands as a primary EU right. Nevertheless, while the ECtHR is exclusively tasked with the protection of fundamental human rights and freedoms, the CJEU – in addition to protecting human rights – is tasked with preserving the goals of the EU, particularly the functioning of the EU common market, which requires a delicate balancing of different interests.[49]

In sum, the CJEU does protect human rights, but in light of EU goals, as evident from its case-law. To remain within the scope of this paper, the relation of the ECtHR and the CJEU will be observed exclusively through the lens of data pro-

---

45 Petrašević, T.; Poretti, P., *Pravo na suđenje u razumnom roku – postoji li (nova) praksa Suda Europske unije?*, Harmonius - Journal of Legal and Social Studies in South East Europe, Vol. 7, No. 1, 2018, p. 189.

46 Petrašević; Markić Kovačić, *op.cit.*, note 41, p. 146.

47 Petrašević; Poretti, *op.cit.*, note 45, p. 193.

48 *Ibid.*

49 See: Jakir, V., *Human Rights – With or without the internal market*, Zagreb, 2012, master thesis.

tection in the context of cybersecurity, and in that adding to the present authors' previous research in that area.[50]

4. CASE-LAW OF THE TWO EUROPEAN COURTS ON DATA PROTECTION IN THE CONTEXT OF CYBERSECURITY

The global war on terrorism has brought to the forefront national and public security and led to security services' mass-invasion of personal data privacy. It is upon the CJEU and the ECtHR to assess the merits of such invasions through testing their necessity and proportionality and evaluating their compliance with legitimate objectives.[51] The standards set by the ECtHR were largely complied with by the CJEU in its rulings, including the ECtHR's test of necessity and proportionality. The CJEU was faced mainly with issues of blanket coverage that enabled mass surveillance and access to user data under EU Directives to national security services. The CJEU declared such measures invalid on grounds of failing the necessity and proportionality test due to the lack of legal measures that could protect those were not suspects under law (more on this below, on *Schrems*).[52]

Both courts acknowledge through their case-law the society's need to fight serious crime and terrorism. While such measures may be indispensable to tackle security challenges such as fighting terrorism and preventing serious transnational crimes, they must not go beyond the strictly necessary. The two courts have also highlighted the importance of the existence of legal remedies against such measures.[53]

The two European courts are tasked with the protection of citizens from the state machinery and security agencies. To do so, they are to carry out the necessity and proportionality tests[54] while finding equilibrium between the right of individuals to data privacy and the national security of member states. The balancing act is made only more arduous by the ongoing global anti-terrorism war.[55]

In contrast to the Convention, the Charter in its Article 8 recognizes the protection of personal data as an independent right. Nevertheless, the ECtHR protects

---

50 Petrašević; Duić, *op.cit.*, note 16, pp. 215-231.

51 Syed, H., *Data Protection Rights & National Security Objectives: Critical Analysis of ECtHR and CJEU Case Law*, Nor. Am. Aca. Res., Vol. 2, No. 3, 2019, p. 155.

52 *Ibid.*

53 *Ibid.*

54 See more on the proportionality and necessity tests: Omejec, J., *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava*, Novi informator, Zagreb, 2013, pp. 1253-1267.

55 Syed, *op.cit.*, note 51, p. 157.

that right under Art. 8 of the Convention (the right to privacy). The term 'personal data' itself has a similar meaning in the two courts' practice.[56]

Below, an analysis of selected ECtHR and CJEU case-law with introductory remarks specific to each court. The concluding remarks offer a comparison of the two courts' positions.

4.1. Case-law of the ECtHR

There is a modest number of Internet-related cases in the ECtHR case-law: to classify as such, a case must contain a cross-border element. In online communication, data are usually transmitted via servers located in different territorial jurisdictions. Occasionally, the establishing of the state of jurisdiction causes significant difficulties.[57] Narrowed to cases concerning data protection in the context of cybersecurity only, the number dwindles even further. A search of the ECtHR case-law (via the HUDOC database) by the terms 'data protection' and 'cybersecurity returns only one result: *K.U. v Finland.*[58] Replacing 'cybersecurity' with 'cyberspace' also returns only one case: *Big Brother Watch.*[59] Only by expanding the search through replacing 'cybersecurity' with 'national security' does it return a sizable number of cases: 1632. (Importantly, these cases include protection of privacy in general, and not only data protection, given that the search cannot be narrowed by that specific criterion/term.) Below is an analysis of selected data protection cases examined by the ECtHR through the lens of national security and with a special reference to cybersecurity.

On the one hand, in deciding certain cases, the ECtHR takes into account the Internet's advantages. In particular, the court highlights the Internet's value to the exercise of certain rights, such as the freedom of expression, observing that it has become one of the main vehicles for the exercising of the right to freedom and for receiving and sharing information and ideas.[60] The ECtHR also recognizes the Internet's value in enhancing the general news availability and facilitating information dissemination, as well as its significance in education and research, especially given its wide availability to the public and being free for use.[61]

---

56 *Ibid*., p. 159.

57 Wiśniewski, *op.cit*., note 3, p. 112.

58 *K.U. v Finland*, Application No. 2872/02, Judgment, 2 December 2008.

59 *Big Brother Watch and Others v the United Kingdom*, Application Nos. 58170/13, 62322/14, 24960/15, Judgment, 13/09/2018; and *Big Brother Watch and Others v the United Kingdom*, Application Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment, 25 May 2021.

60 *Cengiz and Others v Turkey*, Application Nos. 48226/10, 14027/112015, Judgment, 1 December 2015, par. 49.

61 Wiśniewski, *op.cit*., note 3, p. 113.

On the other hand, the ECtHR is aware of the Internet's disadvantages: the ease, extent, and speed of online data sharing, as well as the permanence of the shared data.[62] As the court sees it, compared to traditional media, this alone may significantly exacerbate the repercussions of unlawful speech on the Internet.[63]

The ECtHR is not blind to the dangers of the Internet for human rights, finding that *the rapid development of telecommunications technologies in recent decades has led to the emergence of new types of crime and has also enabled the commission of traditional crimes by means of new technologies.*[64] Clearly aware of the Internet's anonymous character, the court sees its crime-facilitating qualities.[65] Cybercrime (offences against or through computer systems) has become a substantial threat to human rights, democracy, and the rule of law, as well as international peace and stability, with enormous social and economic consequences. The Council of Europe is attempting to combat it.[66]

As its case-law shows, the ECtHR considers that personal data protection and retention falls under private life as protected by Article 8 of the Convention.[67] While the fundamental goal of Article 8 is to safeguard the individual from arbitrary government intrusion, there may be positive responsibilities inherent in effective respect for private or family life.[68] In this sense, member states have a positive obligation to preserve the privacy of individuals on the Internet.

In *K. U. v. Finland* – one of the most notable cases in that regard – the ECtHR took the view that a state may be liable in regard to third-party personal data storage providers. The case involved a provider's refusal to disclose data on the user of the IP address from which certain content defaming to the minor applicant were uploaded. The provider invoked its obligation to comply with the then applicable Finnish law in regard to the protection of the confidentiality of electronic communications. The ECtHR found that, although the exercise of the right to freedom of expression and secrecy of electronic communications is essential, electronic com-

---

62 *Delfi AS v Estonia*, Application No. 64569/09, Judgment, 16 June 2015, par. 147. More in: Wiśniewski, *op.cit.*, note 3, p. 114.

63 *Delfi AS v. Estonia*, *op. cit.*, note 62, par. 147.

64 *K.U. v Finland*, *op. cit.*, note 58, par. 22. More in: Wiśniewski, *op.cit.*, note 3, p. 114.

65 *Ibid.*

66 More at: Council of Europe, *Action against Cybercrime*, 2023, [https://www.coe.int/en/web/cybercrime], Accessed 5 January 2023.

67 See: *S. Marper v the United Kingdom*, Application Nos. 30562/04 and 30566/04, Judgment, 4 December 2008, par. 103.

68 *Airey v Ireland*, Application No. 6289/73, Judgment, 9 October 1979, par. 32.

munications and Internet services' users must be guaranteed protection of privacy and freedom of expression.[69]

Governments frequently obtain data through secret surveillance to safeguard national security. Such secret surveillance systems and actions must contain legal safeguards and be supervisable:[70] even where created to preserve national security, such systems risk the weakening or even destroying of democracy in the name of preserving it.[71] The ECtHR must therefore be convinced that appropriate and effective safeguards against abuse of such systems exist. In brief, where personal information is stored in the interests of national security, robust and effective safeguards against government misuse must be in place. Where such protections exist, the ECtHR will not necessarily find a violation of Article 8.[72]

Another notable case in the domain of mass surveillance – *Big Brother Watch and Others v. the United Kingdom*[73] – involved three applications against the United Kingdom lodged by companies, charities, organizations and individuals. The case was brought after Edward Snowden (a former associate of the US National Security Agency) exposed the surveillance and data sharing programs between the US and the UK. The applicants argued that the nature of their activities implied that their electronic communications had been intercepted or obtained by the UK's intelligence services after being intercepted by foreign governments, and/or obtained by the UK's authorities via communications service providers (CSPs).

After examining the regime for bulk interception of communications, the ECtHR found a number of system deficiencies and a violation of Articles 8 and 10 of the Convention. Since the court did not find a violation of Article 8 with regard to the intelligence sharing regime, the applicants requested a referral to the Grand Chamber. In its decision of 25 May 2021, the Grand Chamber largely confirmed the judgment of the first-instance council but made a clear distinction between targeted and mass surveillance. It also set clear mass surveillance guidelines, starting from the so-called Weber Guidelines that the ECtHR defined in *Weber*,[74] as well as eight additional guarantees (which fall outside the scope of this paper).

---

69 *K.U. v. Finland, op. cit.,* note 58, par. 43.

70 See: *Weber and Saravia v Germany*, Application No. 54934/00, Decision, 29 June 2006, par. 94. *Liberty and Others v the United Kingdom*, Application No. 58243/00, Judgment, 1 July 2008, par. 62.

71 See: *Klass and Others v Germany*, Application No. 5029/71, Judgment, 6 September 1978, paras. 49-50.

72 See also: *Youth Initiative for Human Rights v Serbia*, Application No. 48135/06, Judgment, 25 June 2013.

73 *Op. cit.*, note 59.

74 *Weber and Saravia v. Germany*, *op. cit.*, note 70.

Big Brother Watch was only the first in a slew of cases in which the ECtHR had the opportunity to examine extensive surveillance and data retention regimes of Council of Europe member states such as Sweden[75], Hungary[76], Russia[77], Germany[78], Moldova[79] and Romania.[80,81] The positions of the ECtHR in these cases can be summarized as follows:

- interference with rights under Art. 8 to the Convention is proportionate where the state has a legitimate interest, such as prevention of serious crime for a short period (3 months), and where it affects only the person of interest,[82]
- random secret surveillance by intelligence agencies with blanket access to mass data is considered a serious interference with rights under Article 8 to the Convention,[83]
- national legislation deploying advanced anti-terrorism technologies is considered a legitimate aim, but the lack of legal measures to prevent blanket data access by the security agencies is considered an interference with the rights under Article 8 to the Convention,[84]
- national court's decision permitting blanket interception of communication for a period of one and a half month is considered a violation of Article 8 (and Article 13) to the Convention.[85,86]

A more recent case, *Volodina v. Russia*,[87] concerned the state's obligation to protect the applicant from cyber violence, including the nonconsensual publication of her intimate photographs, stalking and impersonation, and the state's obligation to conduct an effective investigation into such acts. The applicant, a Russian national and resident,[88] claimed that the Russian authorities failed to protect her from repeated acts of cyber harassment. In particular, she claimed that her ex-partner

---

75 See: *Centrum för Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021.

76 *Szabó and Vissy v Hungary*, App. No. 37138/14, Judgment, 12 January 2016.

77 *Roman Zakharov v Russia*, Application No. 47143/06, Judgment, 4 December 2015.

78 *Uzun v Germany*, Application No. 35623/05, Judgment, 2 September 2010.

79 *Iordachi and Others v Moldova*, Application No. 25198/02, Judgment, 10 February 2009.

80 *Dumitru Popescu v Romania,* Application No. 71525/01 (No. 2), Judgment [2007].

81 Zalnieriute, *op. cit.,* note 75, pp. 587-588.

82 *Uzun v Germany*, *op. cit.*, note 78.

83 Zakharov, *op. cit.*, note 77.

84 *Szabó and Vissy v Hungary*, *op. cit.,* note 76.

85 *Mustafa Sezgin Tanrıkulu v Turkey*, Appliaction No. 27473/06, Judgment, 18 July 2017.

86 See: Syed, *op.cit.,* note 51, p. 166.

87 *Volodina v Russia*, Application No. 40419/19 (No. 2), Judgment, 14 September 2021.

88 In 2018, fearing for her safety, the applicant obtained a legal change of name. Her old name is used in the judgment to protect her safety.

impersonated her and used intimate photos to create fake profiles on social networks, put a GPS tracker in her purse, sent death threats via social media, and that the authorities did not effectively investigate her allegations.

Particularly interesting here is that the violation of the applicant's privacy (i.e., personal data) was not committed by the state, but by an individual (the applicant's ex-partner). The ECtHR found that Russian authorities violated Article 8 of the Convention in failing to fulfill their obligations under that provision to protect the applicant from serious abuse. In essence, the court took the view that, despite having mechanisms to prosecute the applicant's ex-partner, the authorities failed to conduct an effective investigation and identify and employ mechanisms to protect the applicant from repeated online harassment.[89]

4.2. Case-law of the CJEU

A search of the CJEU case-law by the terms 'data protection' and 'cybersecurity returns only two cases: *Schrems*[90] and *Natsionalna agentsia za prihodite*.[91] The latter is in proceedings before the CJEU after having been referred for a preliminary ruling. A search by the term 'cyber space' instead of 'cybersecurity' returns zero matches. Replacing the term 'cybersecurity' with the term 'national security' returns a significantly larger number of matches: 142, including the two abovementioned cases. This supports the above premise that for a long time the EU legislator, and consequently the CJEU, viewed cybersecurity through the lens of national security as only one of its elements. To draw conclusions from a sufficiently large sample pool, this paper will turn to analyzing the recent cases concerning the protection of personal data, which the CJEU examines through the lens of national security, but that by their nature concern cybersecurity. The cases in which the CJEU decided on the protection of personal data were referred to the CJEU by national courts. Important to note here is that – unlike the ECtHR – the CJEU has limited jurisdiction in the area of member states' security policy.[92,93] To begin our analysis, we first turn to the indispensable *Schrems*.

---

89 See the comment on the judgment and its importance for fighting violence against woman: *Centre for Women, Peace and Security*, [https://blogs.lse.ac.uk/vaw/landmark-cases/a-z-of-cases/volodina-v-russia-2019], Accessed 29 December 2022.

90 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd* [2020] ECLI:EU:C:2020:559.

91 Case C-340/21 *Natsionalna agentsia za prihodite* (in proceedings).

92 See Art. 2(4) TFEU and Art. 72 TFEU.

93 Syed, *op.cit.*, note 51, p. 160.

In *Schrems*,[94] the CJEU was requested a preliminary ruling in the matter of the transfer of personal data for commercial purposes by a private company in an EU member state to a private company in a third country.[95] With its Decision 2010/87/EU, the Commission established standard contractual clauses for personal data transfer to third-country processors. *Schrems* concerns the validity of Decision 2010/87/EU. Regarding the request for judicial protection, the CJEU ruled that, contrary to Commission Decision 2016/1250, the ombudsperson mechanism provided for in the decision does not guarantee individuals a legal remedy before a body that offers protective measures essentially equivalent to those required by EU law, which could ensure both the independence of the mechanism-provided ombudsperson and the existence of rules enabling said ombudsperson to make decisions binding on the US intelligence services. For these reasons, the CJEU invalidated Commission Decision no. 2016/1250.[96]

In *Digital Ireland*,[97] the CJEU found that, in accordance with Directive 2006/24/EC[98] (Data Retention Directive), the rights under Articles 7 and 8 of the Charter are not absolute and that state interference is justifiable if it serves legitimate objectives such as combatting serious crime and international terrorism. However, the CJEU, after carrying out the proportionality test, invalidated Directive 2006/24/EC on grounds that it "did not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter." Further, the CJEU found that "it must therefore be held that Directive 2006/24/EC entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an in-

94 *Schrems, op. cit.,* note 90.

95 Maximillian Schrems, an Austrian national residing in Austria, had been a Facebook user since 2008. As with other EU residents, Mr. Schrems' personal data was transferred by Facebook Ireland in whole or in part to servers belonging to Facebook Inc. that are located on USA territory, where the data were also processed. Mr. Schrems submitted an application to the Irish supervisory authority essentially asking for a ban on those transfers. He claimed that the law and practices in the US do not guarantee a sufficient level of protection against access by public authorities to data transferred to that country. The application was rejected, inter alia, on grounds of Commission Decision 2000/5205 (Safe Harbor Decision) under which the US provides an adequate level of protection.

96 Schrems, *op. cit.,* note 90, paras. 197-202. See also: Press release of the CJEU No 91/20, Luxembourg, 16 July 2020.

97 See Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238.

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

terference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[99]

In one of the most recent cases, *Ligue des droits humains*,[100] the CJEU had the opportunity to rule on the validity of the EU Directive on Passenger Name Record (PNR) data.[101] Also called a booking file, PNR is reservation data pertaining to an individual or groups of travelers stored by airlines in their reservation and departure control databases. Under the PNR Directive, airlines are to transfer passenger data on flights to and from the EU to the passenger information department of the member state of destination or departure for the purpose of combating terrorism and serious crime. These data are stored for the potential subsequent assessment carried out by the competent authorities of the respective or other member state. The Belgian Ligue des droits humains filed a petition to the Belgian Constitutional Court for the annulment of the Belgian Act transposing the PNR Directive into Belgian law. The CJEU was requested a preliminary ruling in the matter of the validity and interpretation of the PNR Directive and the applicability of the GDPR.

The CJEU found that the PNR Directive clearly and seriously interferes with the rights guaranteed in Articles 7 and 8 of the Charter, in that it, inter alia, seeks to implement a continuous, untargeted and systematic surveillance regime, including the automated assessment of all airline passengers' personal data.[102] Although the CJEU validated the PNR Directive, in interpreting certain provisions of the Directive, it also set up fences around its application. A discussion of them would go beyond the scope of this work, but they are nonetheless worth referring to.[103]

In *Planet49*,[104] the CJEU interpreted the term 'consent' as defined under the Privacy and Electronic Communications Directive,[105] in conjunction with the Data

---

99 *Digital Ireland*, *op. cit.,* note 97, par. 65.

100 Case C-817/19 *Ligue des droits humains v Conseil des ministre* [2022] ECLI:EU:C:2022:491. The case was decided on 21 June 2022.

101 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJL 119.

102 See: *Ligue des droits humains*, *op.cit.,* note 100, par. 111.

103 *Ibid.,* see e.g. paras. 129, 157, 168, etc. For more details see: Press release of the CJEU No 105/22, Luxembourg, 21 June 2022.

104 Case C-673/17 *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* [2019] ECLI:EU:C:2019:801.

105 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337.

Protection Directive[106] and the GDPR. [107] The German Federation of Consumer Organizations contested before the German courts the German company Planet49's use of pre-ticked checkboxes in the company's promotional lottery for obtaining participants' consent for the setting of cookies whose purpose was data collection for Planet49's product advertising partner.

The CJEU found that the consent to store or access data through cookies installed on the website user's devices is invalid if given using a pre-ticked checkbox, regardless of whether the data in question is of a personal nature. Furthermore, the CJEU ruled that the service provider failed to inform the website user of the cookies' duration and any third parties' access to the cookies. The Court also took the view that Article 5(3) of the Privacy and Electronic Communications Directive is aimed at protecting users from invasion of privacy, regardless of whether the invasion targets personal data. It follows that 'consent' should not be interpreted differently if the data stored or viewed on the website user's devices is personal data.[108] Namely, EU law seeks to protect the user from any invasion of privacy, regardless of whether the data stored or viewed on the user's devices is personal data.[109]

5. CONCLUDING REMARKS

In these times of globalization and digitalization, the private lives of individuals are exposed to the public and privacy threats more than ever before. Firstly, the modern way of life increasingly requires the sharing of personal data (e.g. online shopping). Secondly, technology has enabled the creation of large databases of personal data, as well as their storage, connection and sharing. Thirdly, no longer is the state the only one encroaching on private data; large corporations and other entities are increasingly becoming party to it.[110]

With the digital economy's growth, companies are also collecting large amounts of customer data and analyzing them to learn about their habits and target them bet-

---

106 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281.

107 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) [2016] OJ L 119.

108 *Planet49*, *op.cit.,* note 104, paras. 63, 69 and 81.

109 See more in: Press release of the CJEU No 125/19, Luxembourg, 1 October 2019.

110 Schünemann; Baumann, *op. cit.,* note 4, pp. 190-193.

ter, and ultimately generate greater profit.[111] Personal data may also be breached by other individuals for a number of reasons.[112]

Clear from the above is the urgent need to protect the privacy of individuals, especially their personal data – an impossible feat without a sound legislative framework. Not to be overlooked is the national and EU courts' key role in personal data and privacy protection. In this demanding task, the courts must balance the right of individuals to personal data protection and privacy with other legitimate interests, such as national security.

For a long time, cybersecurity was associated with national security, with disregard of what 'secure' Internet means for individual users. It is safe to say that cybersecurity was angled more toward system(s) than individuals, i.e., system users. The 2019 EU Cybersecurity Act and subsequent legislation represent a normative shift in our conception of data ownership in the context of cybersecurity, putting the reins of personal information in the hands of the user instead of the service provider. Unfortunately, the positive legislative shifts at the EU level have yet to be implemented in a greater measure in the CJEU's practice and case-law.

As Brown puts it, it indeed is time to treat cybersecurity as a human rights issue.[113] But is it not also time for the ECtHR to consider cybersecurity as a human right *per se*– as a right to free and secure Internet for individuals*?* If so, at issue would then – instead of the protection of personal data in the context of cybersecurity – be two complementary autonomous human rights. Being a "living instrument" that the Convention is leaves room for the ECtHR to align its approach with the above proposal. Regrettably, as the analysis of its case-law has shown, the ECtHR still takes the traditional approach: human rights vs. national security/cybersecurity.

The differing case-law of the two European courts (ECtHR and CJEU) is in particular opposition to the protection of individuals' personal data in the context of cybersecurity. To exemplify, the ECtHR decision in *Big Brother Watch* is the first decision in which the court had the opportunity to rule on the legality of the international sharing of collected data. The ECtHR's approach to it is in complete contrast to the CJEU's position, which underlines the data-receiving third coun-

---

111 Schünemann; Baumann, *op. cit.*, note 4, p. 3. See also: Savin, A. (ed.), *EU Internet Law*, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2013, pp. 190-218.

112 Savin, *op. cit.,* note 111, p. 191. See case *Volodina v. Russia*, *op. cit.,* note 87, where the infringement on personal data in nature was committed by the applicant's ex-partner.

113 Brown, D., *It's Time to Treat Cybersecurity as a Human Rights Issue,* Human Rights Watch, 2020, [https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue], Accessed 5 January 2023.

tries' protective measures. Specifically, in *Schrems II*,[114] the CJEU annulled the so-called EU-US Privacy Shield[115] agreement that enabled transatlantic data transfers between the two countries that was in line with EU data protection requirements (the US surveillance system lacked adequate protective measures). The only difference between *Big Brother Watch* and *Schrems* is that the UK requested data from a third country, and not supply it. It remains unclear whether the ECtHR requires that adequate safeguards be in place in the receiving third country with which a Charter-contracting state shared the data. Per Zalnieriute, this ECtHR approach is ultimately reductive and dutiful, and angled at procedural safeguards more so than on the substantive legality or the actual effectiveness of the regime.[116]

The relation of the CJEU and the ECtHR has remained unchanged. In earlier research, the present authors found that the relationship of the two courts has been an oscillating one. The CJEU initially protected human rights as general principles of law, while referring to the ECtHR's case-law. Following the entry into force of the Charter, in a reasonably rational move, the CJEU began giving it precedence. This, however, began creating a schism between the two courts' positions. Their differing practices fail the reinforcing of human rights protection in the EU and complicate matters for the national (constitutional) courts. Additionally, the two courts refer to the case-law of the other only when it supports their own position.[117] It follows that the personal data protection standards of the EU are higher than those of the Council of Europe, i.e., that the scope of data protection in the case-law of the CJEU's is broader than that of the ECtHR.[118]

REFERENCES

BOOKS AND ARTICLES

1. Cherubini, F., *The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View of the Accession*, German Law Journal, Vol. 16, No. 6, 2015, pp. 1375-1386
2. Christou, G., *Cybersecurity in the European Union*, Palgrave Macmillan, London, 2016, pp. 87-118

---

114 Case C-311/18 *Schrems*, *op. cit.,* note 90.

115 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (notified under document C/2016/4176) [2016] OJ L 207.

116 Zalnieriute, M., *Big Brother Watch and Others v. the United Kingdom*, Am J Int L, 116(3), 2022, p. 589.

117 Petrašević; Duić, *op.cit.*, note 16, p. 228-229.

118 As found in the present authors' previous research, and the present analysis confirmed. See: Duić; Petrašević, *op. cit.,* note 16, p. 229.

3. Duić, D., *Common Security and Defence Policy and Cyber Defence*, in: Brill, A.; Misheva, K.; Hadji-Janev, M. (eds.), Toward Effective Cyber Defense in Accordance with the Rules of Law, IOS Press, Amsterdam, 2020, pp. 32-42
4. Duić, D., *The EEAS as a Navigator of EU Defence Aspects in Cyberspace*, European Foreign Affairs Review, Vol. 26, No. 1, 2021, pp. 101-114
5. Jakir, V., *Human Rights – With or without the internal market*, Zagreb, 2012, master thesis.
6. Kokott, J., Sobotta, C., *The Distinction between Privacy and Data Protection,* International Data Privacy Law, Vol. 3, No. 4, 2013, pp. 222-228
7. Lazowski, A.; Wessel, R.A., *When Caveats Turn into Locks: Opinion 2/13 on Accession of the European Union to the ECHR*, German Law Journal, Vol. 16, No. 1, 2015, pp. 179 – 212
8. Omejec, J., *Konvencija za zaštitu ljudskih prava i temeljnih sloboda u praksi Europskog suda za ljudska prava*, Novi informator, Zagreb, 2013
9. Pavlova, P., *Human Rights-based Approach to Cybersecurity: Addressing the Security Risks of Targeted Groups*, Peace Human Rights Governance, Vol. 4, No. 3, 2020, pp. 391-418
10. Petrašević, T., Duić, D., *Direktiva o evidenciji podataka o putnicima (PNR) i zaštita podataka u EU,* in: Vukosav, J.; Butorac, K.; Sindik, J. (eds.), Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda, MUP, Policijska akademija, Zagreb, 2016, pp. 638-652
11. Petrašević, T., Poretti, P., *Pravo na suđenje u razumnom roku – postoji li (nova) praksa Suda Europske unije?*, Harmonius - Journal of Legal and Social Studies in south East Europe, Vol. 7, No. 1, 2018, pp. 187-199
12. Petrašević, T., *The relation of Human Rights and market freedoms in case law of the CJEU*, in: Primorac, Ž. ; Bussoli, C. ; Recker, N. (eds.), Economic and Social Development: 16th International Scientific Conference on Economic and Social Development "The Legal Challenges of Modern World", Varaždin/Split, 2016, pp. 142-150
13. Petrašević, T.; Duić, D., *Opinion 2/13 on the EU accession to the ECHR*, in: Vinković, M. (ed.), New Developments in the EU Labour, Equality and Human Rights Law, J. J. Strossmayer University of Osijek, Faculty of Law, Osijek, 2015, pp. 251-267
14. Petrašević, T.; Duić, D., *Standards of Human Rights Protection in the Domain of Personal Data Protection: Strasburg vs Luxemburg*, in: Sander, G. G.; Poščić, A.; Martinović, A. (eds.), Exploring the Social Dimension of Europe- Essays in Honour of Nada Bodiroga-Vukobrat, Verlag Dr. Kovač, Hamburg, 2021, pp. 215-231
15. Petrašević, T.; Kovačić Markić, L., *Položaj nacionalnih ustavnih sudova u primjeni mehanizma prethodnog postupka s posebnim osvrtom na Ustavni sud Republike Hrvatske*, in: Bačić, A. (ed.), Pravo i politika EU: stara pitanja, novi odgovori, HAZU, Zagreb, 2020, pp. 143-176
16. Savin, A. (ed.), *EU Internet Law*, Edward Elgar Publishing, Cheltenham, UK, Northampton, MA, USA, 2013
17. Schünemann, W., Baumann, MO. (eds) *Privacy, Data Protection and Cybersecurity in Europe*, Springer, Cham, 2017
18. Syed, H., *Data protection rights & national security objectives: critical analysis of ECtHR and CJEU case law*, Nor. Am. Aca. Res., Vol. 2, No. 3, 2019, pp. 155-170

19. Wiśniewski, A., *The European Court of Human Rights and Internet-Related* Cases, Bialystok Legal Studies, Vol. 26, No. 3, 2021, pp. 109-133
20. Zalnieriute, M., *Big Brother Watch and Others v. the United Kingdom*, American Journal of International Law, Vol. 116, No. 3, 2022, pp. 585-592

COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd [2020] ECLI:EU:C:2020:559
2. Case C-293/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238
3. Case C-817/19 Ligue des droits humains v Conseil des ministre [2022] ECLI:EU:C:2022:491
4. Case C-340/21 Natsionalna agentsia za prihodite (in proceedings)
5. Case C-673/17 Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV [2019] ECLI:EU:C:2019:801
6. Press release of the CJEU No 125/19, Luxembourg, 1 October 2019
7. Press release of the CJEU No 91/20, Luxembourg, 16 July 2020
8. Press release of the CJEU No 105/22, Luxembourg, 21 June 2022

ECHR

1. *Guide to the Case-Law of the European Court of Human Rights: Data protection*, Council of Europe / European Court of Human Rights, 2022 (Updated on 31 August 2022)

Decisions:

1. *Airey v Ireland,* Application No. 6289/73, Judgment, 9 October 1979
2. *Big Brother Watch and Others v the United Kingdom,* Application Nos. 58170/13, 62322/14, 24960/15, Judgment, 13/09/2018; and *Big Brother Watch and Others v the United Kingdom,* Application Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment, 25 May 2021
3. *Cengiz and Others v Turkey,* Application Nos. 48226/10, 14027/112015, Judgment, 1 December 2015
4. *Centrum för Rättvisa v Sweden*, Application No. 35252/08, Judgment, 25 May 2021
5. *Delfi AS v Estonia,* Application No. 64569/09, Judgment, 16 June 2015
6. *Demir and Baykara v Turkey,* Application No. 34503/97, Judgment, 12 November 2008
7. *Dumitru Popescu v Romania,* Application No. 71525/01 (No. 2), Judgment [2007]
8. *Iordachi and Others v Moldova,* Application No. 25198/02, Judgment, 10 February 2009
9. *K.U. v Finland*, Application No. 2872/02, Judgment, 2 December 2008
10. *Klass and Others v Germany,* Application No. 5029/71, Judgment, 6 September 1978
11. *Liberty and Others v the United Kingdom,* Application No. 58243/00, Judgment, 1 July 2008

12. *Weber and Saravia v Germany,* Application No. 54934/00, Decision, 29 June 2006
13. *Youth Initiative for Human Rights v Serbia,* Application No. 48135/06, Judgment, 25 June 2013
14. *Mustafa Sezgin Tanrıkulu v Turkey,* Appliaction No. 27473/06, Judgment, 18 July 2017
15. *Roman Zakharov v Russia,* Application No. 47143/06, Judgment, 4 December 2015
16. *S. Marper v the United Kingdom,* Application Nos. 30562/04 and 30566/04, Judgment, 4 December 2008
17. *Szabó and Vissy v Hungary* App. No. 37138/14, Judgment, 12 January 2016
18. *Uzun v Germany,* Application No. 35623/05, Judgment, 2 September 2010
19. *Volodina v Russia,* Application No. 40419/19 (No. 2), Judgment, 14 September 2021

EU LAW

1. A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security [2022] 7371/22
2. Charter of Fundamental Rights of the European Union [2012] OJ C 326
3. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield (notified under document C/2016/4176) [2016] OJ L 207
4. Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States [2019] OJ L 129I
5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, [2013] JOIN(2013) 1 final
6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L 337
8. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105
9. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJL 119

10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194
11. Joint communication to the European parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN/2020/18 final
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation) [2016] OJ L 119
13. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L 151
14. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT [2021] OJ L 202
15. Treaty on the Functioning of the European Union (Consolidated version) [2016] OJ C 202

COUNCIL OF EUROPE

1. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) [2003]
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [1981]
3. Convention on Cybercrime (ETS No. 185) [2001]

UNITED NATIONS

1. United Nations, *General Assembly backs right to privacy in digital age,* [https://news.un.org/en/story/2013/12/458232], Accessed 30 December 2022
2. United Nations, High Commissioner for Human Rights, *The right to privacy in the digital age*, [https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age], Accessed 30 December 2022
3. United Nations, General Assembly, Resolution A/RES/68/167 on the right to privacy in the digital age, 18 December 2013
4. United Nations, High Commissioner for Human Rights, Resolution A/HRC/RES/32/13 on the promotion, protection and enjoyment of human rights on the Internet, 18 July 2016

WEBSITE REFERENCES

1. Freedom Online Coalition, *Aims and Priorities*, [https://freedomonlinecoalition.com/aims-and-priorities/], Accessed 25 November 2022

2. Brown, D., *It's Time to Treat Cybersecurity as a Human Rights Issue,* Human Rights Watch, 2020, [https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue], Accessed 5 January 2023
3. Centre for Woman, Peace and Security, [https://blogs.lse.ac.uk/vaw/landmark-cases/a-z-of-cases/volodina-v-russia-2019], Accessed 29 December 2022
4. Council of Europe, *Action against Cybercrime*, 2023, [https://www.coe.int/en/web/cybercrime], Accessed 5 January 2023
5. Council of the EU, *Cyber-attacks: Council extends sanctions regime until 18 May 2025*, 2022, [https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/cyber-attacks-council-extends-sanctions-regime-until-18-may-2025], Accessed 5 January 2023
6. Douglas-Scott, S., *Opinion 2/13 on EU Accession to the ECHR*: *A Christmas Bombshell From the European Court of Justice*, U.K. Const. L. Blog, [http://ukconstitutionallaw.org], Accessed 30 December 2022
7. ENISA - European Union Agency for Cybersecurity, *About*, [https://www.enisa.europa.eu/about-enisa/about/], Accessed 5 January 2023
8. European Commission, *Building strong cybersecurity – Brochure*, 2019, [https://digital-strategy.ec.europa.eu/en/node/1500/printable/pdf], Accessed 5 January 2023
9. Gotev, G., *Court of Justice rejects draft agreement of EU accession to* ECHR, Euractiv, [http://www.euractiv.com/sections/eu-priorities-2020/court-justice-rejects-draft-agreement-eu-accession-echr-310983], Accessed 30 December 2022
10. Peers, S., *The CJEU and the EU's Accession to the ECHR: A Clear and Present Danger to Human Rights Protection*, EU L. Analysis Blog, [http://eulawanalysis.blogspot.com.es/2014/12/the-cjeu-and-eus-accession-to-echr.html], Accessed 30 December 2022
11. Puddephatt, A.; Kaspar, L., *Cybersecurity is the new battleground for human rights,* Open-Democracy, 2015, [https://www.opendemocracy.net/en/cybersecurity-is-new-battleground-for-human-rights/], Accessed 25 November 2022
12. *What is cybersecurity?*, [https://support.microsoft.com/en-us/topic/what-is-cybersecurity-8b6efd59-41ff-4743-87c8-0850a352a390], Accessed 25 November 2022
13. Freedom Online Coalition, *Why Do We Need a New Definition for Cybersecurity?*, [https://freedomonlinecoalition.com/blog/why-do-we-need-a-new-definition-for-cybersecurity], Accessed 25 November 2022