Law, Governance and Technology Series 45
Issues in Privacy and Data Protection

Marek Zubik
Jan Podkowik
Robert Rybski *Editors*

European Constitutional Courts towards Data Retention Laws

Springer

Law, Governance and Technology Series

Issues in Privacy and Data Protection

Volume 45

Issues in Privacy and Data Protection aims at publishing peer reviewed scientific manuscripts that focus upon issues that engage into an analysis or reflexion related to the consequences of scientific and technological developments upon the private sphere, the personal autonomy and the self-construction of humans with data protection and privacy as anchor points. The objective is to publish both disciplinary, multidisciplinary and interdisciplinary works on questions that relate to experiences and phenomena that can or could be covered by legal concepts stemming from the law regarding the protection of privacy and/or the processing of personal data. Since both the development of science and technology, and in particular information technology (ambient intelligence, robotics, artificial intelligence, knowledge discovery, data mining, surveillance, etc.), and the law on privacy and data protection are in constant frenetic mood of change (as is clear from the many legal conflicts and reforms at hand), we have the ambition to reassemble a series of highly contemporary and forward-looking books, wherein cutting edge issues are analytically, conceptually and prospectively presented.

More information about this subseries at http://www.springer.com/series/13087

Marek Zubik • Jan Podkowik • Robert Rybski
Editors

European Constitutional Courts towards Data Retention Laws

Springer

Editors
Marek Zubik
Department of Constitutional Law, Faculty of Law and Administration
University of Warsaw
Warsaw, Poland

Jan Podkowik
Department of Constitutional Law, Faculty of Law and Administration
University of Warsaw
Warsaw, Poland

Robert Rybski
Department of Constitutional Law, Faculty of Law and Administration
University of Warsaw
Warsaw, Poland

ISSN 2352-1902 ISSN 2352-1910 (electronic)
Law, Governance and Technology Series
ISSN 2352-1929 ISSN 2352-1937 (electronic)
Issues in Privacy and Data Protection
ISBN 978-3-030-57188-7 ISBN 978-3-030-57189-4 (eBook)
https://doi.org/10.1007/978-3-030-57189-4

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

About This Book

The turn of the century brought a revolution within the scope of information exchange. Since then the space for the possibilities of human functioning and shaping interpersonal relations has expanded visibly. Means of distance communication have become widespread. All these phenomena are undoubtedly connected to the development of civilisation and technology, as well as the reduction of costs of participation in the global flow of information. It is hard to deny that these changes have increased the possibilities of exchanging thoughts, views, and ensuring the transparency of public life and social control of public authorities, the provision of public services, the purchase of goods and services, and the development of scientific research. They have also brought new opportunities to ensure the safety of people and their property, enabling the monitoring of people and places or their electronic supervision, thanks to which—regardless of some random events—even geographical location is possible.

Increasingly sophisticated technologies seem to have diminished citizens' awareness of the effects of their exertion. Our dependence on technical devices, various types of applications and social forums, as well as the specialists who support them have extremely increased. Moreover, technically advanced mechanisms incur the risk of the phenomenon of civilisation exclusion of social groups which are not prepared for the use of new civilisation inventions. It can be also sometimes noticed—not without connection to fears of losing control over one's privacy, the way of living, or more broadly one's freedom—a phenomenon of a conscious abandonment of the pursuit of modernity.

Human privacy has now undoubtedly become a commodity desired by various entities or corporations of a private nature. More or less consciously, citizens have begun to pay for their participation in cyber reality. The protection of privacy and freedom from advertising or profiling has become a luxury, for which one just has to pay money. Cyberspace has also become a place of rivalry between states and international non-state creations, or even a subject of an impact on social life in other countries.

Not only do new technologies give public authorities new forms and ways to perform their functions, but they also create the opportunity to interfere in the privacy of their citizens. They can be used for a very broad acquisition of knowledge about the behaviour of citizens which is beyond an effective social control. This also refers to the content and forms of provided information, as well as the processing of these data and their subsequent use.

However, technological changes have not changed the human nature, which has got its darker sides, too. New technologies make it also easier for people who violate the law to contact each other. The increasing availability of means of communication increases the risk of using them to commit crimes or trespass. On the one hand, technological development has led to the emergence of new forms of committing 'traditional' crimes. The Internet and means of distance communication are to become a new, specialised tool in the hands of criminals, existing somehow parallel to the techniques having been in use so far. On the other hand, some new, previously non-existent types of crimes have emerged which can be committed only by using new technologies (the so-called cybercrime).

The awareness of the expansion of the area of freedom and citizens' activity and the emergence of new threats have forced public authorities to react. The process of incorporating new technologies into public decision-making procedures has begun, giving the citizens new opportunities for social participation. Legal problems related to the spread of new forms of communication go far beyond the issue of processing subscribers' telecommunication data by private operators and then the acquisition of such data by public authorities. It is necessary to consider in which way new forms of communication and the conclusion of various types of contracts may have a reference to the existing legal culture. The key question is whether we are dealing with completely new manifestations of human freedom, including freedom of contract, or whether these are typical activities but carried out in virtual reality. Key problems have arisen, such as the question about the place and time of the conclusion of contract, sufficient consumer knowledge about a product, the risk of using electronic means to conclude a contract, the use of new value media (cyber money), or how to protect effectively sensitive information, especially regarding human health and other forms of privacy, and not to lead to new discrimination phenomena against this background. It is necessary to introduce new legal solutions, civilising legal transactions with the usage of new technologies. After the first period of enthusiasm, when it seemed that the new media would bring only positive effects, also for democratic life of open societies, the original optimism has already worn out. As social media have become more widespread, the realism about the existence of their harmful face has also increased. Political discussions mainly among anonymous strangers have turned out to be often more emotional and less respectful towards people having different views than such discussions carried on in the real world; extreme views can spread more widely and rapidly; disinformation campaigns have appeared, denying more than once scientific evidence, etc.

These general observations already show the scale of problems and challenges democratic legislators have to face. It appears therefore a very significant problem. It has become the key issue to this publication. Namely, the question has to be

answered how to set limits for the interference of public authorities in the framework of the use of new technologies by citizens, including in cyberspace. It has been quickly realised that one needs to search for the possibly widest recognised standards. However, cyberspace is poorly prone to modalities set by political boundaries. Freedom of communication exists and is protected by public authorities, and the state interference in this sphere respects the general principles of limiting freedom allowed in a democratic state or the state uses cyberspace for social manipulation. Conversely, maintaining general, democratic standards for the protection of human dignity and human freedoms and rights must be at some point met with the need to maintain public security or to protect the freedoms and rights of others. The use of modern technologies in the course of terrorist attacks has shown how urgent it will be to determine the appropriate limits for the gathering and processing data created while using modern forms of communication by citizens. An open question is also the issue of the need to ensure a proper education so as not only to prevent the already mentioned phenomenon of civilisation exclusion among various social groups, but also to show sufficiently the threats and challenges which users usually face when using new channels of communication.

We have never had any doubts that the issue of legal regulations regarding the consolidation and use of telecommunication data is socially significant. The book is the result of work of a number of lawyers from different countries and at least in two dimensions. The first one—and the most obvious—the studies have been written and developed by lawyers. The second dimension—but not less important—court rulings and their justifications were also made as a part of the judicial service of lawyers. All these elements—legal norms, court rulings, and statements of the law literature—reflect the legal framework of freedom of communication in the digital age.

In the book, we have tried to capture the essence of the development of legal thought on the subject of the legal mechanism adopted in European Union countries, which are also members of the Council of Europe. This mechanism consisted of the legal obligation of private telecommunication network operators to record information about the communication of their customers, excluding the content of messages, and it also sets the legal framework for the acquisition and use of this information by public authorities. Legal solutions adopted at the level of the European Union and in particular member states have quickly begun to be questioned. Matters related to them have ended up on the agenda of the national constitutional courts and the Court of Justice of the European Union itself. The longer they have been in force, the more doubts have been growing about the compliance of these regulations with human rights and the rule of law.

The undoubted turning point for the existence of joint solutions regarding the consolidation and acquisition of telecommunication data by public authorities was the judgement of the CJEU of 8 April 2014 in case of Digital Rights Ireland, which annulled the directive 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. Nonetheless, we put forward the thesis that the CJEU's approach to

such a decision would not be so obvious if it were not preceded by a series of judgements of the ECtHR related to the protection of privacy in the digital age, and in particular the judgements of the national constitutional courts proclaiming the unconstitutionality of provisions implementing this directive. The general social reluctance to the excessive interference of public authorities in the cyberspace has certainly also been not without any significance for these decisions.

The book we give to the reader consists of two parts: One of them is an attempt to capture the basic way of seeing standards for the protection of individual freedoms and rights and balancing it with ensuring public safety by the national supreme judicial authorities of the EU countries in which constitutional courts or supreme courts ruled on the provisions regulating the mechanism of telecommunication data consolidation. This is presented in studies written by lawyers from particular countries. The second part constitutes an attempt to reconstruct the common European standard for the protection of freedom of communication in the digital era, as well as to show how the exchange of thoughts and views between national courts, the ECtHR, and the CJEU has taken place. One could say, it is a practical exemplification of the phenomenon that is referred to as 'judicial dialogue'.

The publication can undoubtedly serve as a source of information for those who want to acquire knowledge about legal solutions in force in several countries and about particular court decisions made towards them. The reader can learn the history regarding the assessment of national provisions on the collection of telecommunication data and their use by public authorities. At the end of the book, there are extensive fragments of judgements, which should enable the reader to refer to the source of the case-law (not only for the analytical study itself). Particular studies, however, are not focused on the mere analysis and assessment of judgements, but rather on the search for a common standard for the protection of freedom of communication within a common area of the European legal culture while preserving the constitutional achievements of particular member states.

We have tried to find the actual shape of emerging constitutional and international standards for the protection of freedom of communication in the aspect of telecommunication data retention and processing. Largely devoted to the latter issue is the last study, which is our summary of analyses focused on particular countries and the jurisprudence of the ECtHR and the CJEU. Professor dr. habil. Marek Zubik (retired judge of Poland's Constitutional Tribunal), dr. habil. Jan Podkowik and dr. Robert Rybski.

We are aware that the publication shows the state of development of legal thought at some historical point. Whether the outlined development will persist or collapse over some time, it depends on many factors, not only legal ones. This thesis can be only verified in the future. We hope, however, that the book could serve as a valuable help in further scientific research conducted on both standards for the protection of freedom of communication, as well as cooperation and judicial dialogue in the best way.

The book has been composed as a part of the project "Impact of jurisprudence of European constitutional courts and of the Court of Justice of European Union on forming universal content of freedom of communications in Europe in the era of technological development" conducted at the Faculty of Law and Administration of the University of Warsaw, financed by the National Science Centre in Poland (project No. 2015/17/B/HS5/01408).

Contents

Part I
Data Retention in Europe

Data Retention in the European Union

Barbara Grabowska-Moroz

Abstract Global security challenges after the 9/11 terrorist attacks have revolutionised national approaches on the fight against public security threats. The broad and open-ended concept of terrorism has allowed national legislatures to adopt extraordinary measures to face these undefined threats. Their impact on human rights (personal freedom, freedom of movement, right of privacy, freedom of information) has led to the development of case law, which is aimed at balancing safeguards against unknown threats and the belief that human rights remain binding. One of such security measures—the retention of telecommunication data—was harmonised by the European Union in 2006. Since then it has been one of the most vividly discussed topics in European law involving both political and business issues. This paper aims at analysing the judicial debate held by the Court of Justice of the European Union on the constitutional and international limits of the Data Retention Directive (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.).

1 Data Retention Directive: Scope, Aim, Consequences

The European Commission proposed a Directive on data retention[1] in September 2005, two months after the London bombings. Despite the lack of unequivocal competence in the field of national security, the European Union decided to regulate this issue as an internal market matter. The proposal noted that different retention

[1]Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC {SEC(2005) 1131}.

B. Grabowska-Moroz (✉)
University of Groningen, Groningen, The Netherlands

M. Zubik et al. (eds.), *European Constitutional Courts towards Data Retention Laws*, Law, Governance and Technology Series 45,
https://doi.org/10.1007/978-3-030-57189-4_1

requirements binding in Member States could constitute obstacles to the internal market for electronic communication and therefore needed to be harmonised. However, the European Commission argued that such differences also limited law enforcement's access to data thus impeding the fulfilment of their duties including "preventing and combating organised crime and terrorism."

The Directive was adopted in 2006 and imposed a duty of retaining telecommunication data by service providers and obliged Member States to ensure access to data by "competent national authorities."[2] The scope of the data covered by the Directive was broad and included information regarding the sources of communication; the date, time and duration of a communication; type of communication; and the location of mobile communication equipment. Specific elements of access to the retained data (e.g. procedure) were to be regulated by Member States "in accordance with necessity and proportionality requirements." It constituted a clear exemption from the general rules of data protection established in Directive 2002/58 regarding privacy and electronic communications,[3] which imposed significantly stricter limits on data protection.[4] The Data Retention Directive also constituted a challenge in light of the European Court of Human Rights (ECtHR) case law, since ECtHR required proportionate and strictly tailored measures that would protect not only public security but also respect the essence of right to confidential communication, private life and freedom of speech.[5]

The Irish government initiated the first judicial challenge of the Directive before the EU court based on the assumption that Directive 2006/24 was not appropriately and legally adopted, and that it was an internal market Directive based on Article 95 EC instead of the precedent decision adopted on Title VI of Treaty of European Union (TEU) regulating judicial cooperation and fighting crimes. Determining competence demarcation between the first and the third pillar and clarifying the appropriate body entitled to act—the Union or the Community[6]—resulted from the pre-Lisbon Treaty legal framework that currently is not as relevant as it previously was. However, focusing attention on the issues of procedure and competence instead of the merits detracted from the main arguments analysed in Advocate General Bot's opinion and the Court's ruling. Consequently, the Court found that "Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement

[2]Directive 2006/24/EC, Article 4.

[3]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.

[4]CJEU in *Tele 2/Watson* stated that "retention of traffic and location data is the rule, whereas the system put in place by Directive 2002/58 requires the retention of data to be the exception" (para. 104).

[5]Breyer (2005).

[6]Poli (2010), p. 138.

purposes."[7] Although the Court referenced the 9/11 terrorist attacks, which motivated national legislators to impose obligations on service providers regarding data retention, it analysed the EU's data retention obligations through the "internal market lens". The Court found that the Data Retention Directive regulated the retention of data and not its access or use by law enforcement.[8] For most stakeholders it was obvious that the chief aim of imposing data retention obligations mainly affects security; however, it also undoubtedly and directly affects service providers in the Member States. Nevertheless, applying an internal market approach to regulating this issue might have undermined human rights protections.[9]

In 2011, the European Commission recommended the amendment of the Data Retention Directive and regulation of data retention as a security measure and not merely as a tool harmonising the internal market.[10] The Commission also emphasised the need to strengthen personal data protection within the scheme of telecommunication data protection by shortening the periods of mandatory data retention, ensuring independent supervision of requests for data access and retention, thereby reducing the data categories to be retained.[11] The Commission directly referred to the standard established by the ECHR in the *S and Murper v. UK* ruling,[12] which balanced an individual's concerns about data collection against the public safety and security.

2 The Constitutional Road to *Digital Rights Ireland*

Ireland v. European Parliament was a first step in challenging data retention obligations; however, the challenge failed due to the Irish government's and subsequently the Court's formalist approach. Nevertheless, it was indisputable that future judicial challenges of the Directive would inevitably follow. Implementation of the Directive differed between Member States providing various mechanisms of control and different interpretations of the vague proportionality standard established by the Directive. Therefore, the Court's decision in *Ireland v. European Parliament* did not end the discussion about the Data Retention Directive.

---

[7]Judgment of 10 February 2009, *Ireland v. European Parliament and Council of the European Union*, C-301/06.

[8]Judgment of 10 February 2009, *Ireland v. European Parliament and Council of the European Union*, C-301/06, para. 80.

[9]Herlin-Karnell (2009), p. 1667.

[10]Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC) Brussels, 18.4.2011 COM(2011) 225 final, p. 31.

[11]Report from the Commission to the Council and the European Parliament – Evaluation report on the Data Retention Directive (Directive 2006/24/EC) Brussels, 18.4.2011 COM(2011) 225 final, p. 32.

[12]Judgment of 4 December 2008, applications No. 30562/04 and 30566/04.

Instead, the discussion shifted to the national level where national constitutional courts analysed the implementation of the Data Retention Directive following their national constitutions. In those cases, the courts attempted to properly balance the concerns of law enforcement against the desires of individuals residing in democratic states for data protection. Such an analysis was a new step because the Court of Justice did not analyse the merits of the directive's provisions. National constitutional reviews of data retention in light of the Directive's obligations triggered judicial dialogue between the courts.[13] It was nearly impossible for the Court of Justice of the European Union (CJEU) to ignore national constitutional reviews while adjudicating the Directive. The main arguments against the Directive's retention scheme dealt with the broad scope of retained data and their effectiveness in fighting against serious crimes (Czech Republic). However, the national constitutional courts had to also consider the relation between national and the EU law (Germany, Cyprus).

In 2014, CJEU eventually discussed the constitutional arguments in the *Digital Rights Ireland* decision.[14] Preliminary references—from both the Austrian and Irish courts—addressed whether the Directive was compatible with the human rights expressed in the EU Charter of Fundamental Rights, including the rights to privacy and protection of personal data. The Court followed the typical ECtHR approach used in cases concerning alleged violation of Article 8 European Convention on Human Rights (ECHR) and applied a three-prong proportionality test.[15] The interference with "privacy rights" (rights to privacy and protection of personal data) resulted from two elements regulated by the Directive—(1) the obligatory retention of "data relating to a person's private life and to his communications" and (2) access to data by national authorities. The Court found the interference to be a "particularly serious" one, especially due to the lack of notice, which could lead to "constant surveillance."

Nevertheless, the Court concluded that a "particularly serious interference"—meaning the fight against serious crime to maintain public security—is legitimate because "data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime."[16] However, the Court did not articulate the effectiveness of the entire legal framework for storing and using telecommunication data. It appears that when applying the balancing test, the Court did not fully consider a data retention system's legitimate purpose and failed to specifically explain it. The Court referred to neither the Commission's evaluation of 2011 nor to other sources reviewing the effectiveness of a data retention system.

[13] Vedaschi and Lubello (2015), p. 23.

[14] Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others*, C-293/12.

[15] Tracol (2014), p. 742.

[16] *Digital Rights Ireland*, para. 43.

Nevertheless, the "particularly serious interference" with an individual's right to privacy led the Court to apply a "strict" standard of review.[17] The Court expressly noted shortcomings with the following: interference to both the retention and access to data; no relation between data retention and serious crimes; overly broad data retention covering the entire European population; lack of procedural safeguards regarding access to retained data; vague and ambiguous definition of "serious crime"; and concerns regarding the safety of retained data.[18] The overall shortcomings of the Directive led to the conclusion that the Directive "has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter." Consequently, the Court found the Data Retention Directive invalid.[19]

The Court's decision in *Ireland v. European Parliament* revealed that the criminal and law enforcement concerns played a secondary role to the internal market concerns, whereas in *Digital Rights Ireland* internal market concerns were not the primary focus.[20] The Advocate General referred to the "dual function" of the Directive and stated that it was "manifestly disproportionate" with respect to the goal of internal market harmonisation.[21] Nevertheless, the *Digital Rights Ireland* decision revealed the growing importance of the EU Charter of Fundamental Rights, despite the Court's lack of a detailed legal analysis of the interference with the right to protection of personal data,[22] instead mostly referring to the right to privacy, whereas AG made clear distinction between those two rights.[23]

The Court's ruling caused to some extent legal uncertainty of national legislation implementing the Data Retention Directive. It remains clear that the EU continues regulating personal data protection via Directive 2002/58, which allows for the limitation of data protection rules.[24] Consequently, the EU Charter would apply to national laws implementing this aspect of the EU law, including national data retention schemes. Despite the set of rulings relating to data retention issued by national constitutional courts, it was the *Digital Rights Ireland* decision that was described as a "game changer" in judicial discussions about the EU data retention scheme.[25] This decision elaborated the main disadvantages of the whole data retention system.[26] For this reason, national courts have implemented this decision

[17] *Digital Rights Ireland*, para. 52.

[18] *Digital Rights Ireland*, para. 68.

[19] Advocate General suggested however to suspend the effect of Directive invalidation (para. 158).

[20] Guild and Carrera (2014), p. 7.

[21] Opinion of AG Cruz Villalon of 12 December 2013, Case C-293/12, para. 100.

[22] Tracol (2014), p. 743.

[23] AG opinion, paras. 64–65. The Court cleared it up in *Tele-2/Watson* ruling by stating that data protection does not have any equivalent in the ECHR.

[24] Rauhofer and Mac Sithigh (2014), p. 126; Boehm and Cole (2014), pp. 92–93.

[25] Rauhofer and Mac Sithigh (2014), p. 127.

[26] Rauhofer and Mac Sithigh (2014), p. 127: "the ECJ has now sharply removed the sticking plaster that up to now has held a creaking system together".

when reviewing national legislation following the Data Retention Directive.[27] Although it remains unsettled whether the European Commission would propose a new directive in this respect, it remains obvious that the new EU legal framework and national laws implementing exemption from Directive 2002/58 must meet the criteria discussed by the CJEU.[28]

3 National Legislation on Data Retention Under Scrutiny: *Tele-2/Watson* Develops the *Digital Rights Ireland* Findings

Between the two possible scenarios at the EU level[29]—legislative intervention and judicial challenge—the latter provided clarity sooner. National legislation in Sweden and in the UK was challenged before national courts, which referred their cases to the CJEU for redress of privacy questions with regard to national law.[30] The common denominator in the questions referred to CJEU in *Tele2/Watson* was whether national legislation providing mandatory telecommunication data retention was compatible with the EU law, particularly with Article 15 of Directive 2002/58 and with the Charter of Fundamental Rights (Articles 7 and 8).

Advocate General (AG) Bot's analysis was closer to the approach used by the Court in the *Digital Rights Ireland* decision.[31] The opinion underlined the need of procedural safeguards established by *Digital Rights Ireland* ruling concerning law enforcement's access to retained data rather than the broad scope of data storage by service providers.[32] The AG's analysis was described as a "pragmatic solution" because it followed an analysis similar to the one adopted in *Digital Rights Ireland.*[33] The AG concluded that the general retention of telecommunication data can be compatible with the EU law if certain criteria are met.

Instead of applying the safeguards on access to telecommunication data established in *Digital Rights Ireland*, the CJEU concentrated solely on data retention systems established by Swedish and British law.[34] The Court found that Directive 2002/58 is applicable to national legislation on mandatory data retention[35] because

[27]E.g. Slovakia, Poland, UK in *Davis* ruling of July 2015.

[28]Vedaschi and Lubello (2015), p. 30; Ojanen (2014), p. 540.

[29]Vedaschi and Lubello (2015), p. 3; Guild and Carrera (2014), pp. 13–15.

[30]*Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, C-203/15.

[31]Opinion of Advocate General Bot of 9 November 2016, case C-536/15.

[32]Opinion of Advocate General Bot of 9 November 2016, case C-536/15. para. 205.

[33]Gryffroy (2016).

[34]Judgment of the Court (Grand Chamber) of 21 December 2016, *Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*, C-203/15.

[35]*Tele2/Watson*, para. 81.

retention for combating crimes fall within Article 15 (1) of the Directive.[36] The Court found that the retention of the traffic and location data involved processing them,[37] thus Directive 2002/58 also applies to access to those data by public authorities.[38]

The Court confirmed that the "strict necessity" test is applicable to limitations of personal data protection[39] due to the nature of infringement. The Court followed the findings in *Digital Rights Ireland* that data retention obligations facilitate the precise definition of people's profiles of their private lives.[40] "Very far reaching" and "particularly serious" interference also resulted from the lack of obligatory notice, which is likely to cause a person to feel under constant surveillance.[41] The AG confirmed that the retention of a large amount of traffic and location data can be just as sensitive as access to the actual content of communications.[42] By contrast, in the case of *Digital Rights Ireland* the sensitive nature of data retention did not lead the Court to conclude that the Data Retention Directive breached the essence of individual privacy rights.[43]

According to the Court, such serious limitations of the right to privacy can be justified only by the fight against "serious crime".[44] However, this legitimate goal is not "strong" enough to justify "national legislation providing for the general and indiscriminate retention of all traffic and location data."[45] The Court stated that combatting serious crimes cannot justify indiscriminate retention,[46] otherwise it would become a general rule.[47] Another shortcoming of national regulation was the lack of any relationship between data retention and threats to public security.[48] Furthermore, there were no restrictions on time periods, geographical areas, groups of people likely to be involved or persons who could contribute to fighting crime. Consequently, the national legislation under review exceeded the limits of the "strict necessity" test and was not justified within democratic society.[49]

Nevertheless, the Court noted that Directive 2002/58 and the Charter do not prevent "targeted retention" being limited "with respect to the categories of data to

[36] *Tele2/Watson*, para 73.

[37] *Tele2/Watson*, para. 75.

[38] *Tele2/Watson*, para. 76.

[39] *Tele2/Watson*, para. 96; *Digital Rights Ireland,* para. 52.

[40] *Digital Rights Ireland*, para. 27. *Tele2/Watson*, para. 99.

[41] Interference was found to be "very far reaching" and "particularly serious" (*Tele2/Watson*, para. 100).

[42] Opinion of Advocate General Bot of 9 November 2016, para. 253.

[43] *Digital Rights Ireland*, para. 39.

[44] *Tele2/Watson*, para. 102.

[45] *Tele2/Watson*, para. 103.

[46] *Tele2/Watson*.

[47] *Tele2/Watson*, para. 104.

[48] *Tele2/Watson*, para. 106; *Digital Rights Ireland*, para. 59.

[49] *Tele2/Watson*, para. 107.

be retained, the means of communication affected, the persons concerned and the retention period adopted."[50] This approach was considered following the decision in *Digital Rights Ireland* and suggested a possible method for limiting data retention. In *Tele2/Watson* the Court specifically mentioned limitations based on geographical criterion.[51] The approaches established in these cases would allow retention of telecommunication data where the level of crime is high and there is objective evidence to confirm the scope of the area.

On the rules on access to telecommunication data, the requirements established in the *Digital Rights Ireland* decision were confirmed by the Court in *Tele2/Watson*. National legislation must establish "the substantive and procedural conditions" governing the access of competent national authorities to retained data.[52] Fulfilling those conditions shall be reviewed by independent authority.[53] Moreover, the Court clearly expressed the notification requirement after authorities receive access to data to ensure an individual's right to a legal remedy. The Court also noted the requirement of ensuring prior independent review of processing personal data based on Article 8(3) of the Charter. A court or an independent administrative body shall conduct a review into each request for data access, and each request must specify the reasons for data access for verification by the court or administrative body. The goal of data retention and access is limited only to fighting serious crimes including organised crime, terror, or those that pose serious public security threats. However, the Member State must decide which crimes are sufficiently serious to justify data retention and access.

The Court's analysis led to a conclusion that the EU law, specifically Directive 2002/58 and the EU Charter, prohibits the "general and indiscriminate retention of all traffic and location data of all subscribers." Moreover, access to such data collected based on "targeted retention" must meet the following set of requirements: the goal of data access is limited to "fighting serious crime"; data access is subject to prior review by a court and/or independent administrative authority; and the data are retained within the EU. AG clearly stated that the above requirements must be met cumulatively, whereas the Court did not directly address this issue.[54]

[50] *Tele2/Watson*, para. 108.

[51] *Tele2/Watson*, para. 111.

[52] *Tele2/Watson*, para. 118.

[53] *Tele2/Watson*, para. 120.

[54] Pederson et al. (2018), p. 10.

4 Data Retention in the European Union: Where Are We Now?

The ruling in *Tele2/Watson* inevitably constituted a new stage in the evolution of the CJEU approach on mandatory data retention. In *Digital Rights Ireland*, the Court reviewed the EU legislation, whereas in *Tele2/Watson*, the Court clearly referred to national legislation of the Member States.[55] The Court not only analysed the national laws in Sweden and the United Kingdom in light of the Charter but also in light of secondary law. Despite the differences between the subjects of review, *Tele2/Watson* constitutes a "follow-up" to *Digital Rights Ireland*, although *Tele2/Watson* concentrates on analysing the exemption from Directive 2002/58.[56] The Court presented a new approach on data retention, whereas with respect to access by law enforcement, the Court followed the arguments presented in *Digital Rights Ireland*. However, *Tele2/Watson* analysed both aspects—data retention and access by law enforcement—which was often missed at the national level[57] due to separate regulation of each issue. In this sense, *Tele2/Watson* is the decision that fully invalidated the Data Retention Directive. The Court ruled that "Member States may not impose a general obligation on providers of electronic communications services to retain data."[58]

Both decisions confirmed that data retention enables the creation of precise individual profiles, which constitutes a severe interference with privacy rights. Those Member States that did not react to *Digital Rights Ireland* by initiating a review of their national legislation are now likely to do so. Unfortunately, most of the Member States' legislation do not meet the standards that the Court noted in *Tele2/Watson*.[59] Applying the CJEU's high standard of data protection may have posed risks to the effectiveness of the EU law. The consequences of the ruling for the UK regulation[60] will be particularly interesting especially considering the additional changes resulting from Brexit. The requirement that data be stored within the EU could significantly limit the consequences of Brexit.[61]

The notion that unlimited data retention is incompatible with human rights protected by the EU has generated both positive and negative comments. Positive comments have resulted from the CJEU's increased level of data protection in comparison to the standard established in the *Digital Rights Ireland* decision. It noted that requirements must be established in national legislation to ensure that data retention will be limited only where strictly necessary. "In Tele-2/Watson the CJEU

[55]Tracol (2017), p. 548.

[56]Cameron (2017), p. 1468.

[57]Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson judgment. A Concerning State of Play for the Right to Privacy in Europe*, September 2017, p. 6.

[58]Cameron (2017), p. 1468.

[59]Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson judgment. A Concerning State of Play for the Right to Privacy in Europe*, September 2017.

[60]Takatsuki (2017).

[61]Patrick (2016).

not only confirmed the importance of its ruling in *Digital Rights Ireland* but also expanded on that ruling affirming positive requirements that national data retention legislation must comply with both European and international human rights law".[62]

Criticism of the judgment is much more differential. First, it has been suggested that such a high level of data protection in relation to public security has nothing to do with the "classic" vision of the EU focused on internal market collaboration.[63] Second, it has been suggested that "removing a general duty of retention severely undermines the investigative ability of police and intelligence services"[64] due to lack of access to historical data.[65] The *Tele2/Watson* decision was even described as a "radical" one due to the concern it caused among law enforcement in Member States.[66] The opponents of the ruling even stated that it may cause "actual or potential catastrophe."[67] As a result of the decision in this case, data retention systems in Sweden and the UK should be significantly amended. Therefore, this decision is revolutionary.

It has been argued that this decision leads to the elimination of a useful tool in daily law enforcement. The problem of potentially undermining the effectiveness of law enforcement investigations was noted by Europol after the decision in *Digital Rights Ireland*.[68] However, the main problem now concerns the reshaping of the model for data retention and not the conditions that must be met to access data.

The Court found that the untargeted and indiscriminate retention of data of all persons using mobile phones is unlawful. The Court eliminated the Directive's main justification for data retention. The Court found that such a broad collection of data is not "strictly necessary" and is not proportionate. Nevertheless, the Court proceeded to reflect upon the additional standards and restrictions for targeted data retention and access to data in particular.[69] Looking for situations wherein data retention is untargeted is probably the main challenge after *Tele2/Watson* decision.

Some solutions were already proposed, such as removing one category out of traffic data that will not be retained,[70] as well as different time periods and locations for the data traffic. The Court's analysis of national legislation in *Tele2/Watson*

[62]Privacy International, *National Data Retention Laws since the CJEU's Tele-2/Watson judgment. A Concerning State of Play for the Right to Privacy in Europe*, September 2017, p. 14.

[63]The EU courts all too often hold the Member States to a higher standard of compliance than the EU institutions extending the EU's ever expanding human rights regime into areas of law that have nothing to do with the EU's classical internal market economic governance competences: Beck (2017).

[64]Cameron (2017), p. 1483.

[65]Cameron (2017), p. 1482.

[66]Anderson (2017).

[67]Hil (2017).

[68]Europol, *An Update on Cyber Legislation*. www.europol.europa.eu/iocta/2015/app-2.html. Accessed 16 August 2018.

[69]Väljataga (2017).

[70]Cameron (2017), p. 1486. The author gives an example of unsuccessful connections as those that could be excluded from the scope of retained data.

allows one to state more easily which elements of a data retention system are not permissible, rather than establish regulations that would satisfy EU Charter requirements.[71] This approach was also presented by the Council Legal Service in February 2017.[72] I. Cameron wondered whether better protection of people with duties of confidentiality would "cure" a general duty of retention.[73]

The Court's suggestion in this respect referred to geographic criteria as a measure to limit and target the scope of retained data. Those geographical criteria would also need to be proved by objective evidence for high crime risk.[74] This idea triggered a set of critical comments afterwards. The main criticism suggests that systems based on territorial delineation may lead to discriminatory profiling of certain areas (e.g. suburbs where low-income migrants live).[75] The second point of criticism suggested that the same goal of targeted retention can be achieved through more simple technical means.[76]

The retention of telecommunication data and their usage for law enforcement investigations or intelligence operations require that one consider the many issues that are at stake, including not only the legal aspects of privacy protection but also a detailed technological knowledge and practice of law enforcement work. *Digital Rights Ireland* and *Tele2/Watson* did not specifically analyse these issues.

I. Cameron argued that the "potential chilling effect" caused by untargeted telecommunication data retention is an "empirical question, only answerable in each Member State."[77] D. Anderson, former UK Independent Reviewer of Terrorism Legislation, suggested that the EU Member States might have different past experience with law enforcement competence on surveillance, which might cause difficulty in establishing one standard common for the whole EU.[78] This would suggest that different historical experiences of the Member States could allow the creation of different legal arrangements of data protection and oversight of law enforcement. It is noted that some EU Member States have already imposed notice requirements, thus providing a guarantee of appropriate control over retained data, whereas the

[71] Woods (2016).

[72] Information note of the Council Legal Service to Permanent Representatives Committee (Part 2). https://cdn.netzpolitik.org/wp-upload/2017/05/rat_eu_legal_service_vds_20170201.pdf. 1 February 2017, COREPER (doc. 5884/17) "It is however clear from the operative part of the Tele2 judgment that a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level, since it would violate just as much the fundamental requirements as demonstrated by the Court's insistence in two judgments delivered in Grand Chamber" (p. 6).

[73] Cameron (2017), p. 1488.

[74] Pederson et al. (2018), pp. 10–11.

[75] Väljataga (2017), Woods (2016) and Lynskey (2017).

[76] I. Cameron underlined lack of justification for such an exception; he argued that there are "simpler and more secret ways to get it, most obviously through the use of IMSI catchers.": Cameron (2017), p. 1491.

[77] Cameron (2017), p. 1484.

[78] Anderson (2017).

Court applied an "EU-wide level of (mis)trust in the police and intelligence agencies."[79]

Tele2/Watson also has important implications for the ongoing development of the EU legislation in the field of privacy protection. Particularly interesting are two instruments: the so-called Police Directive[80] and the draft of ePrivacy Regulation that will annul Directive 2002/58. Drafted Article 11 of the ePrivacy Regulation does not specifically mention data retention; however, the EC proposal clearly confirmed that "Member States are free to keep or create national data retention frameworks that provide, inter alia, for targeted retention measures, in so far as such frameworks comply with Union law, taking into account the case-law of the Court of Justice on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights."[81]

When it comes to Directive 2016/680, it was still negotiated when CJEU ruled *Tele2/Watson*. The Police Directive does not state either a clear notice requirement or a criterion on data access by law enforcement. It also limits its scope of application to the goal of "fighting crime" without clearly defining "serious crimes" established in *Tele2/Watson*.

However, the Police Directive could settle some of the concerns relating to geographic criteria as a basis for "territorial data retention," since the Directive clearly prohibits discriminatory profiling.[82] However, it seems that the requirement of data storage within the EU will be confirmed in an effective law.[83] Nevertheless, the requirement constitutes a challenge for any future international transfer of personal data to third countries.[84]

5 Conclusions

The judicial life of data retention in the European Union can be analysed from different perspectives—the relation between market freedoms and individuals' rights, procedural safeguards against abuse of power by law enforcement, and

[79]Cameron (2017), p. 1481.

[80]Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[81]Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD), p. 3.

[82]Article 11 of Directive 2016/680.

[83]Article 32 GDPR.

[84]Lynskey (2017).

effectiveness of investigations conducted by law enforcement. The CJEU case law has evolved and emphasised different aspects of the mass collection of telecommunication data. In *Ireland v. Parliament*, the Court concentrated on data retention and noted the connection between the obligation to retain data and the EU's internal market. In *Digital Rights Ireland*, the Court mainly analysed the shortcomings of regulation on access to data retention by law enforcement, whereas in *Tele2/Watson* the Court focused more on the limits of data retention schemes. Ten years after the Data Retention Directive was adopted, the Court concluded that the main idea of the Directive, the indiscriminate and untargeted collection of data traffic, is unacceptable under the EU law. The decision in *Digital Rights Ireland* opened a real judicial discussion about data retention at the EU level, and *Tele2/Watson* certainly did not close it.[85] The discussion may even intensify due to the requirement established in *Tele2/Watson* which provides that there must be "objective evidence" proving that a given data retention system is "strictly necessary."

The EU approach on protecting human rights was mostly perceived as a reflection of ECtHR case law due to limitations established in Article 51 of the EU Charter of Fundamental Rights. The Data Retention Directive saga shows how CJEU evolved and proposed an innovative approach in balancing data protection and national security. However, the main concern is the implementation of *Tele2/Watson* by Member States facing their own shortcomings. The Court certainly did not answer all the questions concerning data retention. Therefore, there are new reasons to discuss it in Member States with respect to other databases, including private ones gathering data on a voluntary basis.[86] The decision in *Tele-2/Watson* expanded the findings in *Digital Rights Ireland* and proposed a new solution—"targeted retention" as a tool able to effectively support the fight against serious crimes.

Member States are in a difficult position—they must defend both in national and the EU courts something that they were obliged to introduce 10 years ago according to the EU law. Because *Tele2/Watson* requires the introduction of limitations to untargeted data retention based on objective evidence independently verified by courts or independent administrative bodies, it is likely that the real discussion about the effectiveness of data retention has just begun.

References

Anderson D (2017) CJEU Judgment in Watson/Tele2. https://www.daqc.co.uk/2017/04/11/cjeu-judgment-in-watson/

Beck G (2017) Case Comment: C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 SSHD v Tom Watson & Others. https://eutopialaw.com/2017/01/13/case-comment-cases-c-

[85]Beck (2017): "the Court implicitly opened the door to further legal uncertainties and future litigation."

[86]Pederson et al. (2018), p. 13.

20315-tele2-sverige-ab-v-post-och-telestyrelsen-and-c-69815-secretary-of-state-for-the-home-department-v-tom-watson-and-others/
Boehm F, Cole F (2014) Data Retention after the Judgment of the Court of Justice of the European Union, Münster/Luxembourg (Study provided by the Greens/EFA Group in the European Parliament), 30 June 2014
Breyer P (2005) Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR. Eur Law J 11(3):365–375
Cameron I (2017) Balancing data protection and law enforcement needs: Tele2 Sverige and Watson. Common Mark Law Rev 54:1467–1496
Europol, An Update on Cyber Legislation. www.europol.europa.eu/iocta/2015/app-2.html. Accessed 16 Aug 2018
Gryffroy P (2016) Two years after Digital Rights Ireland: general data retention obligations might still be compatible with EU law. A review of the Advocate General's opinion in Joined Cases C-203/15 and C-698/15. http://jean-monnet-saar.eu/?p=1511
Guild E, Carrera S (2014) The political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive, CEPS Papers May 2014, 65
Herlin-Karnell H (2009) Case Comment Case C-301/06, Ireland v. Parliament and Council. Common Mark Law Rev 46:1667
Hil M (2017) Where to after Watson? The challenges and future of mass data retention in the UK. https://infolawcentre.blogs.sas.ac.uk/2017/05/17/where-to-after-watson-the-challenges-and-future-of-mass-data-retention-in-the-uk/
Lynskey O (2017) Tele2 Sverige AB and Watson et al: continuity and radical change. European Law Blog. https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/
Ojanen T (2014) Privacy is more than just a seven-letter word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance Court of Justice of the European Union, Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others. Eur Constit Law Rev 10(3):540
Patrick A (2016) Case Law, CJEU, Tele Sverige/Watson: Who Sees You When You're Sleeping? Who Knows When You're Awake? https://inforrm.org/2016/12/21/case-law-cjeu-tele-sverigewatson-who-sees-you-when-youre-sleeping-who-knows-when-youre-awake-angela-patrick/
Pederson A, Udsen H, Jakobsen SS (2018) Data retention in Europe – the Tele 2 case and beyond. Int Data Priv Law 8(2):160–174
Poli S (2010) The legal basis of internal market measures with a security dimension. Comment on Case C-301/06 of 10/02/2009, Ireland v. Parliament/Council. Eur Constit Law Rev 6 (1):137–157
Privacy International, National Data Retention Laws Since the CJEU's Tele-2/Watson judgment. A Concerning State of Play for the Right to Privacy in Europe, September 2017
Rauhofer J, Mac Sithigh D (2014) The data retention directive never existed. SCRIPTed 11(1):126
Report from the Commission to the Council and the European Parliament – Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) Brussels, 18.4.2011 COM(2011) 225 final
Takatsuki Y (2017) The Tele2/Watson Case: what are the key takeaways? . . . and what is to become of the New Investigatory Powers Act? http://privacylawblog.fieldfisher.com/2017/the-tele2watson-case-what-are-the-key-takeaways-and-what-is-to-become-of-the-new-investigatory-powers-act/
Tracol X (2014) Legislative genesis and judicial death of a directive: the European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it. Comput Law Secur Rev 30 (6):736–746
Tracol X (2017) The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level. Comput Law Secur Rev 33(4):541–552

Väljataga A (2017) CJEU Declares General Data Retention Unlawful in Tele2 Sverige. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/cjeu-declares-general-data-retention-unlawful-tele2-sverige.html

Vedaschi A, Lubello V (2015) Data retention and its implications for the fundamental right to privacy. Tilburg Law Rev 20:14–34

Woods AK (2016) Implications of the EU's Data Retention Ruling. Lawfareblog. https://www.lawfareblog.com/implications-eus-data-retention-ruling

Freedom of Communication and Data Retention in Judgments of the European Court of Human Rights

Maciej Górski

Abstract This article attempts to analyse how the understanding of the universal freedom of communication expressed in the European Convention on Human Rights (ECHR) has been changing in the context of continuous technological progress. Development of both communication tools and communication itself was a serious challenge for the European Court of Human Rights (ECtHR). Its task was to interpret the provisions of the ECHR in a way that, on one hand, would consider new technological circumstances, and on the other, would guarantee full exercise of freedoms provided for by the ECHR. For this purpose, the article contains an overview of the most important judgments of the ECtHR, in which judges pertained not only to new ways and tools of communication, but also to other functions it fulfils. The text also addresses the problem of potential misuse of technology development in the surveillance by state authorities. Attention was also paid to legal guarantees of freedom of communication, which should assist similar development of surveillance tools. Finally, an attempt was made to forecast in which direction the case law of the Court will follow in the coming years and how the technology development will affect it.

1 Freedom of Communication According to the ECtHR

One of key tasks of the European Court of Human Rights (ECtHR) as an international judicial body—added to its basic adjudication activity involving examination of application lodges—is the interpretation of notions that are of material importance from the point of view of the ECtHR's material competence. Due to the structure and the manner of formulating the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), some of freedoms and rights included therein require special judicial activity from the ECtHR.

M. Górski (✉)
Lech Kaczynski National School of Public Administration, Warsaw, Poland

M. Zubik et al. (eds.), *European Constitutional Courts towards Data Retention Laws*, Law, Governance and Technology Series 45,
https://doi.org/10.1007/978-3-030-57189-4_2

The role of the ECtHR with respect to interpretation seems especially important in case of defining the scope of freedoms and rights, the way of exercising which might change significantly together with the technology development. The ECHR had been opened for signature on 10 November 1950, and after obtaining ten ratifications, it came into force on 3 September 1953. Since then, its key parts have remained unchanged, while ECtHR judges were responsible for adjusting their application to changing circumstances. One of the examples of their interpretational endeavours is the evolution of the meaning of freedom of communication.

Freedom of communication is expressed in Article 8 of the ECHR, according to which "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[1]

In the ECHR, the correspondence is broadly understood as communication in various forms to establish contacts with other specifically identified persons, using writing or technical means.[2] In the development of the case law of the ECtHR in this respect, the aforementioned essence of understanding of communication remained, and as a rule, unchanged. However, considering the technology development resulting in a growth in the number and popularisation of tools used in communication, the judges in each case deliberated whether the right to freedom of communication, guaranteed in the ECHR, applies in the particular case.

2 *Klass and Others v. Germany*: Landmark ECtHR Judgment for the Analogue Era

The first judgment of the ECtHR of the crucial importance for the then and the present understanding of freedom of communication was the judgment in the case of *Klass and others v. Germany*.[3] Although it was issued more than 40 years ago, it still retains its precedential character. In this judgment, the ECtHR presented various hypotheses that constituted the base for formulation of the scope of protection of freedom and secret of communication within the meaning of the ECHR. It should be emphasised that the value of the judgment is universal, because based thereon, the ECtHR referred to various issues being basic subjects of its analysis, such as: the

[1] Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950.

[2] Decision of the European Commission of Human Rights of 13 May 1982, *X and Y v. Belgium*, Application No. 8962/80.

[3] Judgment of the European Court of Human Rights of 6 September 1978, *Klass and others v. Germany*, Application No. 5029/71.

definition of a victim of a violation of the ECHR entitled to bring an application, permitted scope of an interference with the right to privacy or the right to effective remedies to protect rights provided for in the ECHR.[4]

The judgment referred to German legislation authorising intelligence service to apply secret measures to obtain information. This is because the special legal situation of Germany after the Second World War was also reflected in the legislation on the surveillance of mail, post and telecommunications. Occupying powers were responsible for this surveillance. As regards the Federal Republic of Germany, neither the entry into force on 24 May 1949 of the Basic Law nor the termination of the occupation regime in 1955 altered this situation.[5] Legal situation in this respect was adjusted not before 24 June 1968, when the Parliament of the Federal Republic of Germany passed new regulations governing the scope of permitted interference by the state with the right to secrecy of the mail.

The law passed assumed that the person, against whom the measures to control mail were ordered, shall not be notified thereof. The mechanism for the verification of the measures taken under the law involved imposing on the competent minister the duty to submit, at least once every six months, a report on the application of the law to the commission appointed by Bundestag.[6]

In the opinion of the applicants, solutions provided by the law were insufficient, and they based their application to the European Commission of Human Rights on the charge that the law allowed applying secret measures without simultaneous obligation of state authorities to subsequently notify persons concerned thereof.

The key issue that must be resolved in the case in question by the ECtHR was whether the individual might effectively claim judicial protection without proving being a victim of secret surveillance. On one hand, the ECtHR emphasised that provisions of the ECHR do not institute for applicants a kind of *actio popularis* and do not allow for *in abstracto* interpretation thereof. However, on the other hand, it must consider the risk of an individual being deprived of the opportunity of lodging such an application because, owing to the specifics of the secret measures, the victim cannot prove that they were actually applied against him.

In the deliberations, the ECtHR concluded that ensuring some possibility of having access to the Commission and submitting application by the individual is of crucial importance. If this were not so, the efficiency of the ECHR's enforcement machinery would be materially weakened. To ensure effective functioning of the protection of the rights granted therein, the ECtHR concluded that an individual may, under certain conditions, claim to be the victim of a violation occasioned by the

[4]Shelton and Carozza (2008), p. 292; Brouwer (2008), p. 166.

[5]Judgment of the European Court of Human Rights of 6 September 1978, *Klass and others v. Germany*, Application No. 5029/71, para. 14.

[6]In addition, the law assumed a more immediate control measure involving providing the commission with an account of the operational measures ordered. The commission decided *ex officio* or on application by an interested person, on both the legality and the necessity of the measures in question. If it declared any measures to be illegal or unnecessary, the minister was obliged to terminate them immediately.

mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions specified by the ECtHR included: indicating a violation of rights protected by the ECHR, the secret character of the measures taken, and the connection between the applicant and the measure taken.[7]

In the case in question, authorities of the Federal Republic of Germany did not question the conclusion that the application of regulations allowing taking secret surveillance measures constitutes interference with the right to privacy guaranteed by Article 8 of the ECHR. In its considerations, the ECtHR significantly extended the aforementioned supposition, by indicating that: "(. . .) in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence."[8]

In the *Klass* case, the influence of the technology development on the understanding of freedom of communication and mail was also noticed—by concluding that although telephone conversations are not expressly mentioned in paragraph 1 of Article 8, it should be considered that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision.[9] More importantly, this catalogue will systematically grow together with the development of the ECtHR case law pertaining to freedom of communication.

Although ultimately the judges did not share the position of applicants and unanimously found no breach of Article 8 of the ECHR, just due to recognising the application as admissible, started the evolution of the notion of "freedom of communication" and "correspondence", emphasising the importance of judicial control of the use of secret measures and recognising that their application is sometimes necessary in a democratic societies, the judgment in the case of *Klass and others v. Germany* is considered one of the most significant and meaningful issued judgments in this matter by the ECtHR.[10]

[7]Judgment of the European Court of Human Rights of 6 September 1978, *Klass and others v. Germany*, Application No. 5029/71, para. 34.

[8]Judgment of the European Court of Human Rights of 6 Sept 1978, *Klass and others v. Germany*, Application No. 5029/71, para. 41.

[9]Judgment of the European Court of Human Rights of 6 Sept 1978, *Klass and others v. Germany*, Application No. 5029/71. para. 41.

[10]Petaux (2009), p. 164; Lambert Abdelgawad and Weber (2008), p. 123; Christakis (2016), p. 153.

3 Technology Perspective Pertaining to the Prison System

When presenting the evolution of the notion of the freedom of communication in its technological aspect, one should also refer to several ECtHR judgments on prisoners' mail that significantly affected the notion in question. The judgment of 25 March 1983 in the case of *Silver and others v. the United Kingdom*[11] is one of judgments widely commented in the doctrine and important in the context of further line of judgments of the ECtHR. The case originated in a few applications lodged by persons detained in prison (one of these persons was at liberty) complaining about prison authorities controlling their mail. Applicants claimed that an unjustified interference with the right to respect for their correspondence took place. In this case, the ECtHR concluded that "some measure of control over prisoners' correspondence is called for and is not of itself incompatible with the ECHR, having regard to the ordinary and reasonable requirements of imprisonment."[12]

It should be emphasised that in subsequent judgments, in line with the aforementioned approach, the ECtHR admitted that: "(. . .) it may be necessary to monitor detainees' contacts with the outside world, including contacts by telephone, but the rules applied should afford appropriate protection against arbitrary interference by national authorities with the detainee's rights".[13] In another judgment, the judges presented the following justification for the detailed and prudent assessment of control applied: "In assessing the permissible extent of such control in general, the fact that the opportunity to write and to receive letters is sometimes the prisoner's only link with the outside world should, however, not be overlooked."[14] Additionally, they noted that prisoners should be provided with certain guarantees related to prison authorities monitoring their correspondence: "Where domestic law allows interference, it has to offer certain protection preventing power abuse (. . .)."[15]

In its extensive case law pertaining to this issue, the ECtHR also criticised preventing correspondence by refusal to supply the prisoner with writing materials,[16] hindering contacts between prisoners and lawyers[17] and the court within the

[11]Judgment of the European Court of Human Rights of 25 March 1983, *Silver and others v. the United Kingdom,* Application Nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75.

[12]Judgment of the European Court of Human Rights of 25 March 1983, para. 98.

[13]Judgment of the European Court of Human Rights of 27 April 2004, *Doerga v. The Netherlands*, Application No. 50210/99, para. 53.

[14]Judgment of the European Court of Human Rights of 25 March 1992, *Campbell v. the United Kingdom*, Application No. 13590/88, para. 45.

[15]Judgment of the European Court of Human Rights of 21 October 1996, *Calogero Diana v. the United Kingdom*, Application No. 15211/89, paras. 32–33.

[16]Judgment of the European Court of Human Rights of 3 June 2003, *Cotleț v. Romania*, Application No. 38565/97, para. 59 and para. 65.

[17]Judgment of the European Court of Human Rights of 20 June 1988, *Schöneberger and Durmaz v. Switzerland*, Application No. 11368/85, paras. 28–29.

meaning of the ECtHR,[18] with journalists,[19] with a doctor[20] or with other entities, such as an ombudsman[21] and NGOs.[22]

In one of the aforementioned judgments, the ECtHR concluded that to effectively exercise rights guaranteed in Article 8 of the ECHR, prison authorities are not only expected to refrain from certain behaviour, but are also expected to implement certain steps to enable the prisoners to effectively exercise their right to communicate. The position of the ECtHR was also repeated in other situations, not related to the prison system.[23]

4 Telephone Tapping

Although in accordance with the traditional understanding of Article 8, letters (written documents) were considered the ordinary form of correspondence, the ECtHR case law that developed over decades has considered the technology progress in this area. In various judgments issued in this respect, the judges not only noticed that communication based on traditional letters is more and more frequently replaced by telephones, but also observed more sophisticated and advanced methods of interference with private life of individuals. For that reason, the development of the case law line has two directions. On one hand, it was examined whether new technical forms of communication are subject to protection under Article 8, and on another hand, attempts were made to reconcile justified needs of authorities to take secret surveillance measures with the right to freedom of communication, to which individuals are entitled.

The main group of judgments of the ECtHR issued before the digital revolution focused on telephone communication and they provided the basis for the standards of freedom of communication formulated at that time. In addition to the judgment in the case of *Klass and others v. Germany*, the judgment in the case of *Malone v. the*

[18]Judgment of the European Court of Human Rights of 23 September 1998, *Petra v. Romania*, Application No. 27273/95, para. 37.

[19]Judgment of the European Court of Human Rights of 5 December 2006, *Fazil Ahmet Tamer v. Turkey*, Application No. 6289/02, para. 53.

[20]Judgment of the European Court of Human Rights of 2 June 2009, *Szuluk v. the United Kingdom*, Application No. 36936/05, paras. 49–53.

[21]Judgment of the European Court of Human Rights of 4 July 2000, *Niedbała v. Poland*, Application No. 27915/95, para. 81.

[22]Judgment of the European Court of Human Rights of 24 February 2005, *Jankauskas v. Lithuania*, Application No. 59304/00.

[23]Judgment of the European Court of Human Rights of 18 April 2006, *Chadimová v. the Czech Republic*, Application No. 50073/99, para. 146; Decision of the European Court of Human Rights on admissibility of the application of 16 June 2009, *Benediktsdóttir v. Iceland*, Application No. 38079/06.

United Kingdom of 2 August 1984[24] was one of judgments that significantly affected the case law line.

The applicant was an antique dealer in the United Kingdom, and in March 1977, he was charged with offences relating to dishonest handling of stolen goods. During the trial, it emerged that one of his telephone conversations was intercepted. After being acquitted, Malone, in civil proceedings ineffectively soughed from the police the declaration to the effect that tapping of conversations on his telephone lines was unlawful. When the case was submitted to the ECtHR, the judges had to answer the question whether there was an unauthorized interference by public authorities with the right protected by Article 8, and they also had to assess how "metering" of telephone calls affects freedom of communication. The process known as "metering" involves the use of a mechanism that registers the numbers dialled on a particular telephone and the time and duration of each call.[25]

The ECtHR confirmed its previous position, in accordance to which telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8. Additionally, it concluded that "the existence (. . .) of laws and practices which permit and establish a system for effecting secret surveillance of communications amounted in itself to an interference."[26] British legislation was considered too general and imprecise to consider it as providing sufficient basis for tapping of telephone conversations.

The judges also concluded that: "The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information without the consent of the subscriber amounts to an interference with a right guaranteed by Article 8".[27] Consequently, the ECtHR has noticed new methods of interference, which the authorities began to use, and responded thereto, by extending legal protection available to individuals based on Article 8.

In 1990, the ECtHR issued judgments in two similar cases against France, pertaining to telephone tapping ordered by a court, a tool used in relation to pending proceedings.[28] Based on both these cases, the judges summarised judgments issued until that time and prepared a catalogue of minimum guarantees that must be included in the law providing a legal basis for the use of telephone tapping in order not to consider it contrary to the ECHR. The following was, *inter alia*, indicated: categories of people liable to have their telephones tapped by judicial

[24]Judgment of the European Court of Human Rights of 2 August 1984, *Malone v. the United Kingdom*, Application No. 8691/79.

[25]Rainey et al. (2017), p. 413.

[26]Judgment of the European Court of Human Rights of 2 August 1984, *Malone v. the United Kingdom*, Application No. 8691/79, para. 64.

[27]Judgment of the European Court of Human Rights of 2 Aug 1984, *Malone v. the United Kingdom*, Application No. 8691/79, para. 84.

[28]Judgment of the European Court of Human Rights of 24 April 1990, *Kruslin v. France*, Application No. 11801/85; Judgment of the European Court of Human Rights of 24 April 1990, *Huvig v. France*, Application No. 11105/84.

order; the nature of the offences which may give rise to such an order; maximum duration of the application of this control measure; procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, particularly where an accused has been discharged by an investigating judge or acquitted by a court.[29]

Another interesting issue was resolved by the ECtHR on 25 March 1998, in the judgment in the case of *Kopp v. Switzerland.* The applicant was a lawyer practicing in Zurich, and his wife was a member of the Swiss government fulfilling the function of the head of the department of justice and police. She was under suspicion of disclosing to her husband confidential information that was subsequently used by one of his clients. As a result of these suspicions, she was obliged to resign. Due to the aforementioned suspicion, the President of the Indictment Division of the Federal Court allowed an application by the Federal Public Prosecutor for monitoring of telephone lines allocated to the office of Mr Kopp, except for telephone conversation with the participation of Kopp as a lawyer. After having concluded that the suspicions against the applicant's wife were unfounded, monitoring of telephone conversation was discontinued, recordings were destroyed, and Mr Kopp was notified that his telephone lines were tapped.

In the application to the European Commission of Human Rights, Mr Kopp submitted that the interception of his telephone communications had breached his right to respect for his private life and correspondence. The most interesting element of this case was the issue of effectiveness of protection of legal professional privilege when a lawyer is being monitored as a third party, and the conversation content is not directly covered by the scope of professional privilege. Judges of the ECtHR also had reservations about the fact that the duty to separate materials specifically connected with a lawyer's work, i.e. the ones that could not have been recorded, was assigned to an official of the Post Office's legal department, without supervision by an independent judge. It was concluded that Swiss law did not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter, and that there had therefore been a breach of Article 8 of the ECHR.

In this case, the ECtHR also referred to challenges to the freedom of communication resulting from the technology development. The recommendation formulated in judgments in the case of *Kruslin v. France* and *Hudvig v. France* was repeated, in accordance to which: "It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."[30] In this context, reflections presented by the judge Louis-Edmund Pettit in

[29]Judgment of the European Court of Human Rights of 24 April 1990, *Kruslin v. France*, Application No. 11801/85, paras. 26–27; Judgment of the European Court of Human Rights of 24 April 1990, *Huvig v. France*, Application No. 11105/84, paras. 54–55.

[30]Judgment of the European Court of Human Rights of 25 March 1998, *Kopp v. Switzerland*, Application No. 23224/94, para. 72.

his concurring opinion, in which he agreed with the verdict, but proposed different arguments, seem interesting. Judge Pettiti admitted that "It is a regrettable fact that State, para-State and private bodies are making increasing use of the interception of telephone and other communications for various purposes."[31] He also stated that "States (...) abuse the concepts of official secrets and secrecy in the interests of national security. Where necessary, they distort the meaning and nature of that term," and described the irresponsible practices of the people running the relevant state services responsible for the communication monitoring as "a sign of the decadence of the democracies and erosion of the meaning of human dignity."[32]

The ECtHR case law line presented in the aforementioned judgments was maintained by judges in judgments issued in last years, among which the following judgments should be, *inter alia*, referred to: *Dragojević v. Croatia*,[33] *R.E. v. the United Kingdom*[34] or *Mustafa Sezrin Tanrikulu v. Turkey*.[35]

5 Other Communication Means

In the development of its case law, the ECtHR often had to answer the question whether new communication tools and platforms are covered by the protection granted by Article 8 of the ECHR. In addition to telephone conversations, other less popular communication methods were also examined, such as, *inter alia*, in the case of *Taylor-Sabori v. the United Kingdom*, where the judges examined the issue of communication with a pager. The issue pertained to the police intercepting messages sent to the pager of the applicant, who was suspected, arrested and ultimately convicted and sentenced for importation and sale of drugs on the territory of the United Kingdom.

The applicant complained that the interception by the police of messages on his pager constituted the interference with the right to privacy and a violation of Article 8 of the ECHR. The ECtHR noted that at that time, in the United Kingdom, there existed no statutory system to regulate the interception of pager messages. It

[31]Concurring opinion to the Judgment of the European Court of Human Rights of 25 March 1998, *Kopp v. Switzerland*, Application No. 23224/94.

[32]Concurring opinion to the Judgment of the European Court of Human Rights of 25 March 1998, *Kopp v. Switzerland*, Application No. 23224/94.

[33]Judgment of the European Court of Human Rights of 15 January 2015, *Dragojević v. Croatia*, Application No. 68955/11.

[34]Judgment of the European Court of Human Rights of 27 October 2015, *R.E. v. the United Kingdom*, Application No. 62498/11.

[35]Judgment of the European Court of Human Rights of 18 July 2017, *Mustafa Sezgin Tanrikulu v. Turkey*, Application No. 27473/06.

concluded that there had been a violation of Article 8 of the ECHR, thus admitting that freedom of communication also applies to communication with a pager.[36]

Based on the decision of 27 June 1994 of the European Commission of Human Rights in the case of *Christie v. the United Kingdom*, communication via telex[37] was also classified as covered by the production under Article 8.

The judges were of a similar opinion about the issue of sending letters by telefax, which was assessed by the ECtHR in the judgment of 16 December 1992 in the case of *Niemietz v. Germany*.[38]

The issue of radio communications, examined by the Commission and the ECtHR in the decision of 13 May 1982 in the case of *X and Y v. Belgium* and in the judgment of 16 December 1997 in the case of *Camenzind v. Switzerland*, respectively, was also resolved in the same way. However, it should be added that communication on frequencies available to third parties was treated in a different way.[39]

6 Technology Development as a Challenge to the ECtHR

The technology development is used not only by citizens, but also by entities authorised by public authorities, responsible for communication monitoring and recording, that systematically develop and improve the methods used.

The ECtHR referred to one of the examples of this phenomena in the decision of 29 June 2006 in the case of *Weber and Saravia v. Germany*. The first applicant was a German journalist investigating drug and arms trafficking and money laundering. To carry out her investigations, she regularly travelled to South America. The second applicant was an employee of Montevideo City Council. They both communicated using a satellite phone.

The issue examined pertained to so-called strategic monitoring of telecommunications. In this application, the applicants noted that "(. . .) technological progress had made it possible to intercept telecommunications everywhere in the world and to collect personal data. Numerous telecommunications could be monitored, in the absence of any concrete suspicions, with the aid of catchwords which remained secret".[40] They drew attention to the practice of services involving monitoring of a

[36]Judgment of the European Court of Human Rights of 22 October 2002, *Taylor-Sabori v. the United Kingdom*, Application No. 47114/99.

[37]Decision of the European Commission of Human Rights on admissibility of the application of 27 June 1994, *Christie v. the United Kingdom*, Application No. 21482/93.

[38]Judgment of the European Court of Human Rights of 16 December 1992, *Niemietz v. Germany*, Application No. 13710/88.

[39]Decision of the European Commission of Human Rights on admissibility of the application of 27 February 1994, *B.C. v. Switzerland*, Application No. 21353/93.

[40]Decision of the European Court of Human Rights on admissibility of the application of 29 June 2006, *Weber and Saravia v. Germany*, Application No. 54934/00.

large number of messages sent via various messengers, by using word filters selecting catchwords that might be alarming from the point of view of that services.[41]

When issuing the decision in this case, the ECtHR focused on the issue of the law's foreseeability. It concluded that "(. . .) foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident."[42] The judges emphasised the importance of sufficient clarity of the domestic law in such a situation that "(. . .) must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[43] In the case in question, they concluded that adequate and effective guarantees against abuses of the state's monitoring powers existed, and the application was considered ill-founded.

Increasing state capabilities with respect to communication monitoring are without doubt related to greater ability to collect data obtained in this way. The ECtHR emphasised the importance of legislation ensuring proper standards in this respect in the judgment in the case of *Liberty and others v. the United Kingdom* of 1 July 2008. The case pertained to a special unit of the British Ministry of Defence intercepting communications of civil liberties' organisations. The judges confirmed that requirements pertaining to surveillance measures against individual presented in the judgment in the case of *Kruslin v. France* and subsequently often repeated should also be respected within the framework of the generalised strategic monitoring, and the procedure for testing, disclosure, storing and destroying the collected material should be presented in a form accessible to the general public.[44]

A different approach was presented in the case of the *Centrum för rättvisa v. Sweden*. The complaint, lodged by a law firm acting in the public interest, concerned provisions allowing the services to collect data on users of mobile phones and Internet without prior notification on massive scale. The complained provisions did not provide for the possibility of appeal of a person who suspected that he was subject of surveillance. The judges found that the questioned act fulfilled the condition of proportionality, providing sufficient guarantees to prevent the risk of arbitrariness. Moreover, the ECtHR considered that to counteract terrorism, the state must have some discretion in shaping regulations concerning operational control.

[41] St Vincent (2017), p. 372.

[42] Decision of the European Court of Human Rights on admissibility of the application of 29 June 2006, *Weber and Saravia v. Germany*, Application No. 54934/00, para. 93.

[43] Decision of the European Court of Human Rights on admissibility of the application of 29 June 2006, *Weber and Saravia v. Germany*, Application No. 54934/00, para. 93.

[44] Judgment of the European Court of Human Rights of 1 July 2008, *Liberty and others v. the United Kingdom*, Application No. 58243/00.