**Željko Karas, PhD, Assistant Professor**
Police College, Ministry of Interior
Av. Gojka Šuška 1, HR-1000 Zagreb
zkaras@fkz.hr

# PRIVACY RIGHTS AND POLICING UNDER THE INFLUENCE OF MODERN DATA TECHNOLOGIES[1]

***ABSTRACT***

*The author analyses the relation between privacy and the powers to collect evidence in the digital environment. With the aim to identify main problems of police powers, the author analysed the Supreme Court, ECHR and ECJ case-law on degrees of intrusion. The lowest degree refers to the collection of general data that does not include collection of the content of communications. According to the results of the research, such a degree of intrusion in Croatian case-law is not considered to be a serious one. For these powers, the retention of data is necessary, and according to the ECJ and ECHR decisions, it must be appropriately regulated.*

*More stringent measures imply surveillance of communications content. The research results show that such measures are prescribed with considerably stricter standards. In addition, information that are available on social networks or similar sources may also be used in criminal investigation. The concept of total internet memory includes both positive and negative events, producing digital image of users. The development of new rights in this area, just as in the aforementioned, shows that the new standards are necessary in the digital domain.*

***Keywords**: police, privacy, surveillance*

## 1. INTRODUCTION

Modern computer technologies integrate many types of activities that citizens frequently use. The communication allows data sharing but also leaves a lot of information about contact. Part of such data can be very useful for crime detection. Some contemporary forms of crime that pose a significant threat to the community are being prepared primarily by using such communication techniques. If a person publishes his intentions of committing criminal offenses on particular social networks, access to such data may be very useful for police. There is a similar situation with the video recordings of the offenses, or many other types of communication. For the purpose of criminal investigation, it is very important to col-

[1] This paper is a product of work which has been supported by Croatian Science Foundation under the project 8282 „Croatian Judicial Cooperation in Criminal Matters in the EU and the Region: Heritage of the Past and Challenges of the Future“ (CoCoCrim)

lect such data. With this aim, a part of the legal regulation has been created which seeks to ensure the gathering of useful data.

This is particularly apparent in cybercrime, terrorism and similar criminal forms. In contemporary society, there are very striking aspirations to find and retain such data in order to increase security. Computer technologies are becoming an integral part of various types of criminal offenses and there is a need to accommodate modern development.[2] Such goals of criminal investigation need to be brought in line with the protection of fundamental rights of citizens. Collecting and analysing data is part of a proactive police approach, as well as intelligence-led policing. Models of predictive police work are adopting new technologies based on crime analysis.

## 2. COMMUNICATION CONTACT CHECKING

### 2.1. General remarks

Particular measure that police can use to collect digital communication data refers to general information about the contacts that have been made, but without insight into theirs content. This action relates to telecommunication data, device labels, and other ancillary features such as the approximate location. This kind of data is commonly referred to as Metadata. Apart from mobile phones, it may also apply to other forms of computer communication such as e-mails. The gathering is aided by the fact that a number of communication capabilities are connected in only one device. In Croatia, such action to collect data is prescribed in Article 68 of the Police Affairs and Authorities Act (PAA),[3] and in Article 339.a of the Criminal Procedure Act (CPA).[4] According to the Croatian system, insight into communication data only does not represent an intense interference with citizens' rights. For that reason, the way of prescribing is also significantly different from the special evidentiary measures that can use intrusive surveillance into the whole content of communication.

Article 68 of the PAA contains substantial (material) prerequisites (danger, search, criminal offenses) and procedural conditions required for a measure (approval in the police hierarchy, fact-finding needs). This provision also sets out the principle of subsidiarity. The Electronic Communications Act (ECA) prohibits network

---

2 Loideain, N., *EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era,* Media and Communication, vol. 3, no. 2, 2015, pp. 53-62

3 Police Affairs and Authorities Act, Official Gazette No. 76/2009, 92/2014

4 Criminal Procedure Act, Official Gazette No. 152/2008, 76/2009, 80/2011, 121/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017

operators from monitoring the content of communication, rather than retaining general communications information only (Article 109, Para 3).[5]

### 2.2. Croatian case-law

Our case-law has been holding the view that this is not a major restriction imposed on the constitutional rights of citizens.[6] Case-law has estimated that this type of action does not affect the secrecy of communication as a constitutional category. An example is a decision in which the Supreme Court ruled that "how much a person is using a telephone in no way can influence the judgment of her dignity, honour and reputation, nor undermine the secrecy of her private communication".[7] Such a low level of restriction does not involve the content of communication. Therefore, legal conditions for this action are less formalized. Such action does not need to have special judicial oversight, court orders, deletion clauses, or any special safeguards. Such guarantees are the same as in Article 339.a of the CPA, as opposed to some special evidence actions in the Article 332 CPA, which represents the restriction of the rights contained in Article 36 of the Constitution.[8]

When this action was introduced for the first time in the CPA in 2002, it was emphasized in the explanatory notes that it "checks the establishment of a connection in a given period. This action does not give the possibility of knowing the content of telecommunication messages or their surveillance".[9] The same was confirmed by the case law, for instance "here is only the list of telephone calls in terms of determining the frequency of a call to a certain phone number" with the conclusion that the police "have the right to request verification from telecommunication services about the identity of telecommunication addresses".[10]

Case-law has allowed additional processing of the collected data by analytical software, which are also not a serious restriction. An analysis of the relationship between a person, a time or a location in the form of an analytical report is an

---

5 Electronic Communications Act, Official Gazette No. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017

6 Karas. Ž., *Coherence of the Supreme court's case-law on admissibility of evidence from police inquiries*. Police and Security, vol. 17, no. 1, 2008, pp. 1-15; Case VSRH, I Kž-4/00

7 Case VSRH, I Kž-502/01

8 The Constitution of the Republic of Croatia, Official Gazette No. NN 56/1990, 135/1997, 8/1998, 113/2000, 124/2000, 28/2001, 41/2001, 55/2001, 76/2010, 85/2010, 05/2014

9 Government of the Republic of Croatia, *Final Draft of Act on Amandements of Criminal Procedure Act*, Zagreb, 2002

10 Case VSRH, I Kž 1162/04

auxiliary means, for example "drawn telephone locations are based solely on listings without having to involve their content".[11] Knowing frequency of telephone calls does not constitute a violation of the rights of the defendant but is lawful within this action.[12]

### 2.3. The ECtHR case-law

There wasn't many cases before the European Court of Human Rights (ECtHR) that refer to general data checks without having access to the content of communication.[13] Such police actions were not considered intrusive for Convention rights. In the case of Roman Zakharov v. Russia,[14] the applicant considered that it was not legal for network operators to install equipment that would allow operational searches without any guarantees. The ECtHR has verified compliance in an abstract manner and found a violation of Article 8 as there was no effective remedy.

There were issues on data type that could be gathered by this action. Collection of non-public data was the subject of decision in the case of Uzun v. Germany.[15] Determination of a person's location was carried out by exploiting GPS device. In this case, it was concluded that such gathering does not represent an overall surveillance of the kind similar to audio-visual one. It is not considered to be an intrusion into privacy rights. The GPS does not directly show any particular information about a person's behaviour, private opinions, or intimate feelings. The ECtHR did not consider that conduction without a court order has to constitute a violation of the Convention. The case was about the surveillance of the suspect involved in several attempted murders. A vehicle of his friend that he was occasionally using was monitored. The ECtHR concluded that action was fully justified because it lasted for a short period of three months, and person was not subjected to full surveillance, but only partially and only when he was in the vehicle.

## 3. SURVEILLANCE OF THE COMMUNICATION

### 3.1. General remarks

Part of the data can only be collected for criminal investigation by monitoring the complete content of communication between targeted subjects. Because of

---

11 Case VSRH, I Kž 598/12

12 Case VSRH, I Kž-Us 21/13

13 Breyer, P., *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, European Law Journal, vol. 11, no. 3, 2005, pp. 365-375

14 Judgment *Roman Zakharov v. Russia*, no. 47143/06, 4 December 2015

15 Judgment *Uzun v. Germany*, no. 35623/05, 2 September 2010

surveillance, such actions are considered as intrusive to fundamental rights. In Croatian system, there are approved forms of restriction of constitutional rights.[16] Therefore, these actions are very detailed in the CPA. They cannot be initiated based solely on police legislation. There has been set minimal standards for such surveillance activities (Malone v. UK).[17] Very strict safeguards must be adhered when it comes to surveillance, such as defining the type of action, scope of supervision, duration of measure, basis for determining and many others (according to Kennedy v. UK).[18] The violation of Article 8 of the Convention was established for legislation in Hungary which provided the surveillance in order to counter terrorist activities, but failed to provide adequate procedural guarantees (Szabó and Vissy v. Hungary).[19] In this field of intrusive measures, there is subsequent obligation for the persons under surveillance to be notified, or there could exist a breach of arbitrariness under Article 10 ECHR.[20]

For such restrictions, it is irrelevant whether they are carried out by the police or by some other official body. In any case, detailed legal regulation is necessary. There were violations when surveillance was performed by employers too. In the case of Halford v. UK,[21] the highest ranked policewoman reported that her superiors monitored her communication to prevent promotion in higher rank. There has been a violation of Article 8 of the Convention because office phones fall into the concept of private life and correspondence too. A similar question was raised in the case of Bărbulescu v. Romania,[22] in which the employer not only monitored the general data of employee, but also the content of the conversation. The employee was not warned, and there was not established if there existed legal basis for the measure to be applied.

### 3.2. Collecting private data

Measures that do not represent surveillance can be intrusive restrictions in the privacy rights. The sensitive data can be affected, regardless of the type of data collection activity. For instance, a violation was found in the case of Trabajo Rueda v. Spain in which the police seized the computer without prior judicial authori-

16 Case VSRH, I Kž Us 23/09; Case VSRH, I Kž-144/05

17 Judgment *Malone v. UK*, no. 8691/79, 2 August 1984

18 Judgment *Kennedy v. UK*, no. 26839/05, 18 May 2010

19 Judgment *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016

20 Judgment *Youth Initiative for Human Rights v. Serbia*, no. 48135/06, 25 June 2013

21 Judgment *Halford v. UK*, no. 20605/92, 25 June 1997

22 Judgment *Bărbulescu v. Romania*, no. 61496/08, 5 September 2017

sation for the purpose of detecting child pornography images.[23] The computer was already in the hands of the police and prior authorisation could have been obtained quickly. In the case of Aycaguer v. France, the violation was established with respect to the obligation to give the DNA sample, but there was no proportionality.[24]

A violation was established for copying the whole content of the laptop because it was based on regulations that did not allow such powers focused on a journalist.[25] When the employer searched the employee's computer for the purpose of finding counterfeit railway certificates, there hasn't been a violation in the case of Libert v. France.[26] The ECtHR ruled that action was not contrary to the Convention when a person was supervised on the job, in a limited time and space only around the cash register.[27] Violation of Article 8 was established when the supervised subjects were not informed about the hidden surveillance in accordance to domestic regulation.[28] The case of Alice Ross v. UK refers to information that is otherwise protected as a professional secret.[29] A person who was engaged in research journalism initiated a procedure because of monitoring the content of internet traffic.

In the case of Copeland v UK, there were discussions about telephone, internet and electronic mail monitored in the office.[30] The institution where the person was employed was overseeing how often she calls particular phone numbers, which web pages she visits, and to whom and when she sends e-mails. The goal was to determine whether or not she uses business facilities for private gains. The ECtHR found that the institution did not have a legal regulation that would proscribe this area and it was not known to the person that such controls would be possible. The ECtHR has determined that this is a matter of privacy. The Court concluded that it was not important at all whether the information was used against applicant in some form of proceedings. Just storing of data was already interfering with her private life. The ECtHR emphasized that there is a possibility that such a measure may be allowed and necessary in a democratic society, but only in certain situations and if prescribed by a law. In this particular case, there weren't regulations

23 Judgment *Trabajo Rueda v. Spain*, no. 32600/12, 30 May 2017
24 Judgment *Aycaguer v. France*, no. 8806/12, 22 June 2017
25 Judgment *Ivashchenko v. Russia*, no. 61064/10, 13 February 2018
26 Judgment *Libert v. France*, no. 588/13, 22 February 2018
27 Judgment *Köpke v. Germany*, no. 420/07, 5 October 2010
28 Judgment *López Ribalda v. Spain*, no. 1874/13, 9 January 2018
29 Judgment *Bureau of Investigative Journalism and Alice Ross v. UK*, no. 62322/14, 9 February 2016
30 Judgment *Copeland v UK*, no. 62617/00, 3 April 2007

that would allow such an action. In England, legislation was subsequently passed to allow such actions.[31]

### 3.3. Other intrusive forms on privacy

Violations may also be committed by public disclosure of sensitive personal data.[32] It is the principle that Article 8 protects data that individuals can reasonably expect not to be published without their consent.[33] If the police are carrying out the actions for disclosing such information to the public, this could be a violation. This fundamental right encompasses the privacy of communication, which means the content of e-mail, ordinary mail, telephone and all other forms of communication.[34] The concept of private life also includes the right of the person to his image, photographs or videos containing his character. That also falls under Article 8 of the Convention, according to Sciacca v. Italy.[35] In the case of Khmel v. Russia,[36] the footage that was created in the police premises was then publicly released. In the Uzun v. Germany case,[37] it was found that surveillance over the GPS system and processing of the data also represents interference with private life.

In several pending cases, main problems were the issues of collecting user identity. The case of Benedik v. Slovenia refers to a file in which the police collected data on computer IP addresses without a court order.[38] The police, based on these data, revealed his identity using service provider. Similar pending case is Ringler v. Austria in which the identity of the person was also established using the data from internet service provider.[39]

## 4. RETENTION OF DATA

### 4.1. General remarks about retaining data

Part of the information on communication could be unavailable until the criminal investigation starts. Loss of data may be the result of some attempts by the perpetrators themselves, or it may be a consequence of the absence of a system that

---

31 Telecommunications (Lawful Business Practice) Regulations 2000

32 Case VSRH, I Kž-562/1996

33 Judgment *Flinkkilä and Others v. Finland*, no. 25576/04, 6 April 2010, par. 75

34 Judgment *Copeland v UK*, no. 62617/00, 3 April 2007

35 Judgment *Sciacca v. Italy*, no. 50774/99, 11 January 2005

36 Judgment *Khmel v. Russia*, no. 20383/04, 12 December 2013

37 Judgment *Uzun v. Germany*, no. 35623/05, 2 September 2010

38 Pending case *Benedik v. Slovenia*, no. 62357/14

39 Pending case *Ringler v. Austria*, no. 2309/10

would retain such data. After the insight into the way of preparing and communicating between the terrorists, agencies came up with ideas about increasing the possibility of retaining data. It was established that terrorists often used the Internet for communications, propaganda or funding.[40] On the European level, there has been adopted the relevant Directive on data retention (DRD).[41] In Article 14 of the DRD, it was stipulated that States may initiate their retention programmes.

Although the DRD has roots in aftermath of Madrid attacks, and in the Declaration on Combating the Terrorism, this disputed regulation has come to criticism from the beginning. After the introduction by the four states, the European Parliament has refused to enforce such rules. The blocking was based on the view that such measures represent an effect that hasn't been fair balanced. Contemporary profiling capabilities could link insight into various privacy areas. Some critics elaborate that about half a year of retention of data, collects approximately 35,000 entries per person.[42]

### 4.2. Investigative needs for data retention

Data retention allows finding the data of perpetrators who were not suspicious nor detectable at the time of communication. Technologies are giving opportunity of very good covering of perpetrators. Sometimes devices that are not linked to suspicious subjects are used. Perpetrators can easily change a mobile device or identifying features. One example is purchasing mobile phones that are only used for one crime. An example may be opening new e-mail address or new connection that is not linked to the IP addresses of the earlier perpetrator's link. Such examples already appeared in the police practice so far.

Collecting data only focused on known former suspects' communications would not have a positive result. Compared to some of the classic investigative measures, it would be like search of the apartment used by the perpetrator during his last known criminal offense. As a perpetrator constantly changes apartments, similarly is with communication devices. Perpetrators that are the most difficult to detect are constantly adjusting to the investigative methods used by the police force.

---

40 Brown, I., Korff, D., *Terrorism and the proportionality of Internet surveillance*, European Journal of Criminology, vol. 6, no. 2, 2009, pp. 119-134

41 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, OJ L 105 (DRD)

42 Loideain, *op. cit.* note 2

In assessing how much this kind of collecting restricts the fundamental rights of citizens, it is not easy to reach a definite conclusion. Namely, although some critics point out very extensive features of profiling people online,[43] part of this is exaggeration and part this does not stem from data retention, but rather from social networks. These powers do not allow the police or some other agency to use the entire retention data permanently. Critics nevertheless state that the aggregation of such data is revealing many personal details to the authorities.[44] However, they ignore that the police or other agency may have access to such data only when it is in accordance with the legal provisions.

Data collected on retention policies do not restrict the privacy area at a level comparable to the one that could be gathered from the content of communication. Contact metadata does not give the meaning of communication. For example, if a police collects data that two entities have communicated over a given period, it is not known what their relationship was. It may be perhaps one of the subjects is trying to avoid such communication. They might be talking about a crime, or maybe about some purely legal deal. The data being retained gives only a superficial description.

By using other actions such are home search or surveillance of telecommunications, much more data can be discovered. Searching a computer or a cell phone may give more private information than data retention. Furthermore, citizens leave more data themselves on social networks. From such data it is possible to profile persons in a more reliable way than it would be ever possible using retention. This is shown recently in notorious examples of exploitation of some social networks by analytical companies.

According to types of criminal offenses for which retention data was used, only 6% of cases were used for investigating terrorism. About 30% were used to investigate property crimes, about 25% for murder investigations, and about 11% for child pornography.[45] In publication it is written that 82 cases were resolved based on historical data in retention. The only terrorist investigation on the basis of these data was a bombing in London, when five perpetrators were arrested.[46]

---

43 Schneier, B., *Data and Goliath,* Norton, New York, 2015

44 Solove, D., *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, New York, 2004

45 Communication from the Commission to the European Parliament, The European Council and the Council, *Ninth progress report towards an effective and genuine Security Union*, COM(2017)407

46 Duport, Y., *A Case Study of the Security-Privacy Shift in the EU Data Retention Directive*, Faculty of Social and Behavioral Sciences, Leiden, 2015

### 4.3. The ECtHR case-law on retention of data

The ECtHR has dealt with retention of data in some other cases. It was not about general retention but about personal data and police databases. The ECtHR considers part of the privacy as to how certain personal data is kept in police databases and is a person able to initiate the procedure for their erasure. The ECtHR takes the view that any retention, analysis or storage may constitute a breach of privacy rights. In several French cases, persons considered that their privacy was violated when data were entered into a national base of sexual offenders, although the base was founded years after they had been convicted. Cases B.B. v. France and Gardel v. France concerned the retention of data on sexual offenses, and the ECtHR concluded that retention periods were from 20 to 30 years, but depending on the seriousness of the criminal offense.[47] There was no violation since they could have requested the deletion. In case of Brunet v. France data have been retained for more than 20 years, although the criminal proceedings were suspended.[48] In the case of Khelili v. Switzerland, there were retained data about suspicion on prostitution, irrespective of lack of judicial verdict.[49] The case of Dalea v. France considered that rights were violated because data entered in the Schengen Information System was obstacle to obtain a visa in certain countries.[50] In the M.M. v. UK, the person objected to retention of data in police bases concerning a reported crime of kidnapping.[51] The ECtHR concluded that the system should have safeguards against the disclosure of sensitive personal data in public.

The retention of certain data in police bases regarding the identification of persons was also observed. In the Kinnunen v. Finland case, retention was related to photos of suspects and theirs fingerprints taken after arrests.[52] In the case Van der Velden v. Netherlands, the Court had given conclusion that storing of the DNA profile was not like storing some neutral features but content that was intrusive to personal life.[53] Key decision in this field was S. and Marper v. UK.[54] In that case, retention is observed in relation to law which proscribed securing the DNA profile of a person on indefinite term, irrespective of the seriousness of the criminal offense. The Court concluded that it is the disproportionate interference of

---

47 Judgment *Gardel v. France*, no 16428/05, 17 December 2009; Judgment *B.B. v. France*, no. 5335/06, 17 December 2009

48 Judgment *Brunet v. France*, no. 21010/10, 18 September 2014

49 Judgment *Khelili v. Switzerland*, no. 16188/07, 18 October 2011

50 Judgment *Dalea v. France*, no. 964/07, 2 February 2010

51 Judgment *M.M. v. UK*, no. 24029/07, 13 November 2012

52 Commission decision *Kinnunen v. Finland*, no. 24950/94, 15 May 1996

53 Judgment *Van der Velden v. Netherlands*, no. 29514/05, 7 December 2006

54 Judgment *S. and Marper v. UK*, [GC] Nos. 30562/04 and 30566/04, 4 December 2008

the authorities with the rights of privacy. For this area, valuable decision is MK v. France about retaining of the fingerprint samples during suspicion of theft, but person was never charged for the crime. The ECtHR concluded that there hadn't been fair balance.[55]

### 4.4. The ECJ's position on retention of data

The European Court of Justice has established that there is a violation of privacy in the DRD provisions because the grounds for retention of data were not specified (C-594/12, C-293/12).[56] The development in this area shows that legal regulation in many systems still requires appropriate standardization in the design, conditions for implementation, and usability of results. The ECJ found that the DRD covers all persons and all forms of electronic communication without any differentiation, limitation and exceptions. This applies also to persons for whom there is no evidence of a link with serious crime.

It also covers persons who are otherwise protected under domestic law, such as examples of subjects who have a duty to keep a professional secret (medics, lawyers etc.). The ECJ has complained that the DRD is not related to any period or geographical zone, or to some of the persons contributing to the crime. A further objection is that the DRD does not contain any substantive or procedural conditions as to how the domestic police or other authorities access the data. There is no requirement for the subjects that would have access to data, or whether it is necessary to impose control by an independent body, judicial monitoring or any other. The DRD provides collecting data for a period of at least 6 to a maximum of 24 months, but without criteria to determine the length in particular circumstances. The ECJ found that the DRD does not have precise rules on interference in the fundamental rights of the Charter. The innocent citizens could be stigmatized, because they are treated the same as the perpetrators.[57]

Several factors contributed to this ECJ decision. It has certainly been inspired by the findings of some former members of the intelligence services on levels of overall communication surveillance.[58] Part of the reason is also in the change of

---

55 Judgment *M.K. v. France*, no. 19522/09, 18 April 2013

56 ECJ, Joined Cases C−293/12 and C−594/12, Digital Rights Ireland Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, and Seitlinger and others v Kärntner Landesregierung, Judgment of the Court (Grand Chamber), 8 April 2014

57 Boehm, F., Cole, M., *Data Retention after the Judgement of the Court of Justice of the European Union*, University of Münster, Münster, 2014

58 Loideain, *op. cit.* note 2

the TFEU whose Article 16 introduced new views on privacy,[59] as opposed to the former Article 286 of the TEC.[60] At a time when the ECJ made a decision, several more lawsuits were under way. Because of the lack of proportionality, the German Constitutional Court has marked unconstitutional provisions of the Telecommunications Act in which the DRD was transposed.[61]

### 4.5. Digital rights in relation to public available content

#### *4.5.1. Analysis of digital data*

Part of the data on social networks is publicly available, so it can be used for police investigation without procedural restrictions. Furthermore, there is a new concept of so called Big Data. Digital development and networking enables the processing of enormous amounts of data. Some of them can be used to build a person's profile. There are estimations that the whole Internet traffic has grown over 1 ZB (zettabyte) in 2016. The zettabyte is a measurement unit that follows after terabyte (TB), petabyte (PB) and exabyte (EB). To give some comparison, the IDC estimated that all hard drives in the world had approximately 160 EB in 2009.

In the Croatian legal system, there haven't been delivered decisions on methods of working with large amounts of data. Analysis of such data can be useful in prediction and proactive systems. The importance of this area for legal regulation has been confirmed by the Council of Europe.[62] Some theories criticize the analytics of Big Data due to the extensive intrusions on privacy.[63] However, the emergence of Big Data is a consequence of technological development rather than police powers. Police must use this field to adapt to the new digital environment.

#### *4.5.2. Development of new digital rights*

Some scholars or legal systems are already proposing new digital rights. One of them is the right to delete the search listings ('the right to be forgotten'), and the proposed right to data expire.[64] Application is elaborated on the case of a teacher who posted a picture of herself getting drunk.[65] As a consequence, university de-

---

59 TFEU - Treaty on the Functioning of European Union

60 TEC - Treaty Establishing the European Community

61 Bundesverfassungsgericht, BVerfG, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, 2 March 2010

62 Directorate General of Human Rights and Rule of Law, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 23 January 2017

63 Schneier, *op. cit.* note 43

64 Mayer-Schönberger, V., *Delete. The Virtue of Forgetting in the Digital Age,* Princeton, New Jersey, 2009

65 Case *Snyder v Millersville*, E.D. Pa., 2008

nied her a certificate for a teacher profession. Certain rights could be invoked by the DPD.[66] The General Data Protection Regulation will supersede the DPD from 2018. It is important that the GDPR in Article 17 prescribes the right to remove results from search engines, defined as right to oblivion.[67] The GDRP abolished the Directive with the aim of introducing higher level of protection. The application will not be absolute, there is an exception directed on the freedom of expression. Critics who were opposed to the introduction of such concept were considering that search engines will lose their neutral status. This right is not an *ex novo* right, it is complementary to previous ECJ decisions and development in legal theory. The GDPR rules were adopted one month after delivering the ECJ decision declaring the DRD invalid.[68]

The ECJ ruling C-131/12 (Google Spain) is relevant to the data listed from the internet search engine.[69] The decision partially accepts the right to be forgotten, but only in relation to the information on listing. Decision doesn't affect the original sources of data. The ECJ found that Internet search engines can be considered data controllers as they play a key role in dissemination of data. The case concerns a Spanish national who has become insolvent and therefore unable to pay the required taxes. His name was published on the public debtor's register. The person requested the deletion, but publisher refused because a list was part of the ministry's ad in journal. The applicant asked the Spanish Personal Data Protection Agency to remove the ad, but they replied that disclosure was legally justified.

Google has pointed out that they have no physical devices in Spain. Internet spiders searching for pages do not imply the use of devices in particular country. The Court found that there is an inextricably link between the headquarters and its subsidiaries. Regarding the protection of personal data, the Court has found that the right to personal data has a greater weight than the right of to access the data from the search engine. Google regularly publishes data on the number of

---

66 Directive No. 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

67 Regulation 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), COM/2012/010

68 Iglezakis, I., *The Right To Be Forgotten in the Google Spain Case (Case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?*, 4th International Conference on Information Law, 2014

69 ECJ, Case C−131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court (Grand Chamber), 13 May 2014

requests received to delete particular search results.[70] In some social networks it is unclear who could be considered as their controller. Some suggest the creation of a separate agency composed of representatives of government, companies and democratically elected representatives.[71]

Certain ECtHR pending cases are relevant in this area. In those cases, the perpetrators who served the sentence initiated a procedure aimed at blocking the data on the search engines. Those cases M.L. v. Germany and W.W. v. Germany are referring to famous German case of murder of an actor.[72] They intended to remove the publication of their verdict because they had served the sentence. The relationship to personal data in the German system has been governed by a famous Lebach's Case, which dates back to 1973. That case refers to the murder of German soldiers. Television intended to record a documentary with the name and the image of the perpetrator. The Federal Constitutional Court has determined that each individual can decide how much will be publicized.[73] In U.S. law it is quite different.[74] The publication of criminal records is protected by the First Amendment, which also served to refuse to delete two offenders from the known case of the Sedlmayr murder on Wikipedia.

## 5. CONCLUSION

Increased number of Internet data, as well as the widespread usage of mobile devices that unite various types of communication, lead to new issues regarding collection of evidence. In the past, people had rare photos of celebrations or perhaps personal diaries containing their memories, and nowadays the computer systems may register numerous events that are stored on social networks and other sources. Shaping an image of a person based on digital data, creates a new term of e-reputation, or the formation of a personal digital reflection. Data storage on computer disks works as a total memory - it does not distinguish between positive or negative events.[75] Given that people cannot influence the data memorization which is

---

70 Google, *Search removals under European privacy law. Transparency Report*, 2018 [https://transparencyreport.google.com/eu-privacy/overview] Accessed 1 April 2018

71 Lee, E., *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, University of California Davis Law Review, vol 49, 2016, pp. 1017-1095

72 Pending cases *M.L. and W.W. v. Germany*, nos. 60798/10 and 65599/10

73 Bundesverfassungsgericht, BVerfG, 1 BvR 536/72, 5 June 1973, Lebach I

74 Myers, C., *Digital Immortality vs. The Right to be Forgotten: A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy*, Romanian Journal of Communication and Public Relations, vol. 16, no 3, 2016, pp. 47-60

75 Terwangne, C, *The Right to be Forgotten and the Informational Autonomy in the Digital Environment*, Publications Office of the European Union, Luxembourg, 2013

published by others, such storage actually has the effect of permanent memory. That is why this area is very problematic from the perspective of privacy rights.

Perpetrators use computer capabilities for numerous types of criminal offenses and therefore police should focus on appropriate collection methods. One of methods is the retention of data of electronic communication, though most of such data will never be processed for some particular needs. Research findings show that retained data is still the most widely used for investigations of classical crimes, but not for countering terrorism. In countries where this area is not adequately regulated, proper arrangements are needed, regardless whether data do not present a serious intrusion in privacy. The emphasis should be placed on the conditions under which such data would be available to the police or other bodies.

A special challenge concerns private data that are voluntarily stored on social networks, but users do not have a full control over their further processing. In order to protect this part of the user's privacy, the social networking platforms should be regulated in more detail. Looking for solutions, it is apparent that many systems still have not found the optimal codification model because the attention was dedicated primarily to the police authorities, and not that much to private companies. This is a propulsive area where technology develops rapidly, and the law still seeks adequate responses.

## REFERENCES

### BOOKS AND ARTICLES


1. Bennett, S., *The "Right to Be Forgotten": Reconciling EU and US Perspectives*, Berkeley Journal of International Law, 30, 2012, pp. 161-195
2. Boehm, F., Cole, M., *Data Retention after the Judgement of the Court of Justice of the European Union*, University of Münster, Münster, 2014
3. Breyer, P., *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, European Law Journal, vol. 11, no. 3, 2005, pp. 365-375
4. Brown, I., Korff, D., *Terrorism and the proportionality of Internet surveillance*, European Journal of Criminology, vol. 6, no. 2, 2009, pp. 119-134
5. Duport, Y., *A Case Study of the Security-Privacy Shift in the EU Data Retention Directive*, Faculty of Social and Behavioural Sciences, Leiden, 2015
6. Guild, E., Carrera, S., *The Political Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*. Liberty and Security in Europe, CEPS Paper in Liberty and Security in Europe, no. 65, 2014
7. Iglezakis, I., *The Right to be Forgotten in the Google Spain Case (case C-131/12): A Clear Victory for Data Protection or an Obstacle for the Internet?*, 4th International Conference on Information Law, 2014

8. Karas. Ž., *Coherence of the Supreme court's case-law on admissibility of evidence from police inquiries,* Police and Security, vol. 17, no. 1, 2008, pp. 1-15
9. Koops, B., *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right to Be Forgotten in Big Data Practice*, SSRN Electronic Journal, vol. 8, no. 3, 2011, pp. 229-256
10. Kralj, T., *Examination of the Identity of Telecommunication Addresses in Criminal Practice*, Police and Security, vol. 18, no. 2, 2009, pp. 166-179
11. Lee, E., *Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten*, University of California Davis Law Review, vol. 49, 2016, pp. 1017-1095.
12. Loideain, N., *EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era*, Media and Communication, vol. 3, no. 2, 2015, pp. 53-62
13. Lynskey, O., *Control over personal data in a digital age*, Modern Law Review, vol. 78, no. 3, 2015, pp. 522-534
14. Mayer-Schönberger, V., *Delete. The Virtue of Forgetting in the Digital Age*, Princeton, New Jersey, 2009
15. Myers, C., *Digital Immortality vs. The Right to be Forgotten: A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy*, Romanian Journal of Communication and Public Relations, vol. 16, no. 3, 2016, pp. 47-60
16. Schneier, B., *Data and Goliath*, Norton, New York, 2015
17. Solove, D., *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, New York, 2004
18. Terwangne, C, *The Right to be Forgotten and the Informational Autonomy in the Digital Environment*, Publications Office of the European Union, Luxembourg, 2013
19. Vervaele, J., *Terrorism and information sharing between the intelligence and law enforcement communities in the US and the Netherlands: emergency criminal law?* Utrecht Law Review, vol. 1, no. 1, 2005, pp. 1-27

## ECHR CASE-LAW

1. Aycaguer v. France, no. 8806/12, 22 June 2017
2. B.B. v. France, no. 5335/06, 17 December 2009
3. Bărbulescu v. Romania, no. 61496/08, 5 September 2017
4. Benedik v. Slovenia, no. 62357/14
5. Brunet v. France, no. 21010/10, 18 September 2014
6. Bureau of Investigative Journalism and Alice Ross v. UK, no. 62322/14, 9 February 2016
7. Copeland v UK, no. 62617/00, 3 April 2007
8. Dalea v. France, no. 964/07, 2 February 2010
9. Flinkkilä and Others v. Finland, no. 25576/04, 6 April 2010
10. Gardel v. France, no 16428/05, 17 December 2009
11. Halford v. UK, no. 20605/92, 25 June 1997
12. Ivashchenko v. Russia, no. 61064/10, 13 February 2018

13. Kennedy v. UK, no. 26839/05, 18 May 2010
14. Khelili v. Switzerland, no. 16188/07, 18 October 2011
15. Khmel v. Russia, no. 20383/04, 12 December 2013
16. Kinnunen v. Finland, no. 24950/94, 15 May 1996
17. Köpke v. Germany, no. 420/07, 5 October 2010
18. Libert v. France, no. 588/13, 22 February 2018
19. López Ribalda v. Spain, no. 1874/13, 9 January 2018
20. M.K. v. France, no. 19522/09, 18 April 2013
21. M.L. and W.W. v. Germany, nos. 60798/10 and 65599/10
22. M.M. v. UK, no. 24029/07, 13 November 2012
23. Malone v. UK, no. 8691/79, 2 August 1984
24. Ringler v. Austria, no. 2309/10
25. Roman Zakharov v. Russia, no. 47143/06, 4 December 2015
26. S. and Marper v. UK [GC] Nos. 30562/04 and 30566/04, 4 December 2008
27. Sciacca v. Italy, no. 50774/99, 11 January 2005
28. Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016
29. Trabajo Rueda v. Spain, no. 32600/12, 30 May 2017
30. Uzun v. Germany, no. 35623/05, 2 September 2010
31. Uzun v. Germany, no. 35623/05, 2 September 2010
32. Van der Velden v. Netherlands, no. 29514/05, 7 December 2006
33. Youth Initiative for Human Rights v. Serbia, no. 48135/06, 25 June 2013

## ECJ CASE-LAW

1. ECJ, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others, and Seitlinger and others v Kärntner Landesregierung, Judgment of the Court (Grand Chamber), 8 April 2014
2. ECJ, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court (Grand Chamber), 13 May 2014

## LIST OF NATIONAL REGULATIONS

1. Police Affairs and Authorities Act, Official Gazette No. 76/2009, 92/2014
2. Criminal Procedure Act, Official Gazette No. 152/2008, 76/2009, 80/2011, 121/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017
3. Electronic Communications Act, Official Gazette No. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017

## COURT DECISIONS


1. Case VSRH, I Kž 1162/04
2. Case VSRH, I Kž 598/12
3. Case VSRH, I Kž-Us 21/13
4. Case VSRH, I Kž Us 23/09
5. Case VSRH, I Kž-144/05
6. Case VSRH, I Kž-562/1996


## WEBSITE REFERENCES


1. Google, Search removals under European privacy law. Transparency Report, 2018, [https://transparencyreport.google.com/eu-privacy/overview] Accessed 1 April 2018