sciendo

Data Protection in Law Enforcement and Judicial Cooperation in Criminal Matters

Rastislav Funta
Peter Ondria

Danubius University
Richterova 1171
Sládkovičovo 925 21, Slovak Republic
Email: rastislav.funta@vsdanubius.sk
Email: peter.ondria@vsdanubius.sk

Abstract: The redesign of data protection in the police and judicial area is intended to create uniformity at the European level for the citizens of EU Member States. This scientific article analyses the subject of data protection in law enforcement and judicial cooperation in criminal matters. The focus is primarily on the existing provisions and the latest developments of the EU with regard to Directive (EU) 2016/680 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. The international level with regard to data protection in the police and judicial area and possible changes due to the developments in data protection under European law are also examined in more detail.

Keywords: *criminal matters, data protection, police and judicial cooperation*

doi: 10.2478/bjes-2021-0019 TalTech Journal of European Studies
Tallinn University of Technology (ISSN 2674-4619), Vol. 11, No. 2 (34)

1. Introduction

Specific legal instruments have been developed in order to balance the interests of individuals in the protection of their data and the interests of society in data collection for the purposes of fighting crime and ensuring national and public security. In regard to the police and criminal justice, the Modernized Convention no. 108 (Convention for the Protection of Human Beings with regard to Automatic Processing of Personal Data) covers all areas of processing of personal data at the European level and its provisions are designed to regulate the processing of personal data in general. As a result, Modernized Convention no. 108 applies to data protection in the police and criminal justice sectors. The processing of genetic data, personal data in connection with criminal offenses, criminal proceedings, convictions and related security measures, biometric data for the unambiguous identification of a person and sensitive personal data is permitted if suitable measures are taken to counter the risks associated with the processing of this data. This article deals exclusively with the subject of data protection in the police and judiciary. The most important terms are explained in advance to ensure a better understanding of the topic. Thus, the focus is primarily on the existing provisions and the latest developments of the EU with regard to Directive (EU) 2016/680. In the following we will also try to give an answer to the question, among others, as to whether the fundamental right under Article 8 of the EU Charter of Fundamental Rights (Tzanou, 2013), is also applicable to the conditions and restrictions created by secondary law for criminal cooperation between the police and the judiciary.

2. Objective and methodology

Our research question is whether the current data protection in the police and judicial area is still able to create uniformity at the European level for the citizens of the EU Member States or whether it requires modifications. The data was collected from legislation, respective case-law through in-depth document analysis and is supported by scientific literature. The main objective of the article is to analyse existing law enforcement and judicial cooperation in criminal matters and to clarify the limits with regard to challenges in connection with data protection (Plavčan & Funta, 2020). We want to achieve our objective particularly through a study of legislation,

scientific literature, as well as case-law. Several scientific methods of knowledge have been used in the exploration and development of our article. We applied the method of analysis in order to examine the state regarding data protection in law enforcement and judicial cooperation in criminal matters. The synthesis will allow us to combine partial information into a single unit. By applying a comparative method we also take a different view from the EU and international perspective, which has allowed us to obtain reliable and valid conclusions and results.

3. Data protection in the police and judiciary at the European level

3.1 The right to respect for private life according to Article 8(1) European Convention on Human Rights

Within the EU, there are general legal principles for data protection in addition to primary and secondary law. Article 8 of the EU Charter of Fundamental Rights (CFR) (Yara *et al.*, 2021) and (indirectly) Article 8(1) of the European Convention of Human Rights (ECHR) are the most important norms of European primary law (Erdősová, 2010). The ECHR forms the basis for the jurisprudence of the European Court of Justice (ECJ) by the general legal principles (Mazák & Jánošíková, 2009) according to Article 6(3) of the Treaty on European Union (TEU). According to Article 8(1) of the ECHR, "[e]veryone has the right to respect for his private and family life, his home and his correspondence." Even if a data protection law and a right to informational self-determination are not expressly stated, these areas are included due to the broad interpretation of the article by the European Court of Human Rights (ECtHR). Article 8(1) of the ECHR gives rise to a right of defense against state interference on the one hand, and the state's obligations on the other. Thus, if the data of a person concerned is collected, stored, used, processed or passed on, this is already an encroachment of Article 8(1) of the ECHR.

The ECtHR confirmed data protection in Article 8(1) of the ECHR in a number of decisions. For example, the ECtHR was of the opinion that the processing of personal data, both through inclusion in a separate file in a secret police register (*Leander v. Sweden* [1987]) and through official secret surveillance measures (*Leander v. Sweden* [1987]), constitutes an encroachment on the scope of protection of Article 8(1) of the ECHR. The disclosure of data from a secret police register (*Leander v. Sweden* [1987]) or medical data without the

consent of the person (*Peck v. The United Kingdom* [2003]) concerned and the inspection of files of personal data (*Gaskin v. The United Kingdom* [1989]) is also in line with Article 8(1) of the ECHR. Information about business activities (*Kopp v. Switzerland* [1998]) or political actions of individuals (*Rotaru v. Romania* [2000]) is also seen as protected data. The form of data processing is also irrelevant. This is due to the fact that all types of personal data processing fall within the scope of data protection according to Article 8(1) of the ECHR.

The ECtHR has repeatedly stated that the storage and retention of personal data by police or national security authorities constitute an interference with Article 8(1) of the ECHR. Many of the judgments of the ECtHR deal with justifying such interventions (see, e.g., *M.K. v. France* [2013] or *Aycaguer v. France* [2017]). For example, in *S. and Marper v. The United Kingdom* [2008], both applicants had been charged with, but not convicted of, certain offenses. Regardless, the police kept their fingerprints, cell samples and DNA profiles on file. The unlimited storage of biometric data was legally permissible if a person was suspected of a criminal offense. The ECtHR ruled that the storage of personal data which was not limited in time constituted a disproportionate interference with the complainants' right to respect for private life (Carpenter, 2020).

3.2 The informational self-determination and claims by the affected

Article 8(1) of the ECHR states that everyone is free to decide whether or not to hand over its personal data. This privilege is called the autonomy of the individual. It is about informational self-determination, which guarantees a right to defend against state interference in the privacy of the individual. This brings the general privacy protection together with the fundamental right to data protection (Stehlík, 2009).

Article 8(1) of the ECHR does not explicitly name claims of those who may be affected. Nevertheless, information (Neszméry, 2019), correction and deletion claims can be derived from the data protection standards. In the Gaskin case, the ECtHR was of the opinion that, depending on the individual case, a decision must be made as to whether the person concerned has an option to inspect the files (*Gaskin v. The United Kingdom* [1989]). A such right of those affected to access the files is therefore not derived from Article 8(1) of the ECHR. In addition, the ECtHR took the view that, under certain conditions, access to the files requires the consent of the person who

submitted the information. If the informant's consent is unjustifiably not given or if the informant's consent is not made, an independent authority decides whether to inspect the files. A major issue, in connection with electronic communication (Šramel & Horváth, 2021), is interference with the rights to privacy and data protection by authorities. Tools for monitoring or intercepting communication are only permitted if they are necessary in a democratic society for the protection of the security of the state (Bakkar & Ögcem, 2019), public order, the economic well-being of the country, prevention of crime, or the protection of the data subject or the rights and freedoms of others. Numerous judgments by the ECtHR deal with justifying interference with the right to privacy through surveillance. For example, in the case of *Roman Zakharov v. Russia* [2015], the plaintiff initiated legal action against three mobile network operators. He argued that his right to the privacy of his telephone communications was violated because the cellular operators installed devices that allowed the secret service to intercept his phone calls without prior judicial authorization. The ECtHR found that national law on interception did not provide adequate and effective safeguards against arbitrariness and the risk of abuse. In particular, the national legislation did not provide for the deletion of the stored data once the purposes for which the storage was carried out had been achieved. Also, in the case of *Szabó and Vissy v. Hungary* [2016], the applicants alleged that Hungarian law violated Article 8 of the ECHR because it was not sufficiently detailed and precise. It was also argued that Hungarian law did not contain sufficient guarantees against abuse and arbitrariness. The ECtHR found that under Hungarian law, surveillance does not require judicial authorization. The ECtHR also pointed out that the supervision required the approval of the Minister of Justice. In addition, national law does not guarantee judicial review, since it does not provide for notification of the persons concerned. The ECtHR found that there had been a violation of Article 8 of the ECHR.

4. Respect for private life according to Article 7 of the EU CFR

The EU Charter of Fundamental Rights also speaks about a right to respect for private life, which guarantees a fundamental right (Králik & Králiková, 2007) under data protection law. Nonetheless, there is an independent standard, Article 8(1) of the EU CFR, which concerns personal data protection. The protection of personal data falls under the privacy of the data

subject (Rotenberg, Horwitz & Scott, 2015) and thus Article 7 of the EU CFR applies to protection of personal data. However, there is a subsidiarity of Article 7 of the EU CFR compared to the *lex specialis* of Article 8(1) of the EU CFR. In line with Article 52(3) of the EU CFR, the grounds of restriction and justification for Article 7 of the EU CFR apply. Accordingly, the justification grounds of Article 8(2) of the ECHR in line with the EU CFR are to be interpreted teleologically.

5. Protection of personal data according to Article 8 of the EU CFR

Article 8 of the EU CFR focuses on the area of protection that is greater than that of Article 8(1) of the ECHR. This consists of the expressly mentioned right to the protection of personal data (*Productores de Música de España (Promusicae) v. Telefónica de España SAU* [2008]), the basic right to informational self-determination and positive protection. Article 8 of the ECHR and Article 8 of the EU CFR pursue the same goal and value for the personal data protection. Nevertheless, Article 8 of the EU CFR represents an extended basic right to the protection of personal data (Karácsony, 2019), which, due to the different structure and content, goes further than the claim to secrecy according to Article 8 of the ECHR. Thus, Article 8 of the EU CFR contains a subjective basic right to informational self-determination (Jankuv *et al.*, 2015) in the application of EU law in line with Article 51(1) of the EU CFR, which is enforceable against Member States of the EU as well as against the institutions of the EU (Stehlík, Hamuľák & Petr, 2017).

5.1 Restriction options

Article 8 of the EU CFR is based on Article 8 of the ECHR, but the former contains different safeguarding claims due to a different structure (Explanations relating to the Charter of Fundamental Rights). Accordingly, since Article 16(1) of the TFEU came into force, the special fundamental rights barrier under Article 52(2) of the EU CFR has to be used.

The question now arises as to whether the right under Article 8 of the EU CFR is also applicable to the conditions and restrictions created by secondary law for cooperation between the police and the judiciary under criminal law (Ivor, Klimek & Záhora, 2013). Personal data is an important tool when

fighting transnational crime and terrorism (Svoboda, 2009). However, the storage and processing of such information constitutes an impairment in Article 8(1) of the EU CFR. The introduction of Article 16(1) of the TFEU as a primary law for personal data protection can be seen as a response to the application of Article 8 of the EU CFR to conditions and restrictions created by secondary law of the police and judicial cooperation in criminal matters. Article 16(1) of the TFEU does not in itself constitute a fundamental right to data protection. The EU CFR and the TFEU are also at the level of primary law. They have priority over secondary EU law (Fenyk & Svák, 2008). Thus, the conditions and restrictions created in secondary law for the personal data protection can only be interpreted within the meaning of Article 8 of the EU CFR and Article 16 of the TFEU. As per the legal basis according to Article 16(2) of the TFEU, the secondary law is intended to give concrete form to primary law. Article 8(1) of the EU CFR does not provide a legal basis for this, but restrictions may be possible if the requirements of Article 8(2) of the EU CFR are met.

The ECJ in the Digital Rights Ireland cases (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014]) invalidated the Data Retention Directive because it created disproportionate and unjustified interference with the EU CFR provisions. In Tele2 Sverige (*Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* [2016]), the ECJ confirmed that data retention for the purposes of combatting crime violated the right to a private life. In late 2020, the ECJ delivered two judgments on data retention, national security and fundamental rights: joined cases of *La Quadrature Du Net and Others*, *French Data Network and Others*, and *Ordre des Barreaux Francophones et Germanophone and Others* (Quadrature Du Net) [2020] and *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others* [2020]. In both judgments, the ECJ ruled that the EU Privacy and Electronic Communications Directive (2002/58) (e-Privacy Directive) and the EU CFR generally prevent national law from enabling bulk data retention of traffic and location data. However, this will not apply if Member States can prove the existence of legitimate threats to national security (Iliopoulos-Strangas, Diggelmann & Bauer, 2010).

6. The EU data protection directive in the field of police and judiciary

6.1 Background of the EU data protection directive

As a result of the changes introduced by the Lisbon Treaty in the police and judicial area, the European Council took action on new data protection strategies at the Union level. As a result, the European Commission announced the procedure it had developed for a solid, more tailored and actionable personal data protection. The strategy presented in January 2012 consisted of the (GDPR) General Data Protection Regulation (Kesa & Kerikmäe, 2020) and the Data Protection Directive for Police and Criminal Justice Authorities (DPD-PaCJ). The DPD-PaCJ should expand the scope of its predecessor, Framework Decision 2008/977/Jl, regarding national and transnational processing of data (Andraško, Horvat & Mesarčík, 2019).

6.2 Scope of application

Article 16(2) of the TFEU serves as an important basis for the DPD-PaCJ. In the area of freedom, security and justice (FSJ), the Directive only extends to judicial co-operation in criminal matters in Chapter 4 and police co-operation in Chapter 5 of Title V of the TFEU (Müller-Graff, 2009). Chapter 3, i.e., judicial co-operation in civil matters, is not subject to the application of the DPD-PaCJ. Due to Recital 14 of the DPD-PaCJ, Chapter 2 of Title V of the TFEU on border control, asylum and immigration is also excluded from the applicability of the Directive. The distinction as to whether there is a criminal or administrative matter (Klimek, 2012) is also a problem of the DPD-PaCJ scope.

6.3 The data subject and his rights

The DPD-PaCJ defines some data subject rights. First of all, a data subject has the right to information according to Article 13 of the DPD-PaCJ. On the one hand, this right includes the right to have basic information from the person responsible or the data protection officer communicated to the data subject. On the other hand, the data subject must be informed about the reason of the processing of his personal data. Furthermore, he must be informed about his right to complain by the supervisory authority, and also about the right to information or deletion of his personal data (Gregušová *et al.*, 2005). In special cases, the data subject must be provided with further

information in accordance with Article 13(2) of the DPD-PaCJ. This includes the legal basis of the data processing, the duration of the data storage and possibly the data recipient. In addition, if necessary, further information must be disclosed if the person concerned does not know about the collection of the data. However, it is questionable to what extent the individual terms of Article 13(2) of the DPD-PaCJ, as in special cases, further information or if necessary, are to be interpreted. It is also uncertain whether the person responsible is obliged to inform the person concerned about his extended right to information within the meaning of Article 13(2) of the DPD-PaCJ. Article 14 of the DPD-PaCJ includes a right to information about the data processing of the person concerned towards the person responsible. This primarily includes the purpose and category of the data and the duration of the storage of the processed data. However, the right to information can be restricted by Article 15 of the DPD-PaCJ. The DPD-PaCJ does not show a deadline for providing the information, but we can assume that the response must be carried out immediately.

6.4 Controller and processor

Articles 19 to 34 of the DPD-PaCJ concern the area of regulation for controller and processor. In accordance with Article 19(1) of the DPD-PaCJ, the person responsible is obliged to adapt his procedure to professional technical and organizational methods so that he can guarantee that the data processing is performed in accordance with the guidelines. According to Article 20(2) of the DPD-PaCJ, the person responsible should also choose suitable technical and organizational methods so that only that part of the personal data is processed that is needed for the data processing purpose. The person responsible now has to create a directory of all processing activities in accordance with Article 24 of the DPD-PaCJ. He must provide this to the supervisory authority at any time. Another regulation for the person responsible is made in Article 27 of the DPD-PaCJ, which provides for a data protection impact assessment (DPIA). This must be done if data processing seriously endangers the rights and freedoms of the person concerned. Law enforcement agencies are required to conduct DPIA to analyse the risks and consequences of personal data processing in order to implement adequate mitigation techniques.

6.5 Data transfer to third countries and/or international organizations

Personal data transfer from Member States to third countries and/or international organizations is specified in Article 35-39 of the DPD-PaCJ. This is allowed if it is required for the purpose of the Directive in accordance with Article 35(1) of the DPD-PaCJ. The data must be handed over to a competent authority (Marquenie, 2017). For this purpose, an adequate level of data protection is required in the third country or at the international organization, which is decided by the European Commission on the basis of an adequacy decision in accordance with Article 36 of the DPD-PaCJ. However, the Directive does not regulate that the transfer of data by Member States and third countries should also be in accordance with the national transfer regulations. Article 37 of the DPD-PaCJ is applicable if there is no adequacy decision according to Article 36 of the DPD-PaCJ. Data may also be transferred to a third country and/or an International organization if a legally binding instrument provides an adequate level of data protection or if the person responsible in the third country or at the international organization accepts the necessary guarantees for data protection (Daňko & Žárská, 2019).

6.6 Implementation of the DPD-PaCJ

The implementation of the DPD-PaCJ is regulated in the final provisions. The framework decision 2008977/JI according to Article 59 of the DPD-PaCJ is repealed. In addition, existing special provisions, such as those relating to Europol or Eurojust, which concern personal data protection, according to Article 60 of the DPD-PaCJ, remain in place. Member States have to inform the EU Commission in accordance with Article 63(4) of the DPD-PaCJ about their national regulations, which they use to implement the DPD-PaCJ. The DPD-PaCJ is legally binding since May 6, 2016. However, the Member States have the option of establishing stricter data protection regulations in domestic law that go beyond the DPD-PaCJ.

7. Issues associated with the data protection directive

Undercover investigation is common in the fight against crime (Klátik, 2020). The data subject does not know about the processing of their personal data. Article 13(3) lit. (b) and (c) of the DPD-PaCJ and Article 15(1) lit. (b) and (c) of the DPD-PaCJ enable the authority to make arbitrary decisions on the restriction of the data subjects right to be informed. This means that the person concerned cannot check whether the authority is taking legal action. It is relevant to mention that Articles 13(4) and 15(2) of the DPD-PaCJ do not prescribe any decisive consideration for the individual case.

7.1 Safe Harbor ruling

In 2000, the EU concluded the Safe Harbor Agreement with the USA. The reason for this agreement was the creation of legal security in accordance with the European data protection directive for the transmission of personal data. However, in the 2015 Safe Harbor ruling, the ECJ ruled that the agreement is invalid (*Maximilian Schrems v. Data Protection Commissioner* [2015]). In this case, the ECJ examined whether the transfer of personal data to the United States under the Safe Harbor Agreement between the EU and the US was in accordance with EU data protection law. The ECJ declared the Safe Harbor adequacy decision invalid. This decision allowed international data transfers from the EU to organizations in the United States that were self-certified under the Safe Harbor system. According to the ECJ, the Safe Harbor system had several shortcomings that threatened the fundamental rights of EU citizens to the protection of privacy, the protection of personal data and the right to effective judicial redress. With regard to violations of privacy and data protection rights, the ECJ highlighted that United States law allows certain authorities to access and process personal data transferred by Member States to the United States. The ECJ concluded that a regulation which does not provide for the possibility of gaining access to personal data by means of a legal remedy or of having them corrected or deleted "violates the essence of the fundamental right to effective judicial protection anchored in Article 47 of the EU CFR". The court stressed that the existence of a judicial remedy to ensure compliance with the law is inherent in the nature of the rule of law.

7.2 The Umbrella Agreement

The Umbrella Agreement (the EU-US data protection agreement for the personal data exchange for law enforcement reasons) regulates the transfer of data in the field of combating terrorism and crime. The agreement was signed in September 2015 and aimed to create effective cooperation (Lacuška *et al*., 2021; Panevski *et al*., 2021; Peráček *et al*., 2020) between the US and the EU. However, it is questionable to what extent is the agreement compatible with EU law, i.e., whether the entire agreement would withstand an examination by the ECJ at all (Šmejkal & Svobodová, 2018). It is true that EU citizens have the option of bringing legal action before American courts if their rights are violated. The individual protection in the USA is only very minimal compared to the EU (Funta, 2011). Only the 4th Amendment, i.e., the fourth amendment to the US Constitution and the Privacy Act as of 1974, can be applied as the legal basis for such protection.

7.3 Transfer to third countries

The area of data transfer to third countries and/or international organizations is not regulated without problems. A weighing up is not required for all regulations in individual cases. The weighing-up clause in Article 35(3) of the DPD-PaCJ is not sufficient, as the remaining provisions do not relate to this need for weighing up in individual cases. There are often too general material requirements for data transmission to a recipient who does not have an adequate level of data protection. Article 38(1) lit. (d) of the DPD-PaCJ, i.e., the justification for the data transmission for the purposes listed in Article 1(1) of the DPD-PaCJ, is also viewed as problematic because it circumvents the adequacy decisions according to Article 36 of the DPD-PaCJ. There are therefore doubts as to whether this rule is in line with EU law. The ECJ will arguably deal with this question in the near future. The main problem is arguably that the transferring authority directs the transfer of personal data for its own benefit. As a result, the weighing of interests cannot be carried out objectively. In certain cases, the data protection supervisory authority must be informed, such as in Article 37(3) of the DPD-PaCJ (Hert & Sajfert, 2017).

8. Data protection in the police and justice at the international level

8.1 Protection of private life according to Article 17 of the International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) is one of the most important international standards that affects the protection of personal data (Vermeulen, de Bondt & Ryckman, 2012). Article 17 of the ICCPR includes the right to privacy, which includes data protection during data processing. Furthermore, Article 17(2) of the ICCPR guarantees every person concerned a right to legal protection against such interference. Article 17 of the ICCPR contains the right of the person concerned to determine whether his personal data is in automated databases of authorities. In addition, every data subject has the right to erasure and correction if the data was collected or processed unjustifiably or is incorrect. That is why every contracting state is obliged to ensure effective protection of processed data.

8.2 Restriction options

Article 17(1) of the ICCPR as an international norm only protects against arbitrary and illegal interference. Article 17 of the ICCPR does not contain a catalog of the possibilities of restriction in comparison to Article 8(2) of the ECHR. Indeed, the justifying interventions were defined by the Human Rights Conference of the United Nations. For the Human Rights Conference of the United Nations, the intervention is unlawful if there is no legal basis for it. This basis must be compatible with the provisions of the ICCPR and be consistent with the goals, purposes and views of the ICCPR. On the other hand, there is arbitrariness if the legal basis of the interference does not harmonize with the provisions of the ICCPR. The interference must therefore meet the objectives and purposes within the meaning of the ICCPR and must therefore not be disproportionate, but also fit with the national law of the respective state.

9. Conclusions

In order to be able to classify the data according to Articles 6 and 7 of the DPD-PaCJ in the police area, new information technology systems have to be created. Methods for search, police case processing, databases and police registers require further development. According to Article 11 of the DPD-PaCJ, decision-making based only on automated processing is prohibited. Such decisions must be unfavorable to the person concerned. In contrast, decision-making is permitted if either EU law or national law guarantees sufficient protection of the freedoms and rights of the data subject. Such automated approach can be seen in the use of intelligent video surveillance systems. Big data analyses are also part of automated decisions. A large number of data sources are analysed and summarized. Such analyses are intended to investigate suspects more quickly by making it possible to identify certain patterns from the criminal proceedings (so-called profiling).

In summary, it can be stated that the introduction of the DPD-PaCJ creates a minimum standard for data protection in the EU Member States (Kováčik, 2010). In regard to the impact of COVID-19 on criminal prosecution and the execution of sentences (Šmejkal, 2020), the situation has improved and it can be highlighted that there has been no major impact on the execution of judicial cooperation instruments (General Secretariat of the Council, 2021). It can be also stated that, on the one hand, the EU Member States are not restricted by the DPD-PaCJ. However, it is questionable whether the implementation of the Directive does not restrict the freedom of individual EU citizens (Pirošíková & Siman, 2012). The Directive does not create a supervisory state in the area of justice and police (Coutis, 2011), but the right to data protection is a highly sensitive issue. New procedures and instruments in the DPD-PaCJ lead to an expansion and changes in the judicial and police fields (de Hert & Papakonstantinou, 2016). Still, the aspect of a massive increase in administrative work, due to the categorization of personal data, can not be ignored. It is therefore important to meet the minimum standard of the DPD-PaCJ and to maintain the existing effective level of data protection in the judicial and police area, taking into account the data protection provisions at the European level. Thus, a redesign of data protection in the police and judicial area will create uniformity at the European level (Jakab *et al.*, 2021) for the citizens of EU Member States, which underpins their civil rights and protects them from misuse of their personal data.

Acknowledgment

The contribution is part of the project VEGA 1/0004/20 'Introduction of mutual recognition of judicial decisions in criminal matters into the legal order of the Slovak Republic'.

Rastislav Funta is an associate professor of EU law and international law at the Janko Jesensky Faculty of Law, Danubius University, Sladkovičovo, Slovak Republic.

Peter Ondria is an associate professor of theory of law at the Faculty of Public Policy and Public Administration, Danubius University, Sladkovičovo, Slovak Republic.

References

Andraško, J.; Horvat, M. & Mesarčík, M. (2019), *Vybrané kapitoly práva informačných technológií I* [Selected chapters of information technology law I], Bratislava: Comenius University.

Aycaguer v. France [2017], ECtHR, 8806/12, 22.7.2017.

Bakkar, Y. & Ögcem, A. R. (2019), 'Democracy and economic development: Disentangling the effect of elections and rule of law,' *Baltic Journal of European Studies*, vol. 9, no. 4, pp. 173–205. https://doi.org/10.1515/bjes-2019-0042

Carpenter, C. (2020), 'Privacy and proportionality: Examining mass electronic surveillance under Article 8 and the Fourth Amendment,' *International and Comparative Law Review*, vol. 20, no. 1, pp. 27–57. https://doi.org/10.2478/iclr-2020-0002

Coutis, S. (2011), 'The Lisbon Treaty and the area of freedom, security and justice as an area of legal integration,' *Croatian Yearbook of European Law and Policy*, vol. 7, pp. 87–107. https://doi.org/10.3935/cyelp.07.2011.121

Daňko, M. & Žárská, P. (2019), *Data Protection vs. Intellectual Property: Computer Law, AI, Data Protection and the Latest Technological Trends*, Brno: MSD.

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014], ECJ, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, 8.4.2014.

Erdősová, A. (2010), 'Právny zrod Charty základných práv EÚ—Pred a Po' [The legal birth of the EU Charter of Fundamental Rights—before and after], *Bulletin slovenskej advokácie*, nos. 9–10.

European Union (2007), Explanations relating to the Charter of Fundamental Rights, *OJ* C 303/17, 14.12.2007.

Fenyk, J. & Svák, J. (2008), *Europeizace trestního práva* [Europeanization of criminal law], Bratislava: Paneurópska vysoká škola (PEVŠ).

Funta, R. (2011), 'EU-USA privacy protection: Legislation and the Swift bank data transfer regulation: a short look,' *Masaryk University Journal of Law and Technology*, vol. 5, no. 1, pp. 23–33.

Gaskin v. The United Kingdom [1989], ECtHR, 10454/83, 7.7.1989.

General Secretariat of the Council (2021), *The Impact of COVID-19 on Judicial Cooperation in Criminal Matters: Executive Summary of Information Compiled by Eurojust and EJN*, 6178/1/21 REV 1.

Gregušová, D.; Dulak, A.; Chlipala, M. & Susko, B. (2005), *Právo informačných a komunikačných technológií* [Information and communication technology law], Bratislava: VO STU.

de Hert, P. & Papakonstantinou, V. (2016), 'The new police and criminal justice data protection directive: A first analysis,' *New Journal of European Criminal Law*, vol. 7, no. 1, pp. 7–19. https://doi.org/10.1177/203228441600700102

de Hert, P. & Sajfert, J. (2017), 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data,' in C. Brière & A. Weyembergh (eds.) *The Needed Balances in EU Criminal Law: Past, Present and Future*, Oxford: Hart Publishing, pp. 243–255.

Iliopoulos-Strangas, J.; Diggelmann, O. & Bauer, H. (2010), *Rechtsstaat, Freiheit und Sicherheit in Europa. Rule of Law, Freedom and Security in Europe. État de droit, liberté et sécurité en Europe*, Societas Iuris Publici Europaei, Bd. 6, Baden-Baden: Nomos.

Ivor, J.; Klimek, L. & Záhora, J. (2013), *Trestné právo Európskej únie a jeho vplyv na právny poriadok Slovenskej republiky* [Criminal law of the European Union and its influence on the legal order of the Slovak Republic], Žilina: Eurokódex.

Jakab, A.; Könczöl, M.; Menyhárd, A. & Sulyok, G. (2021), *Internet Jurisprudence: Encyclopedia*, Budapest: HVG-ORAC.

Jankuv, J.; Lantajová, D.: Šmid, M. & Blaškovič, K. (2015), *Medzinárodné právo verejné* [Public international law], Plzeň: Aleš Čeněk.

Karácsony, G. (2019), 'Managing personal data in a digital environment—did GDPR's concept of informed consent really give us control?' in *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy. Zborník príspervkov z medzinárodnej vedeckej konferencie. Vysoká skola Danubius* [Computer law, AI, data protection and the latest technological trends: Proceedings of

the international scientific conference, Danubius University], June 06 2019, Sládkovičovo, Slovak Republic, Brno: MSD, pp. 1–9.

Kesa, A. & Kerikmäe, T. (2020), 'Artificial intelligence and the GDPR: Inevitable nemeses?' *TalTech Journal of European Studies*, vol. 10, no. 3 (32), pp. 68–90. https://doi.org/10.1515/bjes-2020-0022

Klátik, J. (2020), *Trestné právo hmotné* [Substantive criminal law], Plzeň: Aleš Čeněk.

Klimek, L. (2012), 'Free movement of evidence in criminal matters in the EU,' *The Lawyer Quarterly*, vol. 2, no. 4, pp. 250–290.

Kopp v. Switzerland [1998], ECtHR, 23224/94, 25.3.1998.

Kováčik, B. (2010), 'Chosen aspects of EU institutional reform within the context of the Lisbon Treaty,' in G. Rouet & P. Terem (eds.) *L'Ukraine, entre integration et partenariat / Ukraine, Between Integration and Partnership*, Brussels: Bruylant.

Králik, J. & Králiková, K. (2007), *Základná inštitucionálna báza ochrany ľudských práv* [Basic institutional basis for the protection of human rights], Brno: Masaryk University.

Lacuška, M. & Peráček, T. (2021), 'Trends in global telecommunication fraud and its impact on business,' in N. Kryvinska & M. Greguš (eds.) *Developments in Information & Knowledge Management for Business Applications: Studies in Systems, Decision and Control*, vol. 330, Cham: Springer, pp. 459–485. https://doi.org/10.1007/978-3-030-62151-3_12

La Quadrature du Net (C-511/18 and C-512/18), French Data Network (C-511/18 and C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 and C-512/18), Igwan.net (C-511/18) v Premier ministre (C-511/18 and C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 and C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18), Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministers [2020], ECJ, Joined cases C-511/18, C-512/18 and C-520/18, *OJ* C-433/3, ECLI:EU:C:2020:791, 14.12.2020.

Leander v. Sweden [1987], ECtHR, 9248/81, 26.3.1987.

Marquenie, T. (2017), 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework,' *Computer Law & Security Review*, vol. 33, no. 3, pp. 324–340. https://doi.org/10.1016/j.clsr.2017.03.009

Maximilian Schrems v. Data Protection Commissioner [2015], ECJ, C-362/14, ECLI:EU:C:2015:650, 30.11.2015.

Mazák, J. & Jánošíková, M. (2009), *Základy práva Európskej únie* [Fundamentals of European Union law], Bratislava: Wolters Kluwer.

M. K. v. France [2013], ECtHR, 19522/09 final, 18.7.2013.

Müller-Graff, P. C. (2009), 'Der Raum der Freiheit, der Sicherheit und des Rechts' [The area of freedom, security and justice] (mit Friedemann Kainer), in W. Weidenfeld & W. Wessels (eds.) *Taschenbuch der europäischen Integration*, 11. Aufl., Berlin.

Neszméry, Š. (2019), 'Zverejňovanie fotografií osôb podozrivých zo spáchania trestného činu v médiách' [Publication of photographs of persons suspected of committing a crime in the media], in *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy. Zborník príspervkov z medzinárodnej vedeckej konferencie. Vysoká skola Danubius* [Computer law, AI, data protection and the latest technological trends: Proceedings of the international scientific conference, Danubius University], June 06 2019, Sládkovičovo, Slovak Republic, Brno: MSD.

Panevski, D.; Peráček, T. & Rentková, K. (2021), 'Analysis of the practices of financial intelligence units (FIUs) and other anti-money laundering agencies within EU,' in N. Kryvinska & A. Poniszewska-Marańda (eds.) *Developments in Information & Knowledge Management for Business Applications: Studies in Systems, Decision and Control*, vol. 376, Cham: Springer, vol. 376, pp. 241–269. https://doi.org/10.1007/978-3-030-76632-0_8

Peck v. The United Kingdom [2003], ECtHR, 44647/98, 28.1.2003.

Peráček, T.; Mucha, B. & Brestovanská, P. (2019), 'Selected legislative aspects of cybernetic security in the Slovak Republic,' in *Lecture Notes on Data Engineering and Communications Technologies*, vol. 23, pp. 273–282. https://doi.org/10.1007/978-3-319-98557-2_25

Pirošíková, M. & Siman, M. (2012), *Ludské práva: Vybrané rozhodnutia Európskeho súdu pre Íudské práva a Súdneho dvora Európskej únie* [Human rights: Selected judgments of the European Court of Human Rights and the Court of Justice of the European Union], Bratislava: Euroiuris.

Plavčan, P. & Funta, R. (2020), 'Some economic characteristics of internet platforms,' *Danube*, vol. 11, no. 2, pp. 156–167. https://doi.org/10.2478/danb-2020-0009

Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others [2020], ECJ, C-623/17, *OJ* C-22/29, ECLI:EU:C:2020:790, 6.10.2020, pp. 29–30.

Productores de Música de España (Promusicae) v. Telefónica de España SAU [2008], ECJ, C-275/06, ECLI:EU:C:2008:54, 29.1.2008.

Roman Zakharov v. Russia [2015], ECtHR, 47143/06, 4.12.2015.

Rotaru v. Romania [2000], ECtHR, 28341/95, 4.5.2000.

Rotenberg, M.; Horwitz, J. & Scott, J., eds. (2015), *Privacy in the Modern Age: The Search for Solutions*, New York & London: The New Press.

S. and Marper v. The United Kingdom [2008], ECtHR, Joined cases 30562/04 and 30566/04, 4.12.2008.

Šmejkal, V. (2020), 'Impact of the COVID-19 pandemic on European Antitrust. Mere adaptations or real changes?' Charles University in Prague Faculty of Law Research Paper, no. 2020/II/1. https://doi.org/10.2139/ssrn.3624824

Šmejkal, V. & Svobodová, M. (2018), 'ECJ's new role—guardian of open but not socially inclusive Europe?' *Eastern European Journal of Transnational Relations*, vol. 2, no. 2, pp. 11–32, https://doi.org/10.15290/eejtr.2018.02.02.01

Šramel, B. & Horváth, P. (2021), 'Internet as the communication medium of the 21st century: Do we need a special legal regulation of freedom of expression on the internet?' *The Lawyer Quarterly*, vol. 11, no. 1, pp. 141–157.

Stehlík, V. (2009), 'EU human rights protection under the Treaty of Lisbon,' in *Human Rights. The Modern State System's Formation: Theoretical and Practical Aspects*, Kyiv: Ukrainian Academy of Banking of the National Bank of Ukraine, pp. 123–127.

Stehlík, V.; Hamuľák, O. & Petr, M. (2017), *Právo Evropské unie: ústavní základy a vnitřní trh* [European Union law: Constitutional foundations and the internal market], Praha: Leges.

Svoboda, P. (2009), 'Znovu k hospodářské podpoře terorismu v judikatuře EU' [Revisiting the economic support of terrorism in EU case-law], *Trestněprávní revue*, no. 1.

Szabó and Vissy v. Hungary [2016], ECtHR, 37138/14, 12.1.2016.

Tele2 Sverige AB v. Post- och telestyrelsen and *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis* [2016], ECJ, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, 21.12.2016.

Tzanou, M. (2013), 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right,' *International Data Privacy Law*, vol. 3, no. 2, pp. 88–99. https://doi.org/10.1093/idpl/ipt004

Vermeulen, G.; de Bondt, W. & Ryckman, C., eds. (2012), *Rethinking International Cooperation in Criminal Matters in the EU. Moving Beyond Actors, Bringing Logic Back, Footed in Reality*, IRCP Research Series vol. 42, Antwerpen: Maklu.

Yara, O.; Brazheyev, A.; Golovko, L. & Bashkatova, V. (2021), 'Legal regulation of the use of artificial intelligence: Problems and development prospects,' *European Journal of Sustainable Development*, vol. 10, no. 1, pp. 281–289. https://doi.org/10.14207/ejsd.2021.v10n1p281