THE LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA IN INTERNATIONAL POLICE AND JUDICIAL COOPERATION

Matko Pajčić [*]

I. INTRODUCTION

The technical possibilities for the collection and processing of personal data in modern society are growing, and it is therefore clear that it is necessary to establish a proper legal framework and to protect citizens' privacy, and consequently to allow only the collection and storage of data that is absolutely necessary and justified in attaining a given objective.

On the other hand, there is no doubt that criminal groups, particularly in respect of transnational organized crime, are increasingly using technical resources. Because of this, and the cross-border nature of modern crime, it is clear that effective international cooperation between police and criminal law authorities has long become a necessity for the adequate protection of society from crime. The exchange of information between police and judicial authorities on the one hand contributes significantly to the protection of society against crime, while on the other it creates the need to raise the normative protection of citizens' personal data at the international level.

It is therefore not surprising that a number of international legal documents which govern the protection of personal data exist. In what follows, a brief, and therefore by no means comprehensive, overview of the normative regulations related to this issue in Europe will be presented, with reference to a selection of important legal sources of the European Union and the Council of Europe on three levels. The first level pertains to general documents about human rights including short general provisions about the need for the protection of privacy and the protection of personal data. The second level consists of legal sources which, in the most part, govern the protection of personal data; while the third level relates to sources where the subject of regulation is specifically the protection of personal data during operations by police and judicial authorities, as well as international cooperation related to these.

---

[*] Dr. Matko Pajčić, Assistant Professor, Faculty of Law, University of Split, Croatia. This article is a product of work which has been supported in part 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*.

II. GENERAL DOCUMENTS ON HUMAN RIGHTS AND THE PROTECTION OF PERSONAL DATA

Undoubtedly the most important document of the Council of Europe is the European Convention for the Protection of Human Rights and Fundamental Freedoms, which in Art. 8 guarantees the right to protection of personal data as part of the right to respect for private and family life, home and correspondence. This important provision was the basis for a series of decisions of the European Court of Human Rights, which judicial decisions illuminated many aspects, and also determined the limits, of the provisions of Art. 8, particularly issues related to the surveillance of communications and the storage and processing of personal data by police and judicial authorities.[1]

Unlike the ECHR, the most important general document on human rights within the European Union, the Charter of Fundamental Rights of the European Union, guarantees the protection of personal data, not only in Art. 7 (respect for private and family life), but also in the separate Art. 8, entitled 'Protection of Personal Data.[2] Some of the more important normative requirements are that such data must be processed fairly for specified purposes, on the basis of the concerned person's consent or on some other legitimate basis established by law. The Charter also provides that everyone has the right to access data collected about him/her and the right to correct it.

III. LEGAL SOURCES ON THE PROTECTION OF PERSONAL DATA

The law of the Council of Europe and the European Union contains a number of legal sources dealing exclusively with personal data protection. The importance of the Convention (no. 108) of the Council of Europe of 28 January 1981 on the protection of individuals during the automatic processing of personal data (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) is not merely that it was the first document that tried to systematically regulate the issue of data protection during automatic processing. This Convention was also adopted to ensure that the rights to privacy of individuals during the automatic processing of their per-

---

1 Some of these ECHR decisions are: Amman v. Switzerland [GC], 27798/95, 16 February 2000; Leander v. Sweden, 9248/81, 26 March 1987; M.K. v. France, 19522/09, 18 April 2013; Khelili v. Switzerland, 16188/07, 18 October 2011; Rotaru v. Romania [GC], 28341/95, 4 April 2000; Herczegfalvy v. Austria, 10533/83, 24 September 1992; Haralambie v. Romania, 21737/03, 27 October 2009; and many others.

2 It should not be surprising given the fact that the ECHR was adopted in 1950, and the Charter of Fundamental Rights of the EU in 2012, after the development of social awareness and international human rights law, when the right to protection of personal data was beginning to be considered as a special fundamental human right.

sonal data was respected in the territory of each state that was party to the Convention. Since the scope of its application extends to the public sector in addition to the private sector, the Convention governs the activities of judicial and police authorities. The Convention was amended in 1999 to allow the European Union to become a party. An additional protocol to the Convention, adopted in 2001, is very significant as it introduced provisions on cross-border transfer of data to non-member countries, so called third countries, and provisions on the mandatory establishment of national authorities responsible for data protection. The fundamental principles that the Convention sets forth are primarily related to the methods of collection and automatic processing of data stored for a specific legitimate purpose, which must be fair and lawful. It also determined that this personal data must not be used for purposes other than those which are legitimate and precisely defined, and that data may not be held longer than necessary. But the Convention also imposes some requirements regarding the quality of the data - which should be adequate, relevant and proportionate to the purpose for which they have been collected.

Furthermore, a very significant directive is Directive 95/46/EC of the European Parliament and 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[3], and Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies and on the free movement of such data[4]. There then followed the adoption of 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[5], 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, which did not pass the test of the European Court and is therefore invalid[6].

---

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

5 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.

6 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.

Because of the scope of this paper, below we will reflect only on those sources that relate directly to the activity of judicial and police authorities, international criminal law, and police cooperation in criminal matters relating to the protection of personal data, which are primarily the Prüm Convention and the so-called Prüm decision, and the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed within the framework of police and judicial cooperation in criminal matters, and two resolutions on the establishment of institutions: Council Decision of 6 April 2009 on the establishment of the European Police Office (Europol) and the Council Decision of 28 February 2002 on the establishment of Eurojust.

a) The Prüm Convention and the so-called Prüm decision

The Prüm Convention, adopted in 2005, was signed by 7 EU Member States, with the aim of developing cross-border cooperation particularly in combating terrorism, cross-border crime and illegal migration. Some of the ways of cooperation that the Convention provides for are the exchange of DNA profiles, fingerprints, information about the owners of motor vehicles, joint patrols along borders, the entry into and use of official arms of foreign police officers in the territory of another country, and cross-border pursuit. This Convention became part of the law of the European Union in 2008 under Council Decision 2008/615/JHA on the deepening of cross-border cooperation, particularly in combating terrorism and cross-border crime.[7]

b) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[8]

Compared to the previous law, the most important changes that this Framework Decision adopted concern the purpose of the collection and the principles of legality and proportionality. Such personal information may be collected by the competent authorities only for specific, clear and legitimate purposes within their tasks and may be processed only for the purpose for which the data was collected (Art. 3). The principle of proportionality is primarily reflected in the requirement that data processing must be proportionate to the purpose for which the data is collected. Regarding the restriction of the purpose for which the collected personal data may be used, it is provided that personal data received from another member state may be further processed

7 The decision, because of its content, is often called the Prüm decision.

8 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

only for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions and other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions.

The decision also envisages the possibility of transferring personal data to competent authorities in third countries or international bodies, but this is only allowed if it is necessary for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions; if the body that is the recipient in the third country or the international body that is the recipient is responsible for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions; if the member state from which the data was obtained has given its approval for the transfer in accordance with its national law and the third country or international body concerned ensures an adequate level of protection for the intended data processing.[9]

In addition to the obligations and limitations of government bodies, the decision expressly provides for some rights to persons whose data is collected and processed. He/she has a right to information about the processing of his/her data and has a right of access, correction, erasure or blocking. In order to ensure the exercise of this right, in the event that such rights are denied, he/she has the right to appeal to a competent national supervisory authority, being a judicial body or court.[10]

c) Council Decision of 6 April 2009 on establishing the European Police Office (Europol)[11] and Council Decision of 28 February 2002 on the establishment of Eurojust[12]

It is self-evident that the work of the two mentioned institutions is largely concerned with the exchange of information and collection of personal data, and that legal regulation of their work is therefore extremely important for the protection of citizens' personal data.

---

9 The decision imposes an obligation on member states to ensure one or more public authorities to be responsible for advising and monitoring the application of the provisions of the Framework Decision or for implementing regulations within its territory. These public authorities must be completely independent while performing these functions.

10 The better protection of rights will be ensured by the provision under which any person who has suffered damage as a result of treatment of unlawful processing or any action contrary to the national provisions adopted according to the Framework Decision is entitled to compensation for damage suffered by the supervising or other competent authority under national law.

11 Council Decision of 6 April 2009 establishing the European Police Office (Europol).

12 Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA).

d) Other sources of law and the protection of personal data

In order to legally regulate the accelerated and simplified procedure for the exchange of information and intelligence for the purpose of conducting criminal investigations or operations to collect intelligence information on criminal offenses, the European Union has adopted Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between the authorities responsible for the enforcement of law in EU member states.

Also significant for the legal regulation of personal data protection in judicial and police cooperation among the European countries are Council Framework Decision 2009/315/JHA on the organization and content of exchange of information from criminal records between member states, and the Council decision on the regulation of cooperation between financial-intelligence bodies of member states regarding the exchange of data.

Since this is a very dynamic legal field, its development is by no means complete. The European Commission, in 2012, proposed two new documents: the General Regulation on data protection and the General Directive on data protection. However, these proposals have not yet been adopted, and discussion on the most appropriate solutions still continues.

e) Case law of the European Courts

The European Court has, in a series of decisions, ruled on the issue of personal data protection in the EU. Some of the most important decisions are (in chronological order): Case C-101/01 Lindqvist [2003] ECR I-12971,[13] Case C-317/04 European Parliament v Council and Case C-317/04 European Parliament v Commission,[14] Case C-275/06 Promusicae [2008] ECR I-00271,[15] Case C-301/06, Ireland v. Parliament and Council,[16] C-524/06, Huber v. Germany,[17] Case T-194/04, Bavarian Lager Co. Ltd v. Commission,[18] Case C-28/08, European Commission v. Bavarian Lager Co. Ltd.,[19] T-259/03, Nikolaou v. Commission,[20] Case C-291/12 Michael Schwarz v. Stadt Bochum [2003] I-ECR 12971.[21] In the latter case, the claimant Mr Schwarz argued that

---

13 Judgment of the Court of 6 November 2003.

14 Judgment of the Court (Grand Chamber) of 30 May 2006.

15 Judgment of the Court (Grand Chamber) of 29 January 2008.

16 10 February 2009.

17 16 December 2008.

18 Judgment of the Court of First Instance of 8 November 2007.

19 Judgment of the Court, 29 June 2010.

20 12 September 2007.

21 Judgement of the Court (Fourth Chamber) of 17 October 2013.

Article 1(2) of Regulation 2252/2004, which requires mandatory fingerprinting of persons seeking a passport, was a violation of the right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU. The court did not accept his arguments and argued that these rights under the Charter were not absolute, but should be viewed and interpreted in view of their function in society. It added that the envisaged manner of storing fingerprints reduced the possibility of abuse and of counterfeiting passports, and, listing other arguments, rejected the claim.[22]

IV. FINAL COMMENT

Allow me to conclude this brief and partial review of the legislation which protects personal data in European procedures involving international legal cooperation with a short word about the great significance that the regulation of Eurojust, and the establishment of the European Public Prosecutor's Office, will have in the protection of personal data in investigations with an international element, and any legal assistance attached thereto.

[22] For a more detailed account of the above case, as well as all the above mentioned, v. Gutiérrez Zarza, Ángeles (Ed.) *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer-Verlag Berlin Heidelberg, 2015, p. 37-53.