Ana Batrićević*

THE PROTECTION OF THE RIGHT TO HUMAN DIGNITY IN THE CONTEXT OF THE EU POLICE (LAW ENFORCEMENT) DIRECTIVE

The right to privacy is closely interrelated with the right to human dignity. It is declared in numerous international legal documents, including those of the European Union. The intrusion of the right to privacy in the favor of public interests is particularly noticeable in the cases where personal data is processed by competent authorities such as the police and judicial bodies. European Union adopted the so-called Police Directive in 2016, the aim of which is to maintain a balance between the interest of crime prevention and security protection and the right to privacy in the sense of personal data protection. After defining privacy and its interrelation with the right to human dignity, the author analyzes the provisions of Police Directive, the relation between Police Directive and some other relevant sources of acquis, the significance of its provisions for Serbia and, finally, offers suggestions and recommendations for its more efficient application in the future.

Keywords: *privacy, human dignity, personal data, European Union, Police Directive*

* Ana Batrićević, PhD is a Senior Research Fellow at the Institute of Criminological and Sociological Research. E-mail: a.batricevic@yahoo.com

1. Introduction
The Right to Human Dignity and The Right to Privacy

Dignity is the characteristic of every free human being (Mitrović, 2016: 25). As an inherent feature of every person, dignity in the natural sense only partially overlaps with dignity in the formal or legal sense and turns into a legal value, derived from human nature as its primary source (Mitrović, 2010: 558–559). In modern democratic societies based upon the rule of law, the attitude of the state towards human dignity is considered particularly important, meaning that human dignity should be treated as the supreme value, whereas all other human rights should be understood as its core elements (Mitrović, 2016: 28).

The right to human dignity is indivisible from privacy, as one of fundamental human rights. For example, Bloustein argued that the invasion or the intrusion of privacy is closely intertwined with personhood, individuality and human dignity (Bloustein, 1964: 973-974, in: Lukacs, 2016: 258-259). Similarly, Dürig recognized several types of human dignity violations, including the violation of intimacy, i.e. privacy which he regarded as the key precondition for a person's integrity and identity (Dürig, 1998: 127–132, in: Mitrović, 2016: 30).

It can be said that privacy is actually as old as the mankind and it has known a long development (Lukacs, 2016: 256). However, what should be considered private significantly depends on several circumstances: the era, the society and the individual, and, a difference can be distinguished between what is considered private, on the one hand, and what is legally protected as private, on the other (Lukacs, 2016: 256). In 1890, Warren and Brandeis defined privacy as "the right to be let alone", i.e. the right to determine the extent to which the thoughts, sentiments and emotions of an individual (Bratman, 2002, 630-631) or the information about him or her (Westin, 2003: 432-453) can be communicated to others. In other words, privacy stands for an individual's option to limit the access that others have to his or her personal information as well as to conceal any information about himself or herself (Solove, 2008, in: Puaschunder, 2019: 64). Therefore, it can be argued that the introduction of "the right to be let alone" actually confirmed the need for the legal protection against the unwanted disclosure of private facts, thoughts and emotions (Lukacs, 2016: 258).

Nowadays, the amount of personal data that is being processed is rapidly increasing, particularly via social networking sites, location-based services, smart cards and cloud computing (Karovska-Andonovska, Kirkova, 2016: 80). Technology appears to be

eroding privacy in a much faster way than the legal system can provide adequate legislative frameworks and mechanisms for its protection (Holtzman, 2006: 15-19, in: Karovska-Andonovska, Kirkova, 2016: 80). Despite their numerous advantages, technological developments and innovations tend to threaten not only the right to privacy, but also the right to human dignity, which is highly correlated with privacy, especially in the cases where the public interests (such as crime prevention and public security) need to be protected. Namely, in some cases, the privacy of and individual has to be interrupted due to some more important, i.e. public interests, which means that, particularly from the standpoint of criminal law, not every invasion of privacy is illegal, even if it has been committed without a court permission (Pavlović, 2017: 224). That is when the issue of the balance between public and private interest emerges and there seem to be tendencies everywhere for fragile freedoms to be violated in the name of security, trust or anti-corruption (Buttarelli, 2017: 326).

Starting from the second half of the 20th century, the right to privacy became recognized as the first-generation human right in several international human rights conventions, of universal and regional scope of application, and its introduction into national legislations of states-parties to these conventions followed (Lukacs, 2016: 259). The European Union (hereinafter: EU) has also been dedicating a lot of attention to the issue of privacy and personal data protection, particularly in the past couple of years. The protection of personal data, which is of crucial importance for the protection of the right to privacy, and hence the right to human dignity as well, is analyzed in this paper, with the focus on particularly delicate cases – those involving the processing of personal data by the police and judicial authorities in the EU.

2. The Right to Privacy and Human Dignity in the European Union Law

The General Data Protection Regulation (GDPR, Regulation 2016/679)[1] (hereinafter: GDPR), in force since May 25th 2018[2], represents key source of *acquis* regulating the rights and obligations of data subjects (i.e. persons whose personal data are collected and processed) and data controllers (i.e. companies and governments that collect and process

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, accessed on 25.08.2020.

[2] GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN, accessed on 25.08.2020.

these personal data) (Custers et al., 2018: 235). The adoption of this document is considered by far the greatest effort to prevent the intrusions of the so called "technological hegemony" into citizens' privacy (Snowden, 2020: 342).GDPR constitutes the *lex generalis* in the legal framework for personal data protection (Kędzior, 2019: 506). Due to numerous specific characteristics, the protection of individuals' personal data when their data is being processed by the police and criminal justice authorities is regulated by another source of *acquis*, known as the Police or Law Enforcement Directive[3], the goal of which is also to improve cooperation in the field of combatting terrorism and cross-border crime in the EU by facilitating a more efficient and exchange of information necessary for investigations among police and criminal justice authorities in EU countries[4].

As parts of the EU data protection reform package, Police Directive and GDPR establish fundamental principles and minimal standards for personal data handling in the EU, with the purpose to guarantee the respect of individuals' rights, in particular the right to privacy (Karovska-Andonovska, 2013: 187-196). These sources of *acquis* are focused on the use of consent and personal data, providing data subjects with several rights, and introducing changes that prompted innovation within the EU, affecting both - the industry as well as the academic community (Pandit et al, 2018: 481-482). One of the most important instruments introduced by GDPR is the self-assessment of the digital risks and the modulation of the duties on the grounds of the impact assessment analysis, including special measures designed to preserve human dignity and fundamental rights of the data subject (Palmirani *et al.*, 2018: 139-140).

Despite the fact that it is not applied on data processing in the cases of public security protection and by the police and judicial bodies, GDPR is significant as a document that sets some general standards in the field of personal data protection, hence protecting privacy and human dignity in the context of data processing. That is the reason why some

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN, accessed on 28.08.2020.

[4] Protecting personal data when being used by police and criminal justice authorities (from 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_3&from=EN, accessed on 28.08.2020.

of its provisions significant for the protection of human dignity are briefly presented in this paper.

GDPR explicitly mentions the right to human dignity only in its Article 88, regulating the processing of personal data in the context of employment, prescribing that*: "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context…"* (Article 88 Paragraph 1). This particularly refers to the following purposes: "*the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and the termination of the employment relationship"* (Article 88 Paragraph 1).The right to human dignity is referred to in Paragraph 2 of Article 88, which emphasizes that the aforementioned rules have to include *"suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place".*

The cited provision contains two assumptions: 1) that the data subject has to be a human person, whose dignity is safeguarded (a legal person cannot enjoy human dignity) and 2) that human dignity is different from legitimate interests (Floridi, 2016: 307).Despite the fact that its presence in the GDPR is almost invisible, human dignity seems to represent the fundamental concept, providing the framework for the interpretation not only of GDPR but also of the European culture and jurisdiction in the area of informational privacy (Floridi, 2016: 307). Similarly to the cases regulated by the Police Directive, the cited provision of GDPR refers to the situations where there seems to be a conflict of interests: on one side, there is the interest of the employer to process employees' personal data for the aforementioned purposes, all of which are related to employment and work, whereas on the other, there is the interest of the employees to keep their privacy intact. In the Police Directive, the collision of interests refers to the interests of state bodies, such as judicial authorities and police, to prevent crime and maintain public security, on one side, and individual's interest to protect his or her privacy, on the other. But, while GDPR uses human dignity as the criteria to make a distinction between the acceptable and unacceptable intrusion of privacy for the sake of a "higher" interest, Police Directive does

not contain any provision explicitly mentioning human dignity or the right to human dignity. Also, in the cited provision of GDPR the interest in the favor of which individual's privacy is "sacrificed" (but only within the limits drawn by the right to human dignity) is the interest of the employer, who is not a state body, whereas in the cases regulated by the Police Directive, the advantage is given to public interest, i.e. the interest of state bodies and, in the broader sense, the entire state or society.

3. The Police Directive

3.1. The Adoption of the Police Directive – Background

The Police Directive was adopted as the replacement of the 2008 Data Protection Framework Decision[5] (hereinafter: DPFD) (Article 59, Police Directive), with the purpose to create a more comprehensive and reliable legal framework for data protection in the EU. The main reason for the adoption of DPFD was the intention to set minimal standards in the field of personal data processing by the police and criminal justice authorities (De Hert, Papakonstantinou: 2016, 8). However, its scope eventually became too restricted, the application of its principles was not properly enforced and it prioritized the needs of security instead of the rights of individuals, which led to the adoption of the Police Directive, as a means to correct these imperfections (De Hert, Papakonstantinou: 2016, 8). Namely, Article 16 B of the Treaty of Lisbon[6], which came into force, on December, 1st, 2009, actually required the re-establishment of the EU data protection standards (De Hert, Papakonstantinou: 2016, 8). According to Article 16 B of the aforementioned Treaty, *"Everyone has the right to the protection of personal data concerning them"* and the European Parliament and the Council have to lay down rules pertinent to *"the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data"*. Article 16 B also introduces the control of the application of the rules related to data protection by independent authorities.

[5] 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, OJ L 350, 30.12.2008, p. 60–71, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN, accessed on 27.08.2020.

[6] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/TXT&from=EN, accessed on 27.08.2020.

The establishment of a special regime at the EU level, regulating the protection of personal data processed by the police and judicial authorities is rational for two reasons: 1) the substantial one and 2) the formal one (Pejić, 2019: 3). The substantial reason is derived from the fact that state bodies in charge of law enforcement, unlike other entities, such as for example private companies or non-governmental agencies, collect and process personal data without the consent, and often without the knowledge of the citizens (Pejić, 2019: 3). Moreover, they do it for the cause of public interest, i.e. the prevention of criminality and other public safety risks (Pejić, 2019: 3). So, unlike general personal data processing, processing conducted by the police and judicial bodies and for the purpose of security protection has to be given a certain amount of flexibility (De Hert, Papakonstantinou: 2016, 9). Moreover, when it comes to the requirements related to the quality of data, they cannot be expected to be too strict in the cases when information are collected for the purpose of security protection, because they are often collected from undercover sources or rumors and based on "hearsay" (De Hert, Papakonstantinou: 2016, 9). Also, it is rather difficult to apply the principle of purpose limitations in these cases, since, for example, the information that is collected within one case might be used for resolving other related cases in the future (De Hert, Papakonstantinou: 2016, 9). Finally, it is also important to have in mind the fact that if the right to information and access (which is explained in details in the part of the paper dedicated to the most important provisions of PD) were respected to their fullest extent, no suspect surveillance operation could be conducted properly (De Hert, Papakonstantinou: 2016, 9).

The formal reason for choosing the form of a directive in this case comes from the fact that the jurisdictions of the EU in the field of cooperation between police and judicial bodies are relatively new and less strict in comparison to those related to the common market (on which GDPR is applied), giving the Member States more autonomy and freedom when it comes to regulating proceedings before judicial and police authorities in their national legislations (Pejić, 2019: 3). So, the choice to adopt the rules regulating the protection of personal data in the proceedings conducted by the police and justice authorities in the form of a directive was based upon the fact that a directive, as an instrument, gives Member States a certain amount of flexibility in the process of their incorporation into their national legislations (De Hert, Papakonstantinou: 2016, 9). Namely, a directive as a source of *acquis,* provides only binding frameworks and guidelines that have to be followed in national legislations, but its provisions are not applied directly (Pejić, 2019: 3).

3.2. The Police Directive and General Data Protection Regulation

It should be emphasized that the rules regulating the processing of personal data in the Police Directive are largely consistent with the general data protection norms laid down in GDPR (Kędzior, 2019: 508). However, there are some crucial differences between GDPR and PD. On the one hand, some segments of PD prescribe more flexible standards in comparison to those prescribed by the GDPR, whereas on the other, Police Directive contains some specific solutions designed to respond to the needs of state bodies in charge of law enforcement. (Pejić, 2019: 4).

Whereas the system of data protection established by the GDPR is based upon the assumption that the processing of personal data substantially depends on the consent of the personal data subject, this cannot be applied in the cases when personal data is processed within the activities of police or judicial authorities (Kędzior, 2019: 508). Therefore, in accordance with the principle of legality, such data has to be processed on the basis of a legal act and in harmony with the legal grounds established by that act, exclusively for the purpose of the accomplishment of particular tasks prescribed by the law (Kędzior, 2019: 508).

Furthermore, Police Directive does not insist on the transparency of personal data processing, it minimizes the obligation to reduce the quantity of collected personal data to the necessary minimum, it allows much more severe limitations of the rights of personal data subjects and only generally regulates the jurisdictions of relevant supervisory bodies of Member States (Pejić, 2019: 4). In addition, Police Directive contains some provisions that are designed exclusively for the field of law enforcement and, as such, do not have their equivalents in the GDPR, such as: the obligation to categorize persons and their personal data, the obligation to collect information about each individual approach to data and processing of data as well as the obligation to determine time frames for the conservation of personal data (Pejić, 2019: 4).

Also, the Police Directive insists that Member States should make a clear difference between various categories of data subjects. However, the actual implementation of this provision and therefore the final decision about which data shall be processed in relation to a given data subject stays within the jurisdiction of Member States (Kędzior, 2019: 508).

It should be noted that GDPR and Police Directive are not the only new sources of *acquis* dealing with the issue of data protection. Namely, Regulation 2018/1725 on the protection

of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and the free movement of such data and repealing the Regulation No 45/2001[7] became effective as of 12 December 2018. Its goal is to harmonize the principles of data protection within the EU institutions and to strengthens the role of the European Data Protection Supervisor (Kędzior, 2019: 508). It should also be highlighted that the revised Regulation will apply to Eurojust after the reform of this agency is completed and that in 2022, the rules should be extended to Europol and the European Public Prosecutor's Office (Kędzior, 2019: 508).

3.3. Key Standards of The Police Directive

Police Directive regulates the protection of natural persons' rights in the cases when their personal data are processed by competent authorities for the following purposes: 1) the prevention, investigation, detection or prosecution of criminal offences, 2) the execution of criminal penalties and 3) the safeguarding against and the prevention of threats to public security (Article 1, Paragraph 1). It obliges the EU Member States to: 1) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and 2) ensure that the exchange of personal data by competent authorities within the EU, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data (Article 1 Paragraph 2). Police Directive sets minimal standards in this field, allowing the Member States to provide higher safeguards for the protection of the rights and freedoms of the data subject in the cases of their processing by competent authorities (Article 1 Paragraph 2).

So, Police Directive is applied to the processing of personal data by competent authorities solely for the purposes explained in Article 1 (Article 2 Paragraph 1), to the processing of personal data either entirely or partially by automated means, or to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Article 2 Paragraph 2). However, the Directive is not applied if the processing of personal data is conducted: 1) within an activity which falls outside the scope of EU law and 2) by the EU institutions, bodies, offices and agencies (Article 2 Paragraph 2). In accordance with Article 3 Paragraph 7 of the Police

[7] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725&from=EN, accessed on 31.08.2020.

Directive, Competent authorities refer to the following entities: 1) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; and 2) any other body or entity authorized by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Police Directive defines personal data in Article 3 Paragraph 1, as any information relating to an identified or identifiable natural person (which it refers to as "data subject"), i.e. an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. According to Article 3 Paragraph 2, processing includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

In its Article 4, Police Directive sets several principles that have to be followed in the cases when personal data are processed by competent authorities for the previously mentioned purposes. First of all, personal data must be processed lawfully and fairly. They can be collected only for specified, explicit and legitimate purposes and cannot be processed in a manner that is incompatible with those purposes. Also, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed. Moreover, the data must be accurate and, where necessary, kept up to date. Accordingly, reasonable steps must be made to guarantee that inaccurate personal data (having regard to the purposes for which they are processed) are erased or rectified without delay. Furthermore, data must be kept in the form that allows the identification of data subjects for the period that is not longer than it is necessary for the purposes for which they are processed. Finally, data must be processed in the way that ensures adequate security of the personal data.

Police Directive is familiar with different categories of data subjects and Member States have to oblige the controllers to make a clear distinction between personal data belonging to different categories of data subjects (Article 6). These include:1) persons with regard

to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; 2) persons who have been convicted of a criminal offence; 3) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that they could be the victim of a criminal offence; and 4) other parties to a criminal offence, such as, for example the persons who might be called on to testify in investigations related to criminal offences or subsequent criminal proceedings, persons who can give information about criminal offences, or contacts or associates of one of the persons referred to in points 1 and 2.

According to its Article 7, Police Directive makes a clear distinction between personal data and the verification of quality of personal data, through obliging Member States to ensure that personal data based on facts are distinguished, as much as it is possible, from those that are based upon personal assessments. That is the reason why Member States must ensure that competent authorities take all necessary steps to make sure that inaccurate incomplete or no longer up to date personal data are not transmitted or made available. Therefore, each competent authority has to verify the quality of personal data before they are transmitted or made available and if it happens that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient has to be notified about that without delay.

Processing of personal data in the context of the Police Directive has to be lawful and performed only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and it has to be based on the EU or Member State law (Article 8 Paragraph 1).

Police Directive sets some special standards when it comes to the processing of particularly sensitive personal data. According to its Article 10, these special categories of personal data include: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The processing of such data is allowed only when this is strictly necessary, respecting appropriate safeguards for the rights and freedoms of the data subject, and only under the following circumstances: 1) if it is allowed by the national law of the Member State; 2) in order to protect the vital interests of the data subject or of another natural person; or 3) in the cases when such processing is related to data which have been manifestly made public by the data subject. Also, processing of special categories of personal data by the same or another controller for any of the purposes set out in Article 1(1) other than that

for which the personal data are collected is allowed only if in accordance with the EU or Member State law: 1) the controller is authorized to process such personal data for such a purpose; and 2) processing is necessary and proportionate to that other purpose.

Article 13 of the Police Directive obliges the Member States to provide that some information is made available to the data subject, including: 1) the identity and the contact details of the controller; 2) the contact details of the data protection officer, where applicable; 3) the purposes of the processing for which the personal data are intended; 4) the right to submit a complaint with a supervisory authority and the contact details of the supervisory authority and 5) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject. In specific cases, Member States are also expected to provide for the controller to give to the data subject the following further information with the purpose to facilitate the exercise of his or her rights: 1) the legal basis for the processing; 2) the period for which the personal data will be stored, or the criteria used to determine that period; 3) where applicable, the categories of recipients of the personal data, including in third countries or international organizations; 4) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject. The provision of these information may be restricted or omitted by legislative measures, but only to the extent and until such measures are necessary and proportionate in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned. Hence, the restrictions and omissions are allowed only with the purpose to: 1) avoid obstructing official or legal inquiries, investigations or procedures; 2) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; 3) protect public security; 4) protect national security; 5) protect the rights and freedoms of others.

In Article 14, Police Directive obliges Member States to allow the data subject to obtain the confirmation from controller about whether his or her personal data are being processed and, if that is the case, to access personal data and the following information: 1) the purposes of and legal basis for the processing; 2) the categories of personal data concerned; 3) the recipients or categories of recipients to whom the personal data have been disclosed, 4)where possible, the predicted period for which the personal data will be stored, or, if that is not possible, the criteria applied to estimate that period; 5) the existence of the right to request from the controller to correct or erase personal data or restriction of processing of personal data concerning the data subject; 6) the right to submit a complaint with the supervisory authority and the contact details of the

supervisory authority; 7) communication of the personal data undergoing processing and of any available information as to their origin.

According to Article 15, data subject's right of access can be entirely or partially limited by legislative measures, to the extent and as long as such restriction represents a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, with the purpose to: 1) avoid obstructing official or legal inquiries, investigations or procedures; 2) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; 3) protect public security; 4) protect national security and 5) protect the rights and freedoms of others.

Member States are obliged (in accordance with Article 16) to provide for the right of the data subject to obtain without undue delay from the controller the correction of his or her inaccurate personal data as well as to have incomplete personal data completed. The erasing of personal data has to be provided without undue delay if the processing infringes the provisions adopted in accordance with Articles 4, 8 or 10 of Police Directive or where personal data has to be erased in order to comply with a legal obligation to which the controller is subject. However, instead of erasing, the processing will be restricted if: 1) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or 2) the personal data must be maintained for the purposes of evidence.

The aforementioned Articles are only some of the provisions of the Police Directive that illustrate the approach to the protection of personal data and, through them, the protection of the right to privacy and human dignity in the EU in particularly delicate situations, where the interests of individuals to have their privacy guaranteed is confronted with the interests of the society, i.e. the state to facilitate crime prevention and security protection. It can be noticed that Police Directive frequently uses the terms such as “where possible”, “where necessary”, “where applicable” etc., all of which leave enough space for a rather flexible interpretation of its provisions.

Article 29 of Police Directive obliges Member States to provide for the controller and the processor to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10. In the case of a personal data breach, the controller has to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory

authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (Article 30). Moreover, if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, Member States have to provide for the controller to communicate the personal data breach to the data subject without undue delay (Article 31).

Another guarantee for the protection of personal data is the introduction of a special entity – data protection officer. Namely, in accordance with Article 32 of Police Directive, Member States are obliged to provide for the controller to establish a data protection officer (on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34) allowing them to exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation. A single data protection officer may be designated for several competent authorities, taking account of their organizational structure and size. Data protection officer is in charge at least of the following tasks, enumerated in Article 34: 1) to inform and advise the controller and the employees who carry out processing of their obligations; 2) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller in relation to the protection of personal data; 3) to provide advice where requested as regards the data protection impact assessment and monitor its performance; 4) to cooperate with the supervisory authority; 5) to act as the contact point for the supervisory authority on issues relating to processing,

Another means to ensure the protection of fundamental rights and freedoms of natural persons in relation to processing personal data within the Union is the obligation of the Member States to provide for one or more independent public authorities to be responsible for the monitoring of the application of the Directive (Article 41 Paragraph 1). These entities ate supposed to contribute to the consistent application of the Directive and, in order to achieve that goal, they are supposed to cooperate with each other as well as with the European Commission (Article 41 Paragraph 2). It is important to mention that Police Directive insists that the Member States provide for each supervisory authority to act absolutely independently when performing their tasks and exercising their authorities (Article 42 Paragraph 1). Accordingly, members of supervisory authorities have to remain free from direct or indirect external impact and are not allowed to ask for or accept anybody's instructions (Article 42 Paragraph 2).

3.4. The Relevance of the Police Directive for Serbia

Since the provisions of Police Directive formally oblige only the EU Member States, this document is not applied in Serbia. However, it is important that relevant subjects in Serbia become familiar with its key principles and standards for two reasons. The first one is the intention to fully harmonize Serbian national legislation with the *acquis* within the process of European Integrations, whereas the second one is the requirement that national law enforcement bodies guarantee the same level of personal data protection as the EU bodies, so that they can exchange relevant information for the purposes of transboundary crime suppression (Pejić, 2019: 4).

In Serbia, the protection of individuals' personal data is regulated by the Law on Personal Data Protection[8] (hereinafter: LPDP), adopted in 2018. The intention of LPDP is to provide for the harmonization of Serbian legislation in this field with relevant *acquis,* i.e. with the provisions of GDPR and Police Directive (Sironič, Novak, 2019: 2). However, the articles that regulate the processing of personal data by competent authorities for special purposes (prevention, detection or prosecution of criminal sanctions or the enforcement of criminal sanctions including the prevention of and protection from threats to public and national security) appear to be distributed all over the LPDP, which makes their proper interpretation rather difficult (Sironič, Novak, 2019: 3). Namely, the LPDP only emphasizes either in the final or in some of the paragraphs of a particular article that the entire Article or some of its paragraphs shall not be applied in the cases of data being processed by competent authorities for the special purposes (Sironič, Novak, 2019: 3). However, experts suggest that it would be much more appropriate to create a separate chapter within LPDP that would be dedicated exclusively to the processing of personal data in special cases regulated by the Police Directive. (Sironič, Novak, 2019: 3).

The majority of LPDP's provisions only repeat the provisions of the LED, which makes them remain declarative, without providing for any additional value, clarity or information necessary for the genuine and applicable transposition of Police Directive (Sironič, Novak, 2019: 4). Such approach allows different interpretations of legal provisions and a wide discretion when it comes to their application (Sironič, Novak, 2019: 4). Finally, the sanctions for the violations of certain obligations of competent authorities seem to be missing, which implies that this field should be regulated in a more systematic and detailed manner (Sironič, Novak, 2019: 4).

[8] Law on Personal Data Protection, Official Gazette of the Republic of Serbia, No. 87/2018.

4. Conclusions and Recommendations

Privacy and human dignity, as fundamental internationally and nationally recognized human rights, are closely interrelated and both are seriously endangered due to the development of modern technologies, particularly in the cases when they are in collision with the public interest to protect security and crime prevention. Due to rapid and expansive technological development, the protection of the right to privacy is constantly facing new challenges despite the fact that this field is regulated in national and international legal frameworks (Lukacs. 2016: 261).

As Edward Snowden argues, the lack of a universally accepted definition of privacy makes the citizens of pluralistic technologically advanced democratic societies feel that they should explain why they want their privacy to remain intact, which is wrong because the state is the one should justify the intrusion of privacy (Snowden, 2020: 220). Also, in the context of the development of modern technologies facilitating the intrusion of privacy in various different ways, it seems more reasonable to set the grounds for the protection of privacy directly on the protection of human dignity, instead of opting for an indirect protection through other human rights such as, for example, the right to property or the right to freedom of expression (Floridi, 2016: 308). However, regardless of the manner in which the protection of privacy is provided, maintaining a balance between the interest to protect personal data (and, through it, the right to privacy and human dignity) and achieve the objectives of security policy is a rather delicate task (De Hert, Papakonstantinou: 2016, 9). So, the balance between these two interests (security and freedom on one side and privacy on the other) should be considered of the main goals of a democratic state (Pavlović, 2017: 220).

A detailed and comprehensive legislative framework prescribing not only the basic standards of personal data protection, but also the mechanisms for the monitoring of their application and effective sanctions for their violations, certainly represents a key precondition for the efficient protection of the right to privacy and human dignity. Nevertheless, the actual protection, does not depend solely on the legislative framework, but also on the implementation and interpretation of the legal provisions and the ways in which they are applied by courts and Data Protection Authorities (DPAs) (Custers et al., 2018: 235). This in particular refers to the protection of personal data in the proceedings before the police and judicial bodies, regulated by the Police Directive, analyzed in this paper, since Police Directive contains numerous provisions that leave a lot of space for different interpretations, depending on the actual circumstances. Therefore, the role of

appropriate monitoring by the independent supervisory bodies is crucial for the appropriate implementation of Police Directive.

When it comes to Serbia, it is important to highlight the significance of the implementation of Police Directive into national legislation, in spite of the fact that our country is not an EU Member State. Although LPDP does contain provisions the aim of which is to facilitate the harmonization of Serbian national legislation with Police Directive, they should be organized in a more systematic manner, i.e. in a separate chapter and amended so that they provide for more precision and leave less space for extensive interpretation. Finally, adequate sanctions for the violations of the standards and rules contained in the Police Directive and implemented in national legislation should be provided. One should also concern the fact that the Police Directive leaves a lot of space for different interpretations of its provisions and, in Serbian legal system, the principle of the freedom of judicial discretion is treated as unlimited freedom that allows a judge to hand down completely different decisions in cases of identical or almost identical factual description (Kolaković-Bojović, Tilovska Kechegi, 2018: 124-125). Such approach threatens the equality of citizens before the law and might even degrade the legal predictability (Kolaković-Bojović, Tilovska Kechegi, 2018: 125). This has to be taken into consideration when implementing the Police Directive in Serbian national legislation

References

Bloustein, E. J. (1964) Privacy as an Aspect of Human Dignity: an Answer to Dean Prosser. New York University Law Review, 39, pp. 962-1007.

Bratman, B.E. (2002) Brandeis' and Warren's the Right to Privacy and the Birth of the Right to Privacy. Tennessee Law Review, 69, pp. 623-651.

Buttarelli, G. (2017) Privacy matters: updating human rights for the digital society. Health and Technology, 7(4), pp. 325-328.

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, OJ L 350, 30.12.2008, p. 60–71, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008F0977&from=EN, accessed on 27.08.2020.

Custers, B., Dechesne, F., Sears, A.M., Tani, T., Van der Hof, S. (2018) A comparison of data protection legislation and policies across the EU. Computer Law & Security Review, 34(2), pp. 234-243.

De Hert, P., Papakonstantinou, V. (2016) The New Police and Criminal Justice Data Protection Directive. A First Analysis. New Journal of European Criminal Law, 7(1), pp. 7-19.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50, https://eur-

lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN, accessed on 25.08.2020.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from =EN, accessed on 28.08.2020.

Dürig, G (1998) Einführung zum Grundgesetz, in: Grundgesetz: mit Vertrag über die abschließende Regelung in bezug auf Deutschland, Menschenrechtconvention, Bundesverfassungsg erichtsgesetz, München.

European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01, https://www.refworld.org/docid/476258d32.html, accessed on 26.08.2020.

Floridi, L. (2016) On Human Dignity as a Foundation for the Right to Privacy. Philosophy and Technology, 29(4), pp. 307-312.

Holtzman, D. (2006) Privacy Lost: How Technology is Endangering Your Privacy, San Francisco: Jossey-Bass.

Karovska-Andonovska, B., Kirkova, R. (2016) European Reform Package on Data Protection – Legal Framework and Expectations. Contemporary Macedonian Defence, 16(31), pp. 79-91.

Karovska-Andonovska, B. (2013) Implementation of the European norms and standards for protection of personal data in the Republic of Macedonia. Visions, (20), pp. 187-196.

Law on Personal Data Protection, Official Gazette of the Republic of Serbia, No. 87/2018.

Kolaković-Bojović, M., Tilovska Kechegi, E. (2018) The Uniform Application of Law- EU Standards and Challenges in Serbia. In: Pavlović, Z. (Ed.). Yearbook Human Rights Protection "From Unlawfulness to Legality". Novi Sad: Republic of Serbia Autonomous Province of Vojvodina Provincial Protector of Citizens – Ombudsman and Institute of Criminological and Sociological Research, pp. 115-135.

Lukács, Adrienn (2016) What is Privacy? The History and Definition of Privacy. In: Keresztes, Gábor (éd.): Tavaszi Szél Tanulmánykötet I. Budapest : Doktoranduszok Országos Szövetsége, pp. 256‑265.

Mitrović, D. (2016) Diptih o ljudskom dostojanstvu i toleranciji. Nauka, bezbednost, policija, 21(1), pp. 24-39.

Mitrović, D. (2010) Teorija države i prava. Beograd: Dosije.

Palmirani M., Martoni M., Rossi A., Bartolini C., Robaldo L. (2018) PrOnto: Privacy Ontology for Legal Reasoning. In: Kő A., Francesconi E. (Eds.) Electronic Government and the Information Systems Perspective. EGOVIS 2018. Lecture Notes in Computer Science, vol 11032. pp. 139–152., Cham: Springer.

Pandit, H. J., Fatema, K., O'Sullivan, D., Lewis, D. (2018) GDPRtEXT-GDPR as a linked data resource. European Semantic Web Conference (pp. 481-495). Cham: Springer.

Pavlović, Z. (2017) The Right to Privacy – Challenges of New Commitments. In: Pavlović, Z. (Ed.) Conference Papers - International Scientific Conference „Freedom, Security: the Right to Privacy". Novi Sad: Provincial Protector of Citizens – Ombudsman, Institute of Criminological and Sociological Research, pp. 218-234.

Pejić, J. (2019) Šta je policijska direktiva Evropske unije? Kako organi sprovođenja zakona (treba da) štite lične podatke. Beograd: Beogradski centar za bezbednosnu politiku.

Protecting personal data when being used by police and criminal justice authorities (from 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_3&from=EN, accessed on 28.08.2020.

Puaschunder, J. (2019) Dignity and Utility of Privacy and Information Sharing in the Digital Big Data Age. International Journal of Commerce and Management Research, 5(4), pp. 62-70.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, accessed on 25.08.2020.

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39–98, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725&from=EN, accessed on 31.08.2020.

Sironič, M., Novak, A. (2019) Assessment of the Draft Law on Personal Data Protection of Serbia – Desk Study, https://www.poverenik.rs/images/stories/dokumentacija-nova/Publikacije/engEKStudija.pdf, accessed on 02.09.2020.

Snouden. E. (2020) Trajno zabeleženo, drugo izdanje. Beograd: Vulkan izdavaštvo d.o.o.

Solove, D.J. (2008) Understanding Privacy. Cambridge, MA: Harvard University Press.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, OJ C 306, 17.12.2007, p. 1–271, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12007L/TXT&from=EN, accessed on 27.08.2020.

Westin, A. (2003) Social and Political Dimension of Privacy. Journal of Social Issues, 59(2), pp. 431-453.