AN ASSESSMENT of THE IMPLEMENTATION of the DATA PROTECTION REGULATIONS in CRIMINAL PROCEEDINGS*

Kişisel Verilerin Korunmasına İlişkin Düzenlemelerin Ceza Muhakemesi Süreçlerinde Uygulanmasına İlişkin Bir Değerlendirme

Seçkin KOÇER**

L&JR
Year: 14, Issue: 26
July 2023
pp.1-14

Article Information
Submitted :22.11.2022
Accepted :22.03.2023

Article Type
Research Article

ABSTRACT

The new ways of committing crimes, which have changed with technology, have also changed the modalities of preventing and investigating crimes. All these changes are based on the exponential increase of sharing personal data. For this reason; it is important to keep up-to-date the provisions of legislation that deal with the procedures of prevention and investigation of crimes. It is seen that these updates are generally done in a way that serves both prevention and investigation crimes and protecting personal data. Reforms introduced in the European Union legislation regarding the protection of personal data in recent years also consider a similar balance. In this context, many regulations of Directive 2016/680, which deals with the protection of personal data in the prevention and investigation of crime, aim to protect personal data as well as to carry out seamless procedures in this regard. Even in many regulations, this concern is at a level that goes beyond the purpose of protecting personal data. In Türkiye, on the other hand, uncertainties regarding data protection in this field still exist. It is clear that the Law on the Protection of Personal Data, which came into force in 2016, did not meet the expectations in this regard. It is seen that there are not even basic rules regarding the protection of personal data processed by law enforcement officers, public prosecutors and courts in the procedures of prevention and investigation of crimes. In our study, uncertainties and contradictions in this area have been underlined, and some amendments to the Law on the Protection of Personal Data have been proposed.

Key Words: Protection of personal data, data protection in judiciary and law enforcement.

ÖZET

Teknoloji ile birlikte değişen yeni suç işleme yöntemleri, suçun önlenmesi ve aydınlatılmasına ilişkin yöntemleri de

* There is no requirement of Ethics Committee Approval for this study.

** Dr, Head of Department at the General Directorate for Strategy Development at the Ministry of Justice, e-mail: seckinkocer@gmail.com, ORCID ID: 0000-0001-8350-0817.

değiştirmiştir. Esasında tüm bu değişimlerin temelinde, kişisel verilerin paylaşımının öngörülemeyen bir boyuta ulaşması yatmaktadır. Bu nedenle; suçun önlenmesi ve aydınlatılmasına ilişkin süreçleri ele alan mevzuat hükümlerinin güncel tutulması önem arz etmektedir. Söz konusu güncellemelerin genel itibariyle; hem suçun önlenmesi ve aydınlatılması hem de kişisel verilerin korunması amacına hizmet edecek şekilde yapıldığı görülmektedir. Avrupa Birliği mevzuatında kişisel verilerin korunmasına yönelik son yıllarda gerçekleştirilen reformlar da benzer dengeyi öngörmektedir. Bu bağlamda suçun önlenmesi ve aydınlatılması süreçlerinde kişisel verilerin korunmasını ele alan 2016/680 sayılı Direktif'in pek çok düzenlemesi de kişisel verileri korumayı amaçladığı kadar söz konusu süreçlerin sorunsuz bir şekilde yürütülmesi kaygısını gütmektedir. Hatta bir çok düzenlemede bu kaygı, kişisel verilerin korunması amacının önüne geçecek düzeydedir. Türkiye'de ise söz konusu alana ilişkin belirsizlikler halen devam etmektedir. 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nun beklentilere cevap vermediği açıktır. Bu bağlamda; kolluk görevlilerinin, Cumhuriyet savcısının ve mahkemelerin suçun önlenmesi ve aydınlatılmasına yönelik süreçlerde işledikleri kişisel verilerin korunmasına ilişkin temel kuralların dahi bulunmadığı görülmektedir. Çalışmamızda, bu alana ilişkin belirsizlikler ve çelişkiler ortaya konulmaya çalışılmış, Kişisel Verilerin Korunması Kanunu'na yönelik bazı değişiklikler dikkate sunulmuştur.

Anahtar Kelimeler: Kişisel verilerin korunması, yargı ve kolluk süreçlerinde verilerin korunması.

INTRODUCTION

In today's world, the concern for the protection of fundamental rights has been gaining significance with the increase in the use of technology in every walks of life. Recent amendments made in Europe to safeguard data protection for natural persons are seen as the results of the internet age[1]. The two important documents, the General Data Protection Regulation (hereafter, GDPR) and the Law Enforcement Directive (hereafter LED), have been adopted to ensure harmonisation among member states in the matter of data processing. While the former sets out data protection principles with regard to general data processing, the latter enshrines data protection principles in law enforcement proceedings.

The choice of two separate documents is under criticism in some ways, such as the difficulty experienced in the distinction of the scope of the documents and the intertwined structure of data processing[2]. However, it is evident that the documents are essentially created because of the unique features of each field. For instance, the regulations of the LED are shaped by considering the necessity of prevention, investigation or prosecution of offences. In fact, law

1 Paul De Hert, Vagelis Papakonstantinou, 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis' [2012] 22:6 Society for Computers & Law 7.

2 Ibid 7.

enforcement authorities in each member state may need more flexible rules while fulfilling their duties[3]. Moreover, flexibility among member states when combatting crimes is also another reason for a separate regulation[4]. For these reasons, data protection rules and principles in law enforcement have been regulated in a directive, rather than in the form of a regulation.

The GDPR can not apply to the activities of courts when courts act in their judicial capacities. However, member states could set out specific rules on the protection of personal data in judicial proceedings which must be in compliance with the general terms of the GDPR. As it is underlined in article 55/3 of the GDPR, supervisory authorities are not entrusted with the task of supervising courts in their judicial activities. That rule is laid down to ensure the protection of the independence of the courts. That is, when courts act in their judicial capacities, they are not under the supervision of a personal data protection authority. However, member states could entrust specific bodies in the judiciary to enhance awareness on the processing of personal data.

Even though the LED sets out that the provisions shall be implemented 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, to what extent member states will apply is still in question. Particularly, the implementation of data protection rules during criminal procedures differs among member states. This ambiguity becomes manifestly evident when data processing activities are carried out by courts.

The LED does not completely exclude the processing of personal data by courts and other judicial bodies from its scope. At this point, it is stated in recital 80 of the LED that there should not be any superior authority over the courts to monitor the processing of personal data by courts and other judicial bodies during functioning judicial tasks, otherwise the independence of the judiciary may be damaged. It is also valid for the proceedings conducted by public prosecutors[5]. However, the LED does not preclude member states from introducing protective measures regarding the protection of personal data during judicial proceedings[6]. That is, it may be pointed out that the LED recommends member states to specify the data protection rules in court proceedings. In some member states, new regulations which are deemed coherent with the LED have been introduced.

---

3 Liane Colonna, 'The New EU Proposal to Regulate Data Protection in the Law Enforcement Sector: Raises the Bar But Not High' [2012] 2 IRI Promemoria 2.

4 Murat Volkan Dülger, Onur Özkan, 'Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: Unutulan Direktifin Kapsamlı ve Karşılaştırmalı Analizi' [2020] 91 Ceza Hukuku Dergisi 91.

5 See recital 80 of the LED.

6 See recital 20 of the LED.

On the other hand, Türkiye does not have robust enough data protection provisions for court or other judicial proceedings even though the Turkish Personal Data Protection Law (hereafter, PDPL) sets the bar as high as the EU data protection regulations in many specific issues. The PDPL explicitly enumerates exemptions including data processing by judicial authorities or execution authorities as to investigation, prosecution, judicial or execution proceedings[7]. That is, if data is processed by a judicial authority during an investigation or prosecution, data subjects shall not be entitled to exercise their rights. Moreover, any other provisions of the PDPL shall not apply in any data processing by judicial authorities when they act in their judicial function.

Conversely, provided that data processing is deemed necessary for the investigation of an offence, the provisions of the PDPL would partially apply. In that case, article 10 of the PDPL on the data controller's obligation to inform, article 11 on the rights of the data subjects as well as article 16 on the obligation to register with data controllers' registry shall not be applied. Apart from the abovementioned articles, all other articles of the PDPL shall be applied in a proceeding of crime investigation.

These principles will be under scrutiny in this article and concrete suggestions will be made to make clarification in this regard.

A. The General Approach of the LED on the Data Processing in Criminal Proceedings

The LED lays out a variety of data protection principles ranging from the rights of data subjects to the responsibilities of data controllers which are mainly corresponding to the relevant provisions of the GDPR. In this chapter of the article, all these matters will not be looked into in detail as the main focus of the article is the applicability of data protection rules in criminal proceedings which are conducted by public prosecutors and judges.

The main standout of the LED is the endeavour to strike a balance the between protection of the personal data of natural persons and the smooth flow of the criminal proceedings[8]. As a reflection of this concern, the LED draws a general picture rather than providing bounding details in many articles. That is, in many articles, the final say is left to the discretion of member states. For instance, the LED, instead of setting out a specific timeframe for personal data to be erased in a particular case, leaves that decision to member states[9].

---

7 See the English translation of the Turkish Personal Data Protection Law, https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law accessed on 10 November 2022.

8 Onur Helvacı, 'Data Protection in the European Union Framework in General and in Criminal Investigations, The Balance Between National Security and Right to Privacy' [2021] 21 Law & Justice Review 187.

9 Article 5 of the LED underlines that *"Member States shall provide for appropriate time*

One of the most distinct novelties of the LED is to the necessity of classification of data considering the position of data subjects in criminal proceedings. Pursuant to that, member states shall provide data controllers with an explicit distinction between suspects, convicts, victims as well as other persons involving any criminal procedure[10]. This regulation underlines that any data processing in criminal procedure should be designed according to the position of data subjects[11]. In other words, implementing the same rules for different persons could not be considered in line with the provisions of the LED. There could have been a particular regulation to distinguish between serious offences and minor offences[12]. Even though this regulation is set forth to raise the bar in data protection, the lack of certain rules of how member states could lead to uncertainty in this regard.

Providing data subjects with rights in criminal proceedings is handled in two different manners. The LED firstly emphasises that member states shall make some certain information available to data subjects without any restriction. These are the identity and the contact details of the controller, the contact details of the data protection officer (where applicable), the purposes of the processing for which the personal data are intended, the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority and the existence of the right to request from the controller access to and the rectification or the erasure of personal data and the restriction of processing of the personal data concerning the data subject. Namely, the abovementioned information must be made available to any person whose data involved in a criminal procedure, regardless of whether this procedure is an investigation or prosecution.

---

limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed."

10 Article 6 of the LED reads *"Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:*
(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b)."

11 This distinction may also be used to determine timeframes for data storage and regular reviews. (Article 29 Data Protection Working Party opinion on some key issues of the Law Enforcement Directive (17 EN WP 258), accessed on 10 September 2022.)

12 Ibid (n 4) 6.

However, member states are not obliged to provide data subjects with some information to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, to protect public security, to protect national security and to protect the rights and freedoms of others. The information which may not be shared is also enumerated in the LED. These are the legal basis for the processing, the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period, where applicable, the categories of recipients of the personal data, including in third countries or international organisations, where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject[13]. The reason for these regulations is shown as not to undermine law enforcement proceedings[14]. Nonetheless, member states should implement these restrictions on a case by case basis instead of a blanket exemption[15].

The same grounds for not sharing information could be used in terms of exercising the right to access and the right to rectification or erasure of data as well. But the LED articulates that when member states put restrictions on the use of these rights, data subjects could apply national data protection authority to exercise these rights on his/her behalf[16]. This is an important novelty for both member states and data subjects[17].

The answer to the question of "is the data subject entitled to use these rights during a criminal investigation or a court proceeding?" is left to the discretion of member states. The LED leaves the void in question to be filled by each member state[18]. Member states may enact laws to lay out the details of how a data subject enjoys his/her rights during a criminal proceeding. However, as it will be seen below, this approach has already created unharmonised data protection environment among member states.

The LED also specifies which activities must be recorded by a data controller or a processor during a law enforcement proceeding, including the purpose of the processing to the envisaged time limits for erasure of data[19].

13 See article 13 of the LED.

14 Paul de Hert, Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive A First Analysis' [2006] 7:1 New Journal of European Criminal Law Review 12.

15 Ibid (n 12).

16 See article 17 of the LED.

17 Juraj Sajfert, Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' [2019] Edward Elgar Publishing 13 <https://ssrn.com/abstract=3285873> accessed on 10 November 2022.

18 See article 18 of the LED:

19 See article 24 of the LED.

This records should be made available to the national data protection authority upon request.

Having considered all these details introduced by the LED, it could be stated that the LED enshrines a good many data protection provisions pertinent to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. These provisions are also applicable during an investigation or prosecution procedure that is conducted by either a public prosecutor or a judge. According to an opinion, the Directive does not overtly or covertly applies if it's scope also covers data processing in court proceedings[20]. On the other hand, Backer and Hornung suggest that even though competent authorities in the context of the LED may be found ambiguous, courts and public prosecution offices fall within the scope of the LED[21]. Considering the scope of the LED, which explicitly underlines both investigation and prosecution phases, there is no doubt that the LED applies to data processing in these phases[22]. However, as it is seen in many articles, member states are given a large margin of appreciation to determine the data protection principles in these proceedings. For instance, even though a data controller must designate a data protection officer, courts and other judicial authorities are exempted from this obligation[23]. Another exemption is about the supervision of the national data protection authority over courts and other judicial authorities when they carry out a judicial function. In this case, supervisory authorities are not competent to monitor their data processing activities[24]. According to some researchers, this exemption is the result of the endeavour to lower possible tension between judicial authorities and national supervisory authority and to protect the independence of the judiciary[25]. Such kind of blurred provisions paves the way for new uncertainties.

B. Data Protection Procedures in Criminal Proceedings in Some Countries

1. France

In France Data Protection Act, specified amendments have been made to bring the Act in compliance with the LED. Chapter three of the Act is mainly

20 Ibid (n 9) 192.

21 Matthias Backer, Gerrit Hornung, 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on The National Police Laws and Laws of Criminal Procedure' [2012] 28 Computer Law&Security Review 630.

22 Seçkin Koçer, *Ceza Muhakemesinde Kişisel Verilerin Korunması* (Adalet Yayınevi, September 2022) 62.

23 See article 32 of the LED.

24 See article 45 of the LED.

25 Ibid (n 9) 191.

allocated to the processing of personal data by the law enforcement authorities[26]. After the general provisions, the Act lays down the responsibilities of authorities who are liable to data processing activities, namely the responsibilities of data controllers and processors. For instance, the authorities should take all reasonable measures to ensure that inaccurate or incomplete data are erased or rectified without delay and not transmitted. Furthermore, having made a risk assessment process, data controllers and processors should take distinct measures to prevent any unauthorised data processing activities[27]. On the other hand, the courts in France are not obliged to appoint a data protection officer, if they carry out judicial activities.

The rights of data subjects are under restrictions provided that the investigations, prosecutions, administrative proceedings as well as public safety and national security are at stake. In these cases, data subjects could not be entitled to exercise their rights, such as the right to information and right to access. However, the French regulation ensures that data subjects have two significant paths to follow. Firstly, in the case of restrictions, data subjects could apply to the national data protection authority to exercise their rights. The national data protection authority shall assign one of its members who are also among the representatives of high jurisdictions, namely the Council of State, the Court of Cassation or the Court of Auditors. Additionally, data subjects could file a judicial appeal in the wake of being informed by the relevant authority regarding the restriction.

2. United Kingdom

Data protection principles in law enforcement procedures are laid down in the Data Protection Act which also includes data protection rules in general. Pertinent to article 31 of the Act, it is set out that the provisions in that chapter would apply to the data processed for the purposes of prevention,

---

[26] According to section 87 of the Act, the Chapter on data protection on law enforcement issues applies to the "processing of personal data implemented for the purposes of prevention and detection of criminal offences, investigations and prosecutions in this area or execution of criminal sanctions, including the protection against threats to public security and the prevention of such threats, by any competent public authority or any other body or entity entrusted, for the same purposes, with the exercise of authority and the prerogatives of public power.
The processing is only lawful if and insofar as it is necessary for the performance of a task carried out, for one of the purposes set out in the paragraph above, by a competent authority within the meaning of the same first paragraph and where the provisions of Articles 89 and 90. Processing ensures in particular the proportionality of the retention period of personal data, taking into account the purpose of the file and the nature or seriousness of the offences concerned."

[27] For more detailed information; https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article87

investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Act also enumerates data protection principles, including requirement of lawful and fair processing with a specified, explicit and legitimate purpose. Moreover, data processing in law enforcement procedures shall be adequate, relevant and not excessive, kept up to date as well as processed in a secure manner.

Data processing in law enforcement in the UK is based on the distinction to be made between suspects, convicts, victims, witnesses and other persons. Furthermore, the rights of data subjects are also included in the Act. According to this chapter, data subjects are conferred the right to be informed, the right of access, the right to rectifiation and the erasure of data. However, these rights can not be exercised in the course of an investigation or a criminal proceeding. These are quintessential provisions showing that the Act is in compliance with the LED in many sections[28].

The provisions with regard to the supervisory authority in the Act is corresponding to the regulations set out in the LED. To monitor and take some actions if needed, Judicial Data Processing Panel has been established in the UK. The Panel consists of two judges of senior courts and a judge of the Upper Tribunal or the Employment Appeal Tribunal.

The Panel is responsible for;

- Promoting awareness of data protection law amongst the courts and tribunals judiciary,
- Ensuring effective guidance, including judicial training, is in place to ensure compliance with obligations that arise under data protection law both where courts and tribunals act in a judicial capacity and where judges/panel members otherwise carry out data processing functions in the course of their appointment,
- Ensuring an effective system is in place to investigate complaints in relation to data processing both where courts and tribunals act in a judicial capacity and where judges/panel members otherwise carry out data processing functions in the course of their appointment,
- Communicating with the Information Commissioner, in so far as appropriate, concerning compliance with data protection law[29].

---

28 See part 3 of the Data Protection Act.

29 For more information, see 'The UK Judicial Data Protection Panel Judicial Data Protection Complaints Handling Policy', <https://www.judiciary.uk/wp-content/uploads/2019/04/Judicial-data-processing-complaints-handling-policy-June-2021.pdf,> accessed on 17 September 2022.

3. Ireland

In Ireland, the rules on processing of personal data are laid down in the Data Protection Act which enshrines chapters including "Processing of Personal Data for Law Enforcement Purposes". That is, the rules covering the processing of personal data could also be applied in law enforcement proceedings. However, there are some restrictions on the obligations of data controllers and the rights of data subjects due to the aim of safeguarding judicial independence. For instance; pursuant to article 158 of the Data Protection Act, it is laid down that provisions on the details of supervisory authority[30], the necessity of data protection officers as well as rights of data subjects are restricted provided that the restrictions are deemed as necessary and proportionate for judicial independence. In addition to that, the Act also lays out some specific provisions, such as the publication of court judgments, court decisions or court lists. The processing of personal data will be considered as lawful if that processing is about the publication of a court judgment or decision or list of court hearings.

According to the Data Protection Act, the chief justice of Ireland[31] has the authority to assign a judge who acts as a supervisor of the processing of personal data by courts in judicial proceedings. The assigned judge shall enhance awareness among judges regarding the provisions of GDPR, Directive 2016/680 as well as other regulations on the protection of the personal data. Besides, he/she shall investigate any complaint as to the processing of personal data during judicial proceedings.

CONCLUSION

It is obvious that with the exponential use of technology, the way of committing crimes has significantly changed. As a result of this development, the modalities of conducting an investigation or prosecution have been forced to be evolved. Having adopted these novel modalities, law enforcement authorities have started to process more data than before.

---

30 Even though the provisions on supervisory authority in Ireland is corresponding to the it's counterparts in member states, the data processing by police and armed force fall within the competence of the Irish authority. (David Wright, Paul De Herts, *Enforcing Privacy, Regulatory, Legal and Technological Approaches* (Springer, 2016) 443.)

31 The chief justice in Ireland is the president of the Supreme Court and is naturally considered as the head of the judicial branch. Chief justice in Ireland was conferred with two specific responsibilities. Firstly, he/she is the first member of the presidential commission in Ireland which means he/she acts on behalf of the president in his/her absence. Secondly, the chief justice in Ireland is a member of the Council of State which is a body of consultation for the president. (For more detailed information;
'The Supreme Court of Ireland, The Role of Chief Justice' , http://www.supremecourt.ie/supremecourt/sclibrary3.nsf/0/B86A2D50F97D4EB480257315005A41D2?openDocument&l=en) accessed on 25 September 2022.)

Data processing activities in law enforcement procedures have evolved to an inevitable matter to be handled by legislation in many countries. The LED, which is a complementary document of the GDPR, has been introduced to strike a balance between the protection of personal data and ensuring the efficiency of law enforcement.

In our article, some novelties launched by the LED have been touched upon, such as the categorisation of data subjects according to their positions in investigations and prosecutions. Besides, the new ways of exercising rights of data subjects are also quite significant to underline in this regard. That is, data subjects are given two paths to follow. One of which is to directly apply to the data controller to exercise the relevant right. The second one is the use of that right in an indirect way, through the national data protection authority. The latter is deemed as one of the important tools to further strengthen the use of rights by data subjects.

One could think that the provisions laid down by the LED are not applicable for the data processing activities of courts and other judicial authorities. The LED does not set out an explicit regulation to end all discussions on this matter. However, considering the scope of the LED, which explicitly underlines both investigation and prosecution phases, we think that data processing activities during these phases are covered by the LED in a general manner. On the other hand, the LED leaves a large margin of appreciation to member states in some issues. Furthermore, given the fact that judicial independence must be observed by all, the competence of national data protection authorities has been excluded from the judicial activities of courts and other judicial authorities. Again, the LED draws a general picture and leaves the rest to each state to clarify.

Although Türkiye has a dedicated data protection law since 2016, this legislation is not clear enough to cover data protection issues in criminal proceedings. Pursuant to the 1st paragraph of article 28 of the PDPL, the Law shall not be applied if personal data are processed by judicial authorities or execution authorities with regard to investigation, prosecution, judicial or execution proceedings. This provision clarifies that there is an absolute exemption if the courts or other judicial authorities act in their judicial capacities. That is, it is not likely to implement any provision laid down in the PDPL, including the principles of lawful data processing as well as the rights of data subjects.

One of the most confusing provisions of the PDPL is laid down in the 2nd paragraph of article 28 which regulates a partial exemption. According to that provision, article 10 of the PDPL on the data controller's obligation to inform, article 11 on the rights of the data subjects as well as article 16 on the obligation to register with the data controllers' registry shall not be applied provided that

data processing is necessary for the prevention of committing a crime or for a crime investigation[32].

Namely, if data processing is undergone during a crime investigation which is orchestrated by the public prosecution office, the provisions of the PDPL would apply, except the specific provisions mentioned above. However, it is not clear how this regulation would apply considering the details of the first paragraph of the same article since in the first paragraph, investigation phase is also indicated among the absolute exemptions. If the PDPL implies that data processed by police forces during an investigation fall within the PDPL, how data processed by the public prosecutor offices could be separated from the former is not clear as the work of public prosecutor office and police is inextricable. It would be a better way to prepare a guideline covering these issues by the Personal Data Protection Authority(PDPA). After having prepared the guideline, the PDPA should make it public and share it with data controllers and processors, specifically. If not, it does not seem possible to come to a clear conclusion in this regard.

In addition to the abovementioned points, there are other issues that should be taken into account when an amendment in the PDPL would be on the table. If the PDPL would be amended by considering these issues, it would pave the way for a safer data protection environment.

Provided that personal data processed by courts or other judicial authorities would fall out of the PDPL, it would mean that individuals would be deprived of their rights and the novelties introduced by the PDPL would be meaningless. Yet, as it is indicated in our study, many provisions of the PDPL would be seamlessly applicable in the field of public prosecution and court proceedings. For this reason, there should be some amendments to be made in the PDPL to make the implementation of data protection rules applicable in both prosecution and court proceedings. That is, article 28/1.d of the PDPL should be repealed and be replaced by a new provision that strengthen the rights of data subjects.

When an amendment would be discussed, a new supervisory authority[33] must be laid down to monitor data processing during prosecution and court proceedings. This new authority must be made up of judges with a certain seniority since the balance between law enforcement interests and data protection could be struck would be ensured only in this way[34]. Furthermore, the duties of this authority and the current PDPA should be drawn clearly.

---

32 See article 28 of the PDPL

33 Some researchers suggest that the PDPA, which is responsible for data processing activities in a general manner, should be the supervisory body for data processing in law enforcement in Türkiye as well. (Ibid (n 5) 115.)

34 Ibid (n 4) 5.

After having made such amendments in the PDPL, there should be some guidelines to be issued and delivered to data controllers and processors. The lack of guidelines in this field would cause further problems which would be difficult to solve.

In case there would not make any amendments in the PDPL, there is an undeniable need to clarify some points, such as the applicability of the partial exemption provision regarding an investigation of a crime. Some concrete steps must be taken to ensure that the PDPL would apply in the field of police work.

The rights of data subjects in judicial proceeding should be specified by law and made public on the websites of courts, respectively. In fact, the content of the court websites should be revised and shaped with a user-friendly approach to enhance access to justice for all.

The websites of courts and public prosecution offices should include information on data processing, including on which purpose and by whom data is processed, contact points for data subjects, etc[35].

BIBLIOGRAPHY

Article 29 Data Protection Working Party opinion on some key issues of the Law Enforcement Directive (17 EN WP 258), <https://ec.europa.eu/newsroom/article29/items/610178> accessed on 10 September 2022.

French Data Protection Authority <https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article87> accessed on 12 November 2022.

Backer M., Hornung G, 'Data Processing by Police and Criminal Justice Authorities in Europe – The Influence of the Commission's Draft on The National Police Laws and Laws of Criminal Procedure' [2012] 28 Computer Law&Security Review.

Colonna L., 'The New EU Proposal to Regulate Data Protection in the Law Enforcement Sector: Raises the Bar But Not High' [2012] 2 IRI Promemoria.

De Hert P., Papakonstantinou V., 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis' [2012] 22:6 Society for Computers & Law.

De Hert P., Papakonstantinou V., 'The New Police and Criminal Justice Data Protection Directive A First Analysis' [2006] 7:1 New Journal of European Criminal Law Review.

[35] See the website of the German Federal Constutional Court, https://www.bundesverfassungsgericht.de/EN/Verfahren/Datenschutz%20f%C3%BCr%20den%20justiziellen%20Bereich/Datenschutz%20f%C3%BCr%20den%20justiziellen%20Bereich_node.html.

Dülger M. V., Özkan O., 'Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: Unutulan Direktifin Kapsamlı ve Karşılaştırmalı Analizi' [2020] 91 Ceza Hukuku Dergisi.

Helvacı O. 'Data Protection in the European Union Framework in General and in Criminal Investigations, The Balance Between National Security and Right to Privacy' [2021] 21 Law & Justice Review.

Koçer S, *Ceza Muhakemesinde Kişisel Verilerin Korunması* (Adalet Yayınevi, September 2022).

Sajfert J, Quintel T, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' [2019] Edward Elgar Publishing 13 <https://ssrn.com/abstract=3285873> accessed on 10 November 2022.

The UK Judicial Data Protection Panel Judicial Data Protection Complaints Handling Policy, <https://www.judiciary.uk/wp-content/uploads/2019/04/Judicial-data-processing-complaints-handling-policy-June-2021.pdf,> accessed on 17 September 2022.

Turkish Personal Data Protection Law, <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law> accessed 10 November 2022.

Wright D., De Herts P., *Enforcing Privacy, Regulatory, Legal and Techological Approaches* (Springer, 2016).

'The Supreme Court of Ireland, The Role of Chief Justice' , http://www.supremecourt.ie/supremecourt/sclibrary3.nsf/0/B86A2D50F97D4EB480257315005A41D2?openDocument&l=en) accessed on 25 September 2022.