Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement
Working Paper Series

Transparency in the Face of New Technologies: Information Rights under the Law Enforcement Directive

Irmak Erdoğan*

Abstract

The widespread use of data gathering and analysis technologies enabled a sophisticated form of policing. The new policing tools allowed law enforcement to gather extensive information on citizens, meanwhile leading to a profound interference with fundamental rights, including the right to personal data protection. Particularly in the face of artificial intelligence tools, the rights of data subjects affected by such measures may fall short of protecting them against complicated surveillance techniques. To this end, the rights to access and information are crucial tools for reinforcing the fundamental rights of citizens towards the use of new technologies in the security context. These rights enable the data subjects to understand the procedures regarding the processing of their data and provide an opportunity to have control over these procedures. Furthermore, they ensure transparency and help citizens to supervise the legality of personal data processing, and raise awareness about big data practices. With this perspective, the Law Enforcement Directive ('LED') is an essential tool in the security field to counterbalance the state power that rests on massive information on individuals.

Hence, this paper will first introduce the rights to information and access within the LED. It will analyze what type of information is to be shared with data subjects in the law enforcement context and to what extent. Considering that automated decision-making tools empower law enforcement agencies with a more extended capacity to analyze massive amounts of data, this paper will also tackle the adequateness of informational rights during automated decision-making, including profiling in criminal justice. However, none of these rights are absolute. Therefore, while elaborating on informational rights, this paper will further examine their exceptions and limitations. It will try to draw limits to restrictions within the light of fundamental rights and relevant jurisprudence.

After introducing informational rights in the digital age, the second part of the paper will portray the challenges to the relevant rights. First, the focus will be on the fragmentation in crime prevention and detection. This fragmentation results from the multiple security agencies processing data in these fields and also from the numerous information systems that they operate with. Furthermore, the blurry line between the organizational and functional boundaries of intelligence agencies and law enforcement further complicates defining the relevant legal regime and applying the rights to access and information. Therefore, the paper will also elaborate on the disappearing walls between intelligence and law enforcement agencies. Finally, it will tackle the challenges emerging in the practice. The Member States transpose the Directive into national laws with differences; also, national authorities may have diverging practices. Therefore, the paper will conclude by shedding light on challenges emerging during the application of informational rights in the age of new technologies.

Keywords:

Right to access, right to information, automated decision-making, Law Enforcement Directive

* Postdoctoral researcher at KU Leuven, Center for IT and IP Law, Leuven, Belgium.

Transparency in the Face of New Technologies: Information Rights under the Law Enforcement Directive[*]

Abstract

The widespread use of data gathering and analysis technologies enabled a sophisticated form of policing. The new policing tools allowed law enforcement to gather extensive information on citizens, meanwhile leading to a profound interference with fundamental rights, including the right to personal data protection. Particularly in the face of artificial intelligence tools, the rights of data subjects affected by such measures may fall short of protecting them against complicated surveillance techniques. To this end, the rights to access and information are crucial tools for reinforcing the fundamental rights of citizens towards the use of new technologies in the security context. These rights enable the data subjects to understand the procedures regarding the processing of their data and provide an opportunity to have control over these procedures. Furthermore, they ensure transparency and help citizens to supervise the legality of personal data processing, and raise awareness about big data practices. With this perspective, the Law Enforcement Directive ('LED') is an essential tool in the security field to counterbalance the state power that rests on massive information on individuals.

Hence, this paper will first introduce the rights to information and access within the LED. It will analyze what type of information is to be shared with data subjects in the law enforcement context and to what extent. Considering that automated decision-making tools empower law enforcement agencies with a more extended capacity to analyze massive amounts of data, this paper will also tackle the adequateness of informational rights during automated decision-making, including profiling in criminal justice. However, none of these rights are absolute. Therefore, while elaborating on informational rights, this paper will further examine their exceptions and limitations. It will try to draw limits to restrictions within the light of fundamental rights and relevant jurisprudence.

After introducing informational rights in the digital age, the second part of the paper will portray the challenges to the relevant rights. First, the focus will be on the fragmentation in crime prevention and detection. This fragmentation results from the multiple security agencies processing data in these fields and also from the numerous information systems that they operate with. Furthermore, the blurry line between the organizational and functional boundaries of intelligence agencies and law enforcement further complicates defining the relevant legal regime and applying the rights to access and information. Therefore, the paper will also elaborate on the disappearing walls between intelligence and law enforcement agencies. Finally, it will tackle the challenges emerging in the practice. The Member States transpose the Directive into national laws with differences; also, national authorities may have diverging practices. Therefore, the paper will conclude by shedding light on challenges emerging during the application of informational rights in the age of new technologies.

Keywords: Right to access, right to information, automated decision-making, Law Enforcement Directive

[*] Irmak Erdoğan, postdoctoral researcher at KU Leuven, Center for IT and IP Law, Leuven, Belgium.

1. Introduction

The digitization of life, combined with the advancement in technology led to processing massive data, which is a goldmine for law enforcement activities. On the other hand, it allows massive and systematic surveillance practices and leads to providing a far-reaching picture of the citizens' lives[1].

The imbalanced information power supported by big data and new AI tools requires underlining the access and information rights of data subjects in the security context. In that sense, the General Data Protection (GDPR) and the Law Enforcement Directive (LED) are important responses of the EU to the challenges posed by new technologies and massive data collection. The LED is particularly relevant to the data processing by competent authorities[2] for law enforcement purposes, such as '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[3]'.

Under the security context, informational rights allow the transparency of data processing by security agencies, in so doing raising the trust of citizens in the use of their data in a state of law. Furthermore, they permit a safer and more efficient network for international cooperation, which is based on lawful and accurate data. In that sense, the LED has a central role in providing individual rights while enhancing the exigencies of law enforcement authorities. With this perspective in mind, this paper elaborates on how informational rights contribute to rights-enhanced-security. The following part will use an evaluative approach to examine current information and access rights under the LED, taking into account the related case law. It will further tackle the constraints foreseen by the LED regarding the rights to access and information and scrutinize to what extent they empower the citizens.

1. The rights to information and access under the law enforcement directive

A. Right to information

The right to be informed about personal data processing is one of the most crucial data protection rights as it initiates the application of the other data subjects' rights; such as the right to access the personal data; to rectify it, to have it erased and to make a resort to legal remedies[4]. Article 13 LED regulates the `information to be made available or given to the subject'. The provision differentiates between minimum information to be provided and other information to be shared 'in specific cases', which shall be defined by national law. Accordingly, controllers shall at least make available to the data subjects the identity and contact details of the data controller, data protection officer, and supervisory authority. The data subjects must also be informed of their right to complain to the supervisory authority. Furthermore, the data controllers shall guide data subjects on their right to request access, rectification, or erasure of

[1]Katherine Quezada-Tavárez, 'Impact of the Right of Access on the Balance Between Security and Fundamental Rights: Informational Power as a Tool to Watch the Watchers' (2021) 7 European Data Protection Law Review 59, 63.

[2] According to 3/7 (a) LED, the controller is the competent authority, meaning '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'.

[3] Article 1, LED.

[4] Catherine Jasserand, 'Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in Directive 2016/680?'(2018) 34 Computer Law & Security Review 154, 162.

personal data, and restriction of processing of the personal data concerning the data subject. Finally, the purposes of personal data processing must be shared.

The second category of information covers the additional obligation to inform data subjects in specific cases to enable the exercise of their rights (13/2). Accordingly, the legal basis for the processing, the storage period for the personal data, and where applicable, the categories of recipients of the personal data shall be shared with the data subjects. Finally, 13/2 further enlarges the scope of information to be shared, in particular where the personal data are collected without the knowledge of the data subject. In such a case, the controller might need to give further details and information which are not foreseen within the mentioned article. This second layer of information can be delayed, restricted, or even omitted if such a measure meets the standards of being necessary and proportionate in a democratic society. It is possible to impose some restrictions and omissions on this second group of data for specific purposes exhaustively listed in 13/3[5]. Recital 26 also underlines the possibility of imposing limits considering the nature of law enforcement activities, by noting that transparency about data processing under law enforcement context 'does not in itself prevent the law enforcement authorities from carrying out activities such as covert investigations or video surveillance'[6].

The wording of Article 13 also needs further analysis. Article 13 (1) mentions 'making available' information whereas Article 13(2) indicates 'giving' information 'in specific cases'. Recital 42 helps interpret the wording by giving examples of how to make available information, such as sharing it on the competent authority's website. In that sense, law enforcement authorities must provide information enlisted on 13/1 on their webpage via means like 'publishing their privacy policy on Body Worn Video or firearms registration'[7]. They should also indicate the purpose behind processing data via chosen technologies. Thus, Article 13(1) aims to provide general information 'made available to the public', which implies that this duty does not concern a certain data subject, but embodies a certain processing procedure and targets all data subjects who may be impacted by it[8]. On the other hand, 13(2) is about the 'information to be provided in addition to a particular data subject'. The national legislators can regulate further information to give in individual notices. One can argue that such information, if specific enough, can be offered on the website, along with the minimum information. In any case, all information given to the data subject must be 'in a concise, intelligible and easily accessible form, using clear and plain language'[9].

It can be also disputed if Article 13 of LED establishes a duty of notification. The article does not explicitly oblige informing data subjects about the collection of their data as soon as their data is processed for law enforcement purposes. As a comparison, the Council of Europe's Recommendation on the use of personal data in the police sector[10] formulates this obligation

[5] These purposes are enumerated as to (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; (e) protect the rights and freedoms of others.

[6] Christopher Kuner, Lee A. Bygrave, Christopher Docksey, Laura Drechsler, and Luca Tosoni, *The EU General Data Protection Regulation: A Commentary/Update of Selected Articles* (Oxford Publications 2021), 418.

[7] Article 29 Data Protection Working Party, *Opinion on Some Key Issues of the Law Enforcement Directive (EU 2016/680)*, 29 November 2017, p. 17.

[8] ibid.

[9] Kuner et al. (n 6), 419.

[10] Recommendation No. R (87) 15, regulating the use of personal data in the police sector, was adopted by the Committee of Ministers of the Council of Europe on 17 September 1987.

by stressing that the individual should be 'informed that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.'[11]. The increasing data exchange between private and public parties further complicates such a notification. Considering the right to information of the data subject constitutes an interference with the fundamental right to the protection of personal data, the obligation to inform the subjects needs to be interpreted in line with the relevant European Court of Justice (ECJ) and European Court of Human Rights (ECtHR) decisions.

In the Klass case, the ECtHR confirmed that 'the person concerned must be informed after the termination of the surveillance measures as soon as notification can be made without jeopardizing the purpose of the restriction'. Nevertheless, the Court also acknowledges that the subsequent notification to each individual affected by a suspended measure might well endanger the long-term purpose behind the surveillance[12]. Thus, the Court found the notification an important tool to guarantee effective remedies which redress the balance between the state's surveillance powers and the rights of the targeted individual. In this decision, however, the Court did not indicate the notification a vital precondition to comply with Article 8 ECHR. According to the Court's reasoning, it is due to the fact that the relevant German law had stipulated several other safeguards in case of secret surveillance and the lack of notification alone would not constitute a violation[13].

The ECtHR took one step further In Ekimdzhiez v. Bulgaria case[14] by stressing that the notification is a crucial safeguard against abuse in the framework of surveillance activities. In this case, the ECtHR tackled the Bulgarian 'Special Surveillance Means Act' (SSMA) which empowered the police and the Bulgarian secret service with extended surveillance duties. The Court remarked that Bulgarian law did not foresee any notification duties to the surveilled individuals. It even prohibited the disclosure of information that a person had been exposed to surveillance. The Court first acknowledged that the secrecy of the surveillance may ensure its efficiency. However, not obstructing surveillance does not mean a carte blanche, which allows the States never to notify relevant subjects. Therefore, in this case, the Court concluded that there was a violation of Article 8 ECHR, requiring that, 'as soon as notification can be made without jeopardizing the purpose of the measure', it is a duty to inform the persons concerned. The Court concluded further that if data subjects are never notified, they cannot seek redress for interferences with their rights during surveillance (unless they are prosecuted and the relevant information is shared during a process). Hence, the Court additionally found a violation of a right to an effective remedy stipulated under Article 13 ECHR, considering lack of information on the surveillance measure hindered the applicants from challenging the interference with their rights[15].

---

[11] Jasserand (n 4), 162.

[12] *Klass and Others v Germany*, Application no. 5029/71, (ECtHR, 6 September 1978), para. 58.

[13] Under the relevant G 10 law, an administrative procedure is designed to ensure that measures are not ordered haphazardly and only for serious crimes. The G 10 also lay down strict conditions regarding the implementation of the surveillance measures and the processing of the information such as imposing a time limit for a maximum of three months, review of the necessity of the measures, and destruction of the obtained documents as soon as they are no longer needed to achieve the required purpose, see Klass and Others v. Germany, paras 51, 52.

[14] *Ekimdzhiev and Others v. Bulgaria*, Application no. 70078/12, (ECtHR, 11 January 2022).

[15] Paul de Hert and Franziska Boehm, 'The Rights of Notification after Surveillance is over: Ready for Recognition?', (2012) 3 European Journal of Law and Technology, <https://www.researchgate.net/publication/292105126_The_Rights_of_Notification_after_Surveillance_is_over_Ready_for_Recognition> accessed 13.03.2023.

In some cases, the surveillance is employed by private entities where they shared data with law enforcement. In López Ribalda and Others case, a Spanish supermarket chain used covert video surveillance to trace the employees. The video records were used after suspicions of theft had arisen[16]. The applicants were not informed of the surveillance measures which led the ECtHR to conclude that the video surveillance measure did not comply with the obligation to previously, explicitly, and precisely inform those concerned about the existence and particular characteristics of the personal data collection[17]. Even though this decision does not assess the information rights under the LED, it is crucial to underline that the same obligation to inform the subjects applies also to private parties.

In conclusion, under the light of the relevant jurisprudence, the obligation to be notified of personal data processing under the security context is a crucial element to empower citizens. The notification duty may not have been explicitly addressed under LED, yet the EU Courts accept this duty as a core element for ensuring the right to privacy. Furthermore, the Court scrutinizes the limitations to notifications and carries out the balancing test not only by considering Article 8 ECHR, but also Article 13 ECHR. Therefore, the duty of notification must be considered an indispensable part of informational rights, as well as of the right to respect for private life, and the right to an effective remedy.

B. The right to access under the law enforcement directive

The right of access enables data subjects to exercise more control over their data, by allowing them to grasp the whole data processing procedures. The more complex data processing becomes, the more responsibility data controllers have to provide better and more understandable information for the data subjects[18]. Thus, data subjects need to be offered direct information which is tailored to their situation, thereby they can supervise the lawfulness of the process. Therefore, access rights enable data subjects to have a direct impact on the life cycle of personal data processing.

The right of access is even more relevant in the context of 'the potential life-altering decisions that may result from security-related processing'[19]. Particularly, excessive collection and processing of personal data by law enforcement can challenge the principle of proportionality; whereas the lack of oversight and inaccurate information can give rise to wrongful arrests and convictions[20].

The requirements foreseen in Articles 12 and 13(1) LED can be evaluated as ex-ante obligations, i.e. information obligations ahead of the data processing activities. These obligations are supplemented with the ex-post right of access envisioned in Article 13(2) LED and access rights in Article 14 LED. Following Article 14, data subjects are furnished with the right to obtain more information about the data processing activities than the general information made available to the public. In that way, the right of access enables data subjects

[16] *López Ribalda and Others v. Spain*, Applications nos. 1874/13 and 8567/13, (ECtHR, 9 January 2018).
[17] Ibid para 69.
[18] European Data Protection Supervisor, 'Opinion 7/2015: Meeting the Challenges of Big Data. A Call for Transparency, User Control, Data Protection by Design and Accountability', 2015, https://edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf, accessed 13.03.2023, p. 10
[19] Quezada-Tavárez (n 1), 71.
[20] Ibid.

to have more individualized information from the controller on the current data processing activities concerning him or her[21].

Article 14 LED grants data subjects to receive from the data controllers a confirmation as to whether or not personal data concerning them are being processed; access to several categories of information, including the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; data undergoing processing and of their origin. The origin of data is a crucial resource as it reveals who holds information about the data subject. On the other hand, as Recital 43 LED suggests in case the data stemmed from natural persons, their identity shall not be disclosed, especially if the sources are confidential. This limitation can be justifiable, considering that under the criminal law context, the vulnerable witnesses or victims may be exposed to danger[22].

In addition, the data subject may not receive a full list of recipients of data. Article 3(10) LED excludes from the definition of recipients public authorities that are entitled to receive data in the framework of a particular inquiry in the general interest in accordance with the law. As an example, if tax or customs authorities receive personal data regarding the data subjects, then the data subject may not access this information. While it is understandable to protect vulnerable subjects of criminal procedures, excluding information on a broad category of recipients seems difficult to justify[23].

Furthermore, Article 15 LED acknowledges the discretion of Member States to fully or partially restrict the right to access, provided that such measures are foreseen by law and are necessary and proportionate in a democratic society. These measures can be taken only if access to data interferes with the achievement of crime prevention, legal inquiries, investigations or criminal procedures, prosecution of criminal offenses, or the execution of criminal penalties and hinders the protection of public security, national security, and the rights and freedoms of others. The exceptions stipulated under Article 15 are very broad and leave the states an extensive discretionary power. However, keeping in mind that the right to access is a 'core essence' of the right of data protection[24] and explicitly foreseen in Article 8 (2) of the Charter of Fundamental Rights of the European Union, as well as in Article 9 (1)(b) of the Council of Europe Modernized Convention[25], the limits to this right shall be interpreted narrowly. In other words, Article 15 cannot be seen as a blanket approach of denying access automatically under the stipulated grounds for refusal. Therefore Article 15(3) LED further specifies that in case the right of access is restricted or refused, member state laws must enforce controllers to document the factual or legal reasons behind the refusal or restriction decisions. They shall also share these decisions and their justification by data subjects in writing and without undue delay.

However, if the right of access is restricted not to hamper law enforcement activities in the first place, giving a detailed response on the factual reasons for limitations might not be possible for

[21] Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin and Pierre Dewitte, 'From Theory To Practice: Exercising the Right of Access Under The Law Enforcement and PNR Directives', (2020) 11 JIPITEC 274, 2020, 288.
[22] Diana Dimitrova and Paul De Hert, 'The Right of Access Under the Police Directive: Small Steps Forward', in M. Medina, A. Mitrakas, K, Rannenberg, E. Schweighofer and N. Tsouroulas (eds) *Privacy Technologies and Policy* (Springer 2018), 119.
[23] Ibid, 120.
[24] Eva Brinkmann, *Essence and Effectiveness of the Right of Access*, Master Thesis, KU Leuven Faculty of Law, 2019-2020 Academic Year, 29.
[25] Ibid, 15, 16.

the same reason. Therefore, Article 13 (3) stipulates that 'such information may be omitted', yet the data subjects should be made aware of their right to lodge a complaint with a supervisory authority. Thus, the data controller can communicate that access has been fully or partially denied or that he can neither confirm nor deny that the data is being processed. It implies that in such a case data subject does not receive meaningful information. In order to balance this situation, Article 17 LED introduces indirect access. Indirect access requires that upon the request of the data subject, the supervisory authority shall control the legality of the limits and omission of the right to access on behalf of the data subject. After making necessary checks such as the legality of the processing, the data minimalization, and the accuracy of data, the supervisory authority shall inform the data subject at least about the realization of the necessary verifications in line with 17(3) LED. However, it is disputable if the data protection authority can gain access to all concerning data and have a clear overview of the situation which allows adequate supervision of the concerning case[26]. Nevertheless, if not satisfied with this procedure, the data subject can apply for a judicial remedy.

C. The missing informational rights regarding the automated decision-making

Automated decision-making is increasingly used in the criminal law context. While new technologies allow the massive collection of data, algorithms help analyze the models and affinities between the datasets. Law enforcement uses such an analysis to predict 'potential criminals' or 'potential crime scenes'. Or else, companies designing software for data collection and analysis, work with governments to spot violent crime and to compose "target lists" for further surveillance and investigation purposes[27]. Thus, traditional evidence based on observation, witness statements, and circumstantial evidence might in the future be replaced by alerts created by software[28].

Nevertheless, profiling carries certain risks like bias and non-accuracy, which can give raise to unlawful arrests and convictions. That's why both the GDPR and Directive 2016/180 have granted data subjects some safeguards against automated decision-making, including profiling. On the other hand, even though the rights at stake in criminal law are very crucial, such as the right to security and a fair trial, unlike the GDPR, the LED does not explicitly stipulate the rights to access information in case of automated decision-making. While the GDPR foresee by 13/ 2 (f), 14/2 (g), and 15/1 (h) 'the existence of automated decision-making, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject', the LED does not openly guarantee these rights[29]. Not providing express rights on the existence of automated decision-making, algorithmic logic, or the potential consequences for the data subject is a big shortfall[30]. However, these 'missing rights' are particularly relevant in respect of the fairness of the processing stipulated in Article 4(1)(a).

---

[26] Ibid, 25.
[27] Andrew Guthrie Ferguson, 'Policing predictive policing' (2017) 94 Washington University Law Review 1109, 1140.
[28] Elisabeth Joh, 'The new surveillance discretion: automated suspicion, big data, and policing' (2016) 10 Harvard Law & Policy Review 15, < https://harvardlpr.com/wp-content/uploads/sites/20/2016/02/10.1_3_Joh.pdf > accessed 13.03.2023, 15-16.
[29] These rights are explicitly foreseen by 13/ 2 (f), 14/2 (g), 15/1 (h) of GDPR.
[30] Brinkmann (n 24), 33.

Automated decisions and profiling can be often "opaque" and be carried out beyond the knowledge of the data subject. In that sense, the wording of Article 13(2)(d) requires also informing the data subjects "where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject, should be provided". This provision should be interpreted in a way to make the information available on automated decision-making to data subjects. However, in such cases, the restrictions under Article 13(3) shall be kept in mind. Considering the nature of the law enforcement context, the restrictions or omissions specified in 13 (3) may also apply to the right to information on the automated decision-making process. If the states apply the restrictions, the WP29 urges them to provide the appropriate legal basis via legislative measures. Thus, while transposing the LED into national law, the states should regulate the informational rights and its limits in the framework of automated decision-making.

Moreover, data controllers should follow their obligation to keep a registry of processing operations (pursuant to LED Article 24) which obliges them to specify whether they carry out profiling (LED 24/1 (e)). The obligation to keep logs and registers is not envisioned in the GDPR so explicitly, thus the WP29 underlines that the Member States should be particularly cautious in abiding by this obligation[31] which allows another layer of transparency.

Finally, LED diverges from GDPR also by not setting out further safeguards for data subjects such as the right to express their point of view and to contest the decision[32]. It does not, however, hinder Member States to provide a higher level of protection. Therefore, it is crucial, how the Member States transpose domestically the Directive[33]. Recital 38 of the Directive is also crucial as it stresses that the automated decision-making process should be subject to suitable safeguards, including the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Even though these rights are not articulated within the provisions, denying the existence of the right of data subjects to challenge the automated decisions, since recitals are not legally binding is 'too formalistic', bearing in mind that the Court's case law regularly uses 'recitals as an interpretative aid'[34].

2. Challenges to the right to information and to access

After having tackled the information rights within LED, this part will analyze the challenges to these rights. These challenges rise sometimes due to the fragmented regulations and actors in the security context. On the other hand, the disappearance of institutional and functional boundaries of different agencies threatens data protection rights, including the right to information and access. Finally, analyzing only the LED provisions does not suffice to have a bird's eye over the practical application of these rights. The data subjects may confront some obstacles in practice that hamper the enjoyment of informational rights. Therefore, this part of the paper will tackle these relevant challenges and obstacles by elaborating on different security agents, pointing out different regulations, and concentrating on the practice of data controllers.

[31] Article 29 Data Protection Working Party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)*, 29.11.2017, pp. 14, 15.
[32] GDPR stipulates these rights under Article 22(3).
[33] Orla Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection From Predictive Policing', International Journal of Law in Context, Iss:15, 2019, pp.162-176, p.173.
[34] Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-making in the Framework of the GDPR and Beyond', (2019) 27 International Journal of Law and Information Technology 91, 115.

A. Fragmentation in the area of freedom, security, and justice

The legal framework in the Area of Freedom, Security, and Justice involves many instruments such as SIS II Council Decision[35], PNR[36], VIS[37], and EURODAC[38]. All these instruments, except the PNR Directive, contain substantive and procedural rules on the rights of data subjects, including the rights to information and access[39]. For data subjects, it means a complicated and fragmented framework to exercise their informational rights.

The right to access must be exercised first against the controller. According to 3/7 (a) LED, the controller is the competent authority, meaning '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'. The same provision stipulates that authorities entrusted by national law with public powers to perform the functions of a public authority are also competent authorities. On the other hand, the fragmentation in the security context is reflected in the LED, as it acknowledges the split in the legislative structure between the GDPR, Europol regulation, and regulation for the (EU) institutions[40]. Thus, based on the actor of data processing, the data controller and the regime of data processing will change.

However, these regulations foresee a different regime for access rights. In line with Article 58 SIS II and 14 VIS, indirect access via the national supervisory authority is the rule, meaning that the relevant authority will decide what and how information is to be communicated to the data subject, whereas in LED, direct access is the rule. On the other hand, the EU PNR Directive and EURODAC Regulation simply refer to the 2008 Framework Decision for the exercise of data subjects' rights, which is replaced by LED. It means they should allow direct access as a rule. However, depending on how Member States transpose these directives, the procedures might vary from one state to another. It is also not easy to anticipate now whether instruments such as SIS II and VIS will be amended accordingly[41].

The fragmentation becomes more intermingled if the data is transmitted from one controller to the other or if one controller holds information that is also within the scope of other regulations.

---

[35] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007.
[36] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016.
[37] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008.
[38] Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180, 29.6.2013.
[39] Dimitrova, and de Hert (no 22), 112.
[40] Brinkmann (n 24), 16.
[41] Dimitrova and Paul de Hert (n 22), 124.

For instance, a competent national law enforcement authority may hold data on one or several national information systems. If such an authority receives a request from a data subject under LED, It is not definite whether the contacted authority has an obligation to disclose information regarding the data subject based on SIS II. Depending on if the relevant authority is also a controller according to SIS II or if they interpret the notion of the controller or informational obligations broadly, the data subject may receive such comprehensive information or have to file a separate request for access under the SIS II Council Decision.

However, the SIS II regime has more limitations on the right to access. For example, if a state enters an alarm to SIS II and the data subject makes an access request to another state, Article 58 (3) Council Decision SIS II allows the disclosure only if the State who originally entered the alarm agrees.

Under the security context, EU EUROPOL, EUROJUST, and other European agencies add another layer of complexity, since they are not within the scope of Directive 2016/680[42]. In that sense, the new policy framework on interoperability within Europe will be relevant to have a new perspective on the complicated framework regarding the data subject's rights within the Area of Freedom, Security and Justice. However, as it is not put into effect now, the practice of data subject rights in a fragmented security context remains still unclear.

Finally, in practice it poses also a challenge to untie the GDPR from the LED. For example, data processing for profiling in criminal justice shows how complicated it can get to apply the relevant regulatory framework in practice. Particularly, crime mapping software models such as HART[43] or recidivism risk calculators such as COMPAS[44] include several different predictors as input data. Some of these predictors, such as prior criminal offences may have been collected by the competent authority for law enforcement purposes, thereby the LED applies to data processing. They may also rely on data scraped from various public sources or other data collected for non-law enforcement purposes (e.g. civil status, unemployment status, education level), thus some of the input data would fall within the scope of the GDPR. Considering the legal basis of profiling pursuant to Article 22 GDPR differ from LED 11/1 and the informational rights may be exposed to different restrictions within LED, it would be very complicated to check the legality of process and ensure the relevant rights. Lastly, the fluidity of data flows between public and private actors in the example of predictive policing makes even identifying applicable legal regime a tricky task[45].

B. The fall of the wall between law enforcement and intelligence agencies

Law enforcement agencies work increasingly with intelligence agencies or rely on information obtained initially by these agencies. However, Recital 14 and Article 2/2 (a) LED precise that the Directive should not apply to the processing of personal data in the course of an activity that falls outside the scope of Union law. Thus the activities concerning national security agencies or units dealing with national security issues are not within the scope of LED.

[42] Ibid, 125.
[43] Lynskey (n 33), 175.
[44] For more detailed information on COMPAS see Eleftherios Chelioudakis, 'Risk Assessment Tools in Criminal Justice: Is There a Need for Such Tools in Europe and Would Their Use Comply with European Data Protection Law?' (2020) 2 Australian National University Journal of Law and Technology 72, 89.
[45] Lynskey (n 33), 175.

In comparison to the police, intelligent services are exposed to less regulation or supervision. Therefore, it is very problematic that in reality, the institutional and functional boundaries start to disappear between police and intelligence services. Yet the police shifts increasingly towards an intelligence-type of modus operandi. The 'intelligence-isation' of police agencies (and the term intelligence-led policing) implies that law enforcement applies more sophisticated surveillance technology and enjoys more intrusive investigative powers, approaching their functions to that of intelligence agencies[46]. Increasingly, data mining, trojan horses, and other intrusive methods are enforced to search potential suspects, and the merge with intelligence databases operates beyond the reach of legal access and contestation. Information sharing and exchange may not in itself abolish the institutional barriers between agencies[47], but the nature of large-scale information-sharing activities jeopardizes the safety of data protection rights. In the meantime, the powers of intelligence agencies extend also more towards everyday law enforcement[48]. This deepening erosion can undermine not only the informational safeguards in LED but with a broader perspective the rule of law and civil liberties in general.

An interesting outcome of the wall between agencies can be traced to how some countries transposed the LED. Cyprus, for example, regulated that 'national security activities carried out by police bodies do not fall under the scope of the transposing act'.[49] It proves that police powers are not limited to law enforcement duties, but shows also the danger that some states may not apply informational rights within LED to even to data processing for crime prevention or detection purposes.

Germany, on the other hand, implemented a law that entails that in case the data recipients are intelligence, military counterintelligence, constitutional protection authorities, or any other authorities tackling national security, then data subjects can receive information on these recipients only if the concerned recipient agrees to it. It leaves an extended discretionary power to the recipients, which in turn shows that enabling the right to access, and information is not only in the hands of the data controller[50]. Therefore, the blurring line of duties are worrisome as in the near future less supervised regime for intelligence services may apply to data processing by law enforcement. Furthermore, the national security might be used as an excuse more increasingly to circumvent the data subjects rights.

C. Practical challenges

Unlike GDPR, LED needs to be transposed by Member States into national laws, which causes divergences in practice on data subject rights, including the right of access and information. An empirical study led by KU LEUVEN researchers in 2020 on the national transposition of the LED [51] gave insight into implemented laws in 12 member states [52].

To enjoy the right to access, the first step is finding information on the controller. In practice, even at the first step, there are challenges for data subjects to find out to whom to address the access request. According to the aforementioned study, seven countries under the scope did not

[46] Aleš Završnik, 'Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?' (2013) 9 Journal of Contemporary European Research 181, 186.
[47] Ibid, p. 192.
[48] Ibid, p. 182.
[49] Vogiatzoglou et al (n 21), 282.
[50] Dimitrova and de Hert (n 22), 122.
[51] For the methods and findings of the study, see Vogiatzoglou et al (n 21).
[52] The study concentrated on Italy, Belgium, the United Kingdom, Ireland, the Netherlands, Malta, Spain, Cyprus, Portugal, Greece, Luxembourg, and France.

include information on who the controller is in the case of the LED in their national laws. It is also not always easy to find the relevant information on the website of the centralized entity governing the LEAs (national police authority or the competent ministry)[53].

Another practical impediment for the data subjects is language restriction. Almost all information, which guides the right to access and the answers provided to access requests is in the language of the Member State. However, not all people residing in a country are native speakers, they are yet subject to its laws. It will inevitably put an obstacle for data subjects of other nationalities who request access to their data. Therefore, it might be a better option to provide information on the website of the controller also in English, as it is the language understandable by most [54].

The study also showed that some competent authorities demanded further requirements to enable the right to access, even if such requirements are not stipulated in the national laws[55]. The extra prerequisites include proof of residence (Luxembourg, United Kingdom, Netherlands), an Alien Registration Number (Cyprus), or even proof of residence in the country of request (Ireland for LED). Some member states also impose rather burdensome procedures, such as requiring data subjects to request access by post instead of electronic means (Netherlands, France, and Italy), while others may require official proof of residence in one preferred language (Luxembourg)[56]. Taking into account official documents issued by a local government most likely cost money and time, small practical requirements might turn into discouraging data subjects to use their informational rights.

A third point to mention is the content of the answers. For the rights to access and information to go beyond formalistic rights and be effective in real-life situations, giving substantial answers to access requests plays an important role. However, the above-mentioned study empirically showed the cases where the data controllers refused the right to access due to formalistic conditions such as not being sent via post or the broadness of the scope of the request[57]. Furthermore, practical exercise of the right of access resulted sometimes in the mere confirmation as to whether or not the personal data of the applicants were processed, but the answers did not make any further disclosure. Such customary responses can nevertheless be considered 'formally' compliant, yet if they are short and deprived of content, they would not provide full insight into the processed data. The abovementioned empirical study showed that in most of the responses to access requests, information regarding the recipients to whom the personal data have been disclosed, the envisaged storage period, and the indication of a right to rectification or erasure were missing. In the case of response from data protection authorities, (for example, in Belgium, where indirect access is the rule) some answers confirmed only that the necessary verifications on the lawfulness of processing had been made without confirming whether or not personal data are being processed[58].

[53]The researchers showed that some websites provided very easily accessible information (like Cyprus or Luxembourg National Polices) and others complex in presentation (for instance, Belgium's or Netherlands' authorities), see Vogiatzoglou et al (n 21), 293.
[54] Brinkmann (n 24), 41.
[55] Vogiaztoglou, (n 21) 297.
[56] Brinkmann (n 24), 40.
[57] Vogiatzoglou et al (n 21) 295.
[58] Ibid, 297.

Formal requirements on how to make access requests are not defined in the national act, yet the practical obstacles still persist. Furthermore, the practice differs among the states regarding the type of information that is to be provided and how. Therefore, there is a further need to foster a data protection culture among security authorities and officers, whereby data subjects should feel more invited to exercise their rights. The practical impediments are relatively easier to be solved. In that sense, it could be possible to have a more centralized website with all the information about the processing of personal data in a security and law enforcement context. Providing automated submission forms or standardized templates for data subjects who are less accustomed to the procedures could also facilitate the enjoyment of the right to access. Finally, there is a need to abolish extra requirements such as a certificate of residency or an address[59]. All these practical improvements are easily accomplishable. Nevertheless, further empirical research is needed to point out the inadequacies of other aspects of informational rights in practice. Moreover, there is a need for more supervision of the security authorities for the implementation of best practices.

3. Conclusion

The rights to access and information have broad purposes which contribute to transparency, thus supervision of personal data processing. Furthermore, they raise awareness for a whole society, as in the example of Schrems case[60] which started with a simple request to access personal data. Especially in a security context, these rights enable citizens to surveil the surveillants and from a bigger perspective ensure the rule of law. In an age where massive data collection and analysis may lead to molding people into profiles and stamping them with permanent records, informational rights are crucial to ensure the accuracy of data, prevent its excessive use and control the purposes they are used for. In that sense, LED constitutes an important intervention by empowering the data subjects with rights to access and information.

Nevertheless, these rules and obligations need further clarification to guide the competent authorities, as the practice unfolds differently than the theory. Especially the rights regarding risk assessment tools and profiling need to be strengthened and the limits of information on the impact and functioning of new technologies must be drawn. The exceptions to the right to access and information should be exercised with a perspective that they should be indeed ‘exceptional’. Thus, broader notions such as ‘public security’ and ‘national security’ shall not be extensively used to deprive the citizens of powerful informational rights.

Furthermore, fragmentation of the regulations in a world of interconnected data complicates the exercise of informational rights for citizens, who have to confront several data controllers. Therefore, the right to information and access should be able to give a picture of the whole data circulation.

Finally, the overlapping powers between law enforcement and intelligence agencies require more scrutiny. The disappearance of the wall between different security agents creates an asymmetrical power balance which may well lead to a state of security where the attempts to use informational rights may face several barriers and secrecy. Therefore, considering the shift towards intelligence-led policing and the increased capacity to collect and exchange massive

[59] For more detailed recommendations, see Vogiatzoglou et al (n 21) 298, 99.
[60] Case C-362/14 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrem*s, [2020] ECLI 559.

information, it is imperative now to rebuild the functional and institutional walls between different actors in the security context even more strongly than before.