Impact of the right of access in the balance between security and fundamental rights

Informational power as a tool to watch the watchers

Katherine Quezada-Tavárez[*]

This paper discusses data-driven security practices and the role played by data protection rules in the balance between security and the protection of fundamental rights. Emphasis is placed on the effectiveness of the right of access as a potential tool for informational power at the disposal of citizens, also in the context of security. While the role of the right of access in the general data protection regime has been widely investigated, the impact of data subject empowerment measures in a security context has received little scholarly attention. This article examines to what extent can the right of access under the Law Enforcement Directive and the Passenger Name Record Directive be instrumental in the information empowerment of citizens, thus helping reduce power and information asymmetries in this context. It concludes that the right of access may contribute to the enhancement of citizen empowerment in terms of increasing the transparency and accountability of security-related activities and, hence, can operate as a tool for citizens to 'watch the watchers'.[1]

Keywords: right of access; data protection; Law Enforcement Directive; PNR Directive; informational power

I. Introduction

Predictive analytics, facial recognition and body worn cameras, are some of the sophisticated systems whereby European citizens are being watched.[2] The processing of (personal) data and the free flow of that data enables competent authorities[3] to execute their tasks more efficiently, which in turn facilitates the safeguarding against and the

[*] Katherine Quezada-Tavárez, KU Leuven Centre for IT & IP Law (CiTiP). For correspondence: <katherine.quezada@kuleuven.be>.

[1] This article is based on the first part of the author's thesis defended as part of the final examination for the Master of Intellectual Property and ICT Law at KU Leuven in June 2020. Thesis promotor was Prof. dr. Anton Vedder (KU Leuven) and co-reader Dr. Jan De Bruyne (KU Leuven). Work on the master thesis was conducted within an empirical study into the right of access under the Law Enforcement Directive and the PNR Directive, coordinated by Plixavra Vogiatzoglou, Stefano Fantin and Pierre Dewitte. The empirical study was reported in JIPITEC: Plixavra Vogiatzoglou and others, 'From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives' (2020) 11 JIPITEC 274. The author would like to thank Dr. Sofie Royer (KU Leuven) for helpful comments and suggestions on an earlier version of this paper, and René Mahieu (Vrije Universiteit Brussel) for providing useful input for the reference on indirect access; any error or omission is however the sole responsibility of the author.

[2] See Patrick Williams and Eric Kind, 'Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe' (2019) Project Report 14–27 <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf> accessed 26 September 2020.

[3] As defined in the Law Enforcement Directive (LED), art. 3(7).

prevention of security threats within the EU. For its part, the efficient fight against crime enables the accomplishment of an Area of Freedom, Security and Justice (AFSJ).[4] At the same time, the growing use of sophisticated and invasive technologies for security-related purposes may result in increased surveillance and pose greater risks to fundamental rights.

The above illustrates the competing interests at stake in security-related processing operations. On the one hand, the increasing amounts of (personal) data and the implementation of cutting-edge technology facilitate the work of competent authorities in the pursuit of security needs. On the other hand, the increased sophistication of data-driven security practices has fundamental rights implications and may upset the balance of power between private and public interests. Therefore, it is necessary to find mechanisms to strike a fair balance between both interests. Within the wide range of fundamental rights that may be affected by the use of technological innovations facilitating surveillance practices, privacy and data protection are deemed the most prominently impacted.[5]

In 2016, the EU legislator adopted the Law Enforcement Directive[6] (LED) as part of the data protection package. Along with the data protection reform, the Passenger Name Record (PNR) Directive[7] was introduced in the EU legal framework. Both instruments relate, in one way or another, to data-driven security practices.[8] The LED regulates the processing of personal data by competent authorities for crime-fighting and criminal justice purposes. The PNR, in turn, puts in place air passenger surveillance measures for the prevention, detection, investigation and prosecution of terrorism and serious crime.

Both directives enshrine an arsenal of data protection rights, including the right of access. A large proportion of the scholarly work on data protection has considered the right of access as a tool contributing to the empowerment of data subjects.[9] This appears

---

[4] Which, by the way, is precisely part of the *raison d'être* of the Law Enforcement Directive (LED). See LED, rec. 2.

[5] European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume I: Member States' Legal Frameworks' (2015) 9 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf> accessed 6 September 2019.

[6] 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 [2016] OJ L 119, 89.

[7] 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 [2016] OJ L 119, 132.

[8] Another element in common is that both instruments find their legal basis in the TFEU: art. 16(2) for the adoption of the LED and arts. 82(1)(d) and 87(2)(a) for the adoption of the PNR Directive, respectively.

[9] See for example Xavier L'Hoiry and Clive Norris, 'Introduction – The Right of Access to Personal Data in a Changing European Legislative Framework' in Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer 2017); Jeff Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors. Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4; René

to be the case at least in the framework of data processing by private and public actors that are not law enforcement or security authorities. Surprisingly, little research has focused on investigating its role in a security context.[10] Therefore, this contribution tackles the following question: how does the right of access under the LED and the PNR Directive affect the balance between fundamental rights and the security powers of EU countries? It is addressed using a doctrine-legal approach,[11] i.e. exploring legislation, related case law and literature on the issue.

The three-pronged structure of this paper follows this attempt to answer the research question. First, an analysis of the limitation of fundamental rights for security purposes and the concept of security provides context. Second, this paper tackles two aspects: i) it explores the balance between security and fundamental rights, and ii) it delves into legal safeguards applicable in a security-related context by examining the data protection rules in two EU legal instruments, namely the LED and the PNR Directive. Third, the scope and limitations of the right of access under the LED and the PNR Directive are examined, to then assess the potential effectiveness of the right of access as an empowerment mechanism for citizens in security situations.

II. Limitation of fundamental rights for security purposes

Security powers, as essential components of the state, are based on the social contract between citizens and the executive.[12] As a result, the state is in charge of ensuring the security of its citizens and its territory and holds the powers to prevent and investigate crime. These state powers often presuppose the need to restrict some fundamental rights. For instance, proactive and pre-emptive actions by competent authorities are largely based upon the collection, processing and exchange of personal data.[13] Those activities may entail interferences with the rights to privacy and to data protection.

LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review <https://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect> accessed 29 April 2020; Jeff Ausloos, Michael Veale and René Mahieu, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2019) 10 JIPITEC 283; René LP Mahieu and Jeff Ausloos, 'Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access. A Call to Support the Governance Structure of Checks and Balances for Informational Power Asymmetries' [2020] LawArXiv <https://osf.io/preprints/lawarxiv/b5dwm> accessed 14 July 2020.

[10] During the original research, only one scholarly work devoted to the right of access under the LED was found. See Anna Dimitrova and Paul De Hert, 'The Right of Access Under the Police Directive: Small Steps Forward' in Manel Medina and others (eds), *Privacy technologies and policy* (Springer 2018); however, an empirical study recenlty published examines how does the right of access under the LED and the PNR Directive work in practice (see Vogiatzoglou and others [n 1]).

[11] The original work was part of a larger research endeavour consisting of an empirical study into the right of access under the LED and the PNR Directive. Thus, the master thesis also includes an empirical part, while this paper focuses on the desk-based research. The findings of the empirical study were reported in JIPITEC (see Vogiatzoglou and others [n 1]).

[12] As explained in classical social contract theory. Kenneth Einar Himma, 'Why Security Trumps Privacy' in Adam D Moore (ed), *Privacy, Security and Accountability. Ethics, Law and Policy* (Rowman & Littlefield Publishers 2015) 165.

[13] Valsamis Mitsilegas, 'The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance' (2014) 8 International Political Sociology 104, 104.

The EU Charter of Fundamental Rights (the Charter) provides that interferences with fundamental rights are only permissible if in compliance with certain conditions: (i) as set out by law, (ii) without undermining the very substance of those rights, and (iii) if necessary to pursue a legitimate aim, where proportionate (that is, when those restrictions genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others).[14] Considering the AFSJ as one of the objectives of general interest recognised by EU law,[15] security comprises a legitimate aim that may justify the state interference with fundamental rights. Regardless, even when relying on exceptions to EU law, Member States have to ensure the full effectiveness of EU law.[16]

Both the LED and the PNR Directive relate to the processing of data for security purposes. The LED regulates the protection of personal data with regard to the prevention, investigation, detection or prosecution of criminal offences, including the prevention of threats to public security.[17] Moreover, the LED enables Member States to restrict the provision of information and limit the right of access of data subjects on the grounds of public or national security.[18] The PNR Directive, on the other hand, pursues amongst other objectives that of enhancing internal security.[19] While explicitly referring to various facets of security (i.e. national, internal and public security), neither the LED nor the PNR Directive provide a definition or explanation on what is to be understood by any of those notions. To shed some light on security as used in these two instruments, this section presents a brief analysis on the issue, and ultimately offers a working definition.[20] It then provides some insights on the need for data protection safeguards in security-related processing of data.

1. Concept of security

Defining security and distinguishing its different formulations from one another is not an easy task,[21] and the doctrine is unfortunately still struggling to do so.[22] An approach that

---

[14] Charter, art. 52(1). Likewise, the European Convention on Human Rights (ECHR) states that all interferences with the right to privacy should pursue a legitimate aim (art. 8(2)). In particular, the ECHR refers to national security as one of the legitimate aims to interfere with this fundamental right.

[15] TEU, art. 3.

[16] Hermann-Josef Blanke, 'Article 4: The Relations Between the EU and the Member States' in Hermann-Josef Blanke and Stelio Mangiameli (eds), *The Treaty on European Union (TEU): A commentary* (Springer-Verlag Berlin Heidelberg 2013) 238.

[17] LED, rec. 4.

[18] LED, art. 13(3).

[19] PNR Directive, rec. 5 and 6.

[20] For a comprehensive analysis of national and public security, see Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (Springer International Publishing 2016) s 4.5.2 and 6.8.

[21] European Union Agency for Fundamental Rights, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update' (2017) 53 <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf> accessed 6 September 2019.

[22] See for example Iain Cameron, *National Security and the European Convention on Human Rights* (Kluwer Law International 2000) ch 1; Sophie Stalla-Bourdillon, Joshua Phillips and Mark D Ryan, *Privacy vs. Security* (Springer London 2014) s 1.5.1 and 1.5.2; and Plixavra Vogiatzoglou and Stefano Fantin, 'National and Public Security within and beyond the Police Directive' in Anton Vedder and others (eds), *Security and Law. Legal*

may be used to differentiate them is identifying what each category is not. However, even such an exercise could lead to overlaps.[23]

According to Article 4(2) of the Treaty on European Union (TEU),[24] 'national security' remains the sole responsibility of Member States.[25] On the other hand, reference to 'internal security' is made in three articles of the Treaty on the Functioning of the European Union (TFEU). Two of those three[26] provide an exemption from EU law for Member State measures aimed at safeguarding internal security.[27] Finally, 'public security' can also be found in the TFEU, where it is used in at least three occasions, namely when setting out the conditions for a legitimate restriction of the free movement of goods,[28] in relation to the free movement of workers,[29] and as concerns the freedom of workers from overseas countries and territories.[30]

'National security' is explicitly mentioned in Article 4(2) TEU, a provision that sets forth an important limitation of EU competence in view of the national identity and sovereignty of Member States. Notably, that provision not only declares that the Union shall respect the essential functions of the state (such as security), but goes beyond that by making Member States the only holders of powers over their national security.[31] While this may seem to be a clear cut derogation from EU law, that is not necessarily the case. Firstly, the Treaties give some powers to the EU in certain areas that may affect national security.[32] Secondly, a full understanding of the issue would require a comprehensive analysis of the interpretations by the Court of Justice of the EU (CJEU) of the national security exception, which goes beyond the scope of this contribution. Nonetheless, it is worth mentioning that, according to the settled case law of the Court, the fact that a

---

and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. (Intersentia 2019) ss 3 and 4.

[23] Regardless, it should be noted that none of the notions discussed in this section concern the many other facets of security, such as the security of information systems or cybersecurity, or the right to security. Despite the implications of other formulations for this study, this paper only considers the three notions of security that determine the context(s) where the LED and the PNR Directive apply, or involving circumstances that could have an impact on the application of their provisions. This explains the choice for national, internal and public security.

[24] For a detailed analysis of Article 4(2) TEU, see Blanke (n 16).

[25] However, that derogation from EU law has to be interpreted restrictively, as the Court of Justice of the EU (CJEU) has said in various occasions and reaffirmed in recent case law. See Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service and the Secret Intelligence Service* [2020] ECLI:EU:C:2020:790, para 44; and Joined Cases C-511/18 *La Quadrature du Net and Others*, C-512/18 *French Data Network and Others*, and C-520/18 *Ordre des barreaux francophones et germanophone and Others* [2020] ECLI:EU:C:2020:791, para 99.

[26] The first one only refers to the creation of a committee for cooperation in internal security matters, the Standing Committee on Operational Cooperation on Internal Security (COSI). See TFEU, art. 71.

[27] TFEU, arts. 72 and 276.

[28] TFEU, art. 36.

[29] TFEU, art. 45.

[30] TFEU, art. 202.

[31] Hijmans (n 20) 139.

[32] See for example Article 75 TFEU, providing the legal basis for EU legislation on some areas relating to the prevention and fight against terrorism and related activities, and Article 24(1) TEU, stating that the competence of the Union in respect of issues of common foreign and security policy shall cover all questions relating to the security of the EU.

Member State has taken a measure to protect national security is not a sufficient condition to render EU law inapplicable.[33]

Other sources of EU law seemingly do not provide further clarification on this. National security appears to relate to threats to the interests of the state and protecting its existence or territorial integrity, as seems to be confirmed by the use of the notion in EU secondary law.[34] Yet, it is not limited to threats to the territorial integrity of the state posed by external or internal armed forces, or by foreign actions. It is also a reason that the state would be able to invoke when taking measures that involve a limitation or refusal to comply with its treaty obligations.[35] This brief analysis shows the complexity of this area.

'Internal security', as defined in the Internal Security Strategy for the EU),[36] in a nutshell involves a variety of sectors that pose a threat to '*people and the values of freedom and democracy, [and that hinder the possibility for] everyone [to] enjoy their daily lives without fear*'.[37] It involves the challenges of living in a globalised society and implies security and safety threats with a cross-border effect. The list of the main challenges for the internal security of the EU includes terrorism, serious and organised crime, cross-border crime, and natural and man-made disasters.[38] Considering the components of internal security, it appears to be difficult to draw a clear line between this concept and the other two examined in this section.

'Public security' is also difficult to define. This concept is very much construed depending on the context where it is applied, and is open to interpretation by the CJEU. Scholars have considered public security a somewhat nebulous notion because it is interpreted differently depending on the legal and policy circumstances at the national level.[39] This is evidenced by the *Tele2*[40] judgement, where the CJEU provided a rather unclear reasoning on this.[41]

Public security encompasses both internal and external security.[42] While it was initially left to Member States and considered beyond the tasks of the EU, this changed with the establishment of the AFSJ.[43] While the AFSJ is an area of shared competence

---

[33] See, amongst others, Case C-300/11 *ZZ v Secretary of State for the Home Department* [2013] ECLI:EU:C:2013:363, para 38; Case C-187/16 *Commission v Austria (State printing office)* [2018] EU:C:2018:194, paras 75 and 76; *Privacy International* (n 25), para 44; and *La Quadrature du Net* (n 25), para 99.

[34] Cameron (n 22) 39.

[35] ibid 44–47.

[36] Council of the European Union, 'Internal Security Strategy for the European Union: Towards a European Security Model' (2010).

[37] ibid 12.

[38] ibid 13-15.

[39] Panos Koutrakos, 'Public Security Exceptions and EU Free Movement Law' in Panos Koutrakos, Niamh Nic Shuibhne and Phil Syrpis (eds), *Exceptions from EU Free Movement Law: Derogation, Justification and Proportionality* (Hart Publishing 2016) 191.

[40] CJEU Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* [2016] ECR I-970.

[41] See Christopher Kuner and others, 'An Unstoppable Force and an Immoveable Object? EU Data Protection Law and National Security' (2018) 8 International Data Privacy Law.

[42] Koutrakos (n 39) 190.

[43] Hijmans (n 20) 290.

under Article 4 TFEU, the EU has specified and well-defined powers to legislate in this space. Also, it could be argued that public security is most closely related to the sphere wherein the state has primary responsibility to protect its territory and citizens (usually known as the core of national sovereignty).[44] A different approach, however, suggests that public security concerns 'the security of the European public, its citizens and the EU territory'.[45]

Given the complexities to define it and its different facets, 'security' in the context of this paper is to be understood in the sense of the mandate of national competent authorities for the fight against crime and terrorism, which is essentially what the LED and the PNR Directive are about.[46] This should be regarded as a working definition and is by no means an attempt to grasp all the aspects surrounding this concept.

2. Security-related data processing and its dangers

Although the impact of data processing in the fight against crime and terrorist attacks is difficult to measure,[47] it could hardly be argued that security goals could be fulfilled without the processing and exchange of data. The current digitalisation of life, coupled with the ongoing proliferation of modern-day technology, facilitate the processing of massive amounts of data to detect unlawful activity,[48] with the downside of posing challenges to fundamental rights.[49]

One of the related dangers is indiscriminate mass surveillance. While surveillance is not a new practice, it has been facilitated and improved by the technological advancements.[50] The problem is the scale and systematicity of surveillance practices in the contemporary world.[51] Moreover, the capacity to aggregate a wealth of data items (which may depict a detailed picture of an individual's public and private life),[52] enables the monitoring to occur without the awareness of the individuals concerned.[53]

---

[44] Koutrakos (n 39).

[45] Anna Dimitrova and Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018) 56 Journal of Common Market Studies 751, 760.

[46] Although this may be considered an oversimplification of the notion, it has enabled the author to proceed with the other aspects of the study.

[47] Cian C Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing 2012) 179–181.

[48] Rosaria Sicurella and Valeria Scalla, 'Data Mining and Profiling in the Area of Freedom, Security and Justice: State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection' (2013) 4 New Journal of European Criminal Law 409, 414.

[49] European Union Agency for Fundamental Rights (n 21) 17; for an analysis on the impact of the use of data processing mechanisms as investigative tools, see Sicurella and Scalla (n 48) 412–417.

[50] Franziska Boehm, 'Assessing the New Instruments in EU-US Data Protection for Law Enforcement and Surveillance Purposes' (2016) 2 European Data Protection Law Review 178, 179; Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (NYU Press 2017) 4.

[51] David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001) 1.

[52] Nick Taylor, 'To Find the Needle Do You Need the Whole Haystack? Global Surveillance and Principled Regulation' (2014) 18 The International Journal of Human Rights 45, 48–49.

[53] Eleni Kosta, 'Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights' [2020] Regulation & Governance 2–3 and 7.

Other related dangers in this context emerge from profiling practices. In Europe, profiling techniques for security purposes have been on the rise during recent years, particularly after terrorist attacks in European capitals (such as the 2004 ones in Madrid and the 2005 London attacks).[54] While adopted in the pursuit of legitimate interests, security policies based on profiling entail the massive collection and processing of personal data, thereby posing significant threats to the rights to privacy and data protection. Considering the nature of the security field, the impact on the individuals concerned are likely to be serious.[55]

Although the effectiveness of surveillance technology to deter crime and terrorism is questionable,[56] surveillance is increasingly becoming more indiscriminate, open-ended and affects an ever-growing number of individuals. Thus, in the context of security, many concerns have been raised over massive and pervasive information systems that may enhance the state's (informational) power over citizens, to the detriment of individual rights.[57] A good and relatively recent example of this are the mass surveillance scandals revealed by Snowden, which raised awareness over global mass surveillance activities by security bodies of Western democracies and revived the debate about the balance between security and fundamental rights.[58] These revelations called into question the wide margin of discretion left to states to interpret the extent of limitations on individual rights in the name of national security. Moreover, concerns flourished over the erosion of privacy and data protection in the name of security, which may lead to a surveillance society[59] or even go beyond the usual suspects (i.e. harms to privacy and data protection).[60] For the record, the post-9/11 mass surveillance program exposed by Snowden was recently ruled unlawful and possibly unconstitutional.[61]

---

[54] See Javier Argomaniz, Oldrich Bures and Christian Kaunert, 'A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment' (2015) 30 Intelligence and National Security 191.

[55] In this regard, it is important to note that, to satisfy the requirement of proportionality, only the objective of fighting serious crime could justify measures entailing such a serious interference with the right of data protection such as profiling. This has been reiterated by the CJEU in various occasions (see for example Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECR I-238, paras 27 and 37; Tele2 (n 40), paras 99 and 100; and *Privacy International* (n 2525), para 71.

[56] Joseph A Cannataci, 'Squaring the Circle of Smart Surveillance and Privacy' (2010).

[57] Douwe Korff, 'Passenger Name Records, Data Mining & Data Protection: The Need for Strong Safeguards' (Council of Europe - Directorate General Human Rights and Rule of Law 2015) T-PD(2015)11 <https://rm.coe.int/16806a601b> accessed 9 March 2020.

[58] Dimitrova and Brkan (n 45) 764.

[59] David Lowe, 'The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit for Purpose?' (2017) 17 International Criminal Law Review 78, 89–91.

[60] As Christopher Parsons argued in 2015, by stating that surveillance may even have detrimental effects on how democracies work by undermining the integrity of democratic processes and institutions. Christopher Parsons, 'Beyond Privacy: Articulating the Broader Harms of Pervasive Mas-Surveillance, in Media and Communication' (2015) 3 Media and Communication 1; for a similar line of argument, see Titus Stahl, 'Indiscriminate Mass Surveillance and the Public Sphere' (2016) 18 Ethics and Information Technology 33.

[61] In accordance with the recent judgement by a US Court of Appeals in United States of America v Basaaly Saeed Moalin, AKA Basal, AKA Muse Shekhnor Roble; Mohamed Mohamed Mohamud, AKA Mohamed Khadar, AKA Sheikh Mohamed; Issa Doreh, AKA Sheikh Issa; and Ahmed Nasir Taalil Mohamud (Apps no 13-50572, 13-50578, 13-50580 and 14-50051) [United States Court of Appeals for the Ninth Circuit, 2

III. The LED and the PNR Directive in the balance between security and fundamental rights

The search for a fair balance between security interests and fundamental rights is a long-term effort[62] and a complex exercise.[63] National competent authorities, as state agents, must fulfil their security duties, while doing everything in their power to ensure that the basic rights and freedoms protected in the EU are not undermined. In an age of increased connectivity, security-related processing practices may entail a greater threat to fundamental rights.[64] Measures taken in the interest of security, including large-scale collection of data and surveillance, are not detrimental in themselves. What is wrong is for competent authorities to carry out those activities systematically, arbitrarily and disproportionately.[65] For this reason, state actions need to be accompanied by adequate protection of fundamental rights to conform with EU law and alleviate the power imbalance arising from contemporary data processing practices.

The foregoing raises questions about the balance of power. As the old saying goes, 'knowledge is power'. Although this appears to be accurate on many levels, perhaps it is time to adjust that adage to the digital age by saying that 'data is power'.[66] Given that the government suddenly has massive amounts of data as well as the capacity to process these, it can be argued that the state's powers over its citizens have significantly increased. Although some pieces of data might not be that useful in themselves, the possibility to combine information from different sources empowers competent authorities to create richer profiles and draw precise conclusions on the private life of individuals. Hence, modern data-driven security practices are leading to an informational imbalance between citizens and the state as they facilitate the amplification of prior surveillance practices.[67]

Against this backdrop, it is appropriate to study the role of the EU data protection rules in the tension between the need to protect fundamental rights and the need to process data for security purposes. To that end, this section explores the materialisation of data protection requirements in the EU legal instruments applicable to security-related processing. The analysis focuses on the LED and the PNR Directive.

1. Overview of the LED[68]

September 2020] <https://cdn.ca9.uscourts.gov/datastore/opinions/2020/09/02/13-50572.pdf> accessed 7 September 2020.

[62] Stalla-Bourdillon, Phillips and Ryan (n 22) 66.

[63] Diana Alonso Blas, 'Ensuring Effective Data Protection in the Field of Police and Judicial Activities: Some Considerations to Achieve Security, Justice and Freedom' (2010) 11 ERA Forum 233, 243–244.

[64] As explained in the previous section.

[65] See *Big Brother Watch and Others v the United Kingdom* App no 58170/13 (ECtHR, 13 September 2018) para 495.

[66] See Lena Ulbricht and Maximilian von Grafenstein, 'Big Data: Big Power Shifts?' (2016) 5 Internet Policy Review.

[67] See, to that effect, 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) 8 <https://edps. europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 20 June 2020.

[68] This sub-section consists of a shortened version of the LED's overview provided in the original work.

The LED[69] constitutes the single EU legal instrument largely covering the protection of personal data in the context of police and criminal justice. It sets forth a set of principles and requirements that seek to achieve a balance between individual rights and the objectives pursued by competent authorities in security-related processing. In its preamble, the LED starts by acknowledging the new challenges for the protection of personal data brought by rapid technological developments and globalisation, involving a significant increase in personal data collected and shared in law enforcement activities.[70] In response to that, the LED sets limits and conditions for the processing of personal data by competent authorities and promotes good data practices.

a. Subject matter and scope

The LED regulates the protection of personal data in the law enforcement sector, covering both transborder and domestic processing[71] by competent authorities[72] for the purposes of the prevention, investigation, detection or prosecution of criminal offences. While it is for national laws to further specify and concretise those purposes, the LED creates the conditions for a more uniform application of data protection rules in law enforcement across the EU.[73] Considering its application to a specific sector (i.e. law enforcement), the LED constitutes a *lex specialis* to the general and more widely known GDPR.

b. Data subject rights

One of the key objectives of the European Commission when first announcing the data protection reform in 2010 was to 'enhanc[e] control over one's own data'.[74] Accordingly, the reform paved the way for an approximation of Member State's laws as to the procedures to exercise data subject's rights. Moreover, the LED proceduralised the remedial system under EU data protection law by tackling discrepancies in data protection rules across the EU and strengthening data protection safeguards.[75]

---

[69] Which repealed the Council Framework Decision 2008/977/JHA. LED, rec. 4 and 7.

[70] LED, rec. 3.

[71] Which means that it broadens the scope of the previous legal framework. This extension of the scope entails that police and criminal justice authorities no longer have to apply various data protection rules on the basis of the origin of the personal data. Paul De Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive: A First Analysis' (2016) 7 New Journal of European Criminal Law 8.

[72] Defined in LED, art. 3(7).

[73] Thomas Marquenie, 'The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework' (2017) 33 Computer Law & Security Review 324, 328. It should be noted that, despite the shortcomings addressed by the data protection reform, the amended data protection framework reportedly remains flawed, in particular when it comes to the use of modern data-driven technology by competent authorities. See 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; Thilo Gottschalk, 'The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement' (2020) 6 European Data Protection Law Review 21.

[74] European Commission, 'COM(2010) 609 Final Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of Regions - A Comprehensive Approach on Personal Data Protection in the European Union' (European Commission 2010) 7 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 20 June 2020.

[75] For an analysis of the proceduralisation rules stemming from the EU data protection regime, see Antonella Galetta and Paul De Hert, 'The Proceduralisation of Data Protection Remedies under EU Data

Under the LED,[76] data subjects have the right to be informed about the processing of their personal data, have access to their data and obtain certain information about the processing, have their personal data rectified by the controller, ask for the erasure or restriction of their personal data, and exercise data subject rights either directly or indirectly (through the competent supervisory authority).[77] Other rights in the LED include the right not to be subject to decisions based solely on automated processing and to obtain human intervention in case such decisions are authorised by law.[78]

2. Overview of the PNR Directive[79]

Numerous legal instruments regulating the use of PNR data[80] were adopted worldwide in the aftermath of major terrorist attacks, particularly after 9/11[81] in view of the way in which these attacks were performed.[82] PNR data are collected and processed to track terrorists and other criminals by identifying potential unsuspected individuals before they reach the territory of the target state.[83]

a. Subject matter and scope

The PNR Directive governs the collection, use, retention and exchange of PNR data.[84] PNR data may support security-related activities by facilitating the identification of known or potential suspects of terrorism or serious crime. Such identification results from the performance of assessments based on travel patterns and other indicators that usually relate to criminal activities.

Under the PNR Directive, air carriers are obliged to share PNR data with the relevant Passenger Information Unit (PIU)[85] to support the fight against terrorism and serious crime.[86] As specified in the legal text,[87] the scope of the PNR Directive is limited to the PNR data collected for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[88] In principle, the Directive applies to international

---

Protection Law: Towards a More Effective and Data Subject-Oriented Remedial System?' (2015) 8 Review of European and Administrative Law 125.

[76] Arts. 13-17.

[77] See also section IV.4 below.

[78] LED, rec. 38 and art. 11.

[79] This sub-section consists of a shortened version of the PNR Directive's overview provided in the original work.

[80] i.e. information related to air passengers that is collected and maintained for commercial purposes in the reservation and departure control systems of carriers. See PNR Directive, art. 3(5).

[81] Which resulted in a 'post-war on terror world'. See Murphy (n 47).

[82] Taylor (n 52) 46; Valsamis Mitsilegas, *The Criminalisation of Migration in Europe: Challenges for Human Rights and the Rule of Law* (Springer 2015) 25.

[83] PNR Directive, rec. 7.

[84] PNR Directive, art. 1.

[85] A specific entity created under the PNR Directive responsible for the collection, storage, and processing of PNR data (PNR Directive, art. 4).

[86] PNR Directive, art. 1 and 4(2).

[87] PNR Directive, art. 1(2).

[88] Annex II of the PNR Directive enumerates the offences that fall under the category of 'serious crimes'. That list of offences is broad and much wider than the serious crimes that are enumerated in art. 83(1) TFEU.

flights to and from the EU.[89] However, its scope may extend to intra-EU flights, which is a decision left to the Member States' discretion, provided they notify the Commission.[90]

b. Relation with the LED[91]

Considering the impact of a PNR scheme on the protection of personal data, it should be coupled with fundamental rights safeguards.[92] Accordingly, the PNR Directive allows the use of PNR data, while considering fundamental rights, such as data protection and non-discrimination.[93] While the safeguards incorporated by the PNR Directive have been considered sufficient by some,[94] others disagree. That could explain why the PNR Directive is being challenged in different courts across the EU, leading to references for preliminary rulings before the CJEU with questions over its compatibility with fundamental rights.[95]

What is certain is that the PNR Directive is closely tied to the LED and, as such, to the data protection regime. Notably, the PNR Directive contemplates a data protection clause (Article 13), whereby it embraces data protection standards established in the LED. That clause mandates that personal data are to be protected under the terms of the LED for every passenger subject to the PNR system, including the rights granted to data subjects in the LED. The PNR Directive also mandates that a high level of protection of privacy and personal data must be ensured in the transmission and processing of the PNR data.[96]

3. Role of the two directives in the legal framework

A key objective of the LED and the PNR Directive is to facilitate the exchange of (personal or PNR data) between EU competent authorities,[97] a goal in line with the AFSJ policy.[98] 'The architecture of surveillance also needs an architecture of accountability,'[99] which in a data-rich environment can be achieved by applying the highest standards of data protection in security. Yet, as the EU legislator has acknowledged, the field of security

[89] PNR Directive, art. 1(a).
[90] PNR Directive, art. 2.
[91] See also Vogiatzoglou and others (n 1) s D.III.
[92] As Hornung and Boehm highlighted in a study comparing three EU-US PNR agreements which existed before the PNR Directive (i.e. those of 2004 and 2007, and a draft of 2011). Gerrit Hornung and Franziska Boehm, 'Comparative Study on the 2011 Draft Agreement between the Unites States of America and the European Union on the Use and Transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security' (Greens/EFA Group in the European Parliament 2012) <https://www.zar.kit.edu/DATA/veroeffentlichungen/237_PNR-Study-FINAL-120313_6a66ded.pdf> accessed 10 April 2020.
[93] PNR Directive, rec. 20 and 36.
[94] See for example Lowe (n 59).
[95] See request for a preliminary ruling in: Case C-817/19 *Ligue des droits humains*, lodged on 31 October 2019; joined Cases C-148/20, C-149/20 and C-150/20 *Deutsche Lufthansa*, lodged on 16 and 17 March 2020; and Case C-222/20 *Bundesrepublik Deutschland*, lodged on 27 May 2020.
[96] PNR Directive, rec. 23 and 31.
[97] LED, art. 1(2)(b). PNR Directive, art. 1(b).
[98] Anna Jonsson Cornell, 'EU Police Cooperation Post-Lisbon' in Maria Bergström and Anna Jonsson Cornell (eds), *European Police and Criminal Law Co-operation* (Hart Publishing 2014).
[99] Ferguson (n 50) 201.

merits a special legislative treatment.[100] Therefore, the particularities of security-related processing, as opposed to more general data processing, call for more flexible rules not to undermine security operations.[101] This manifests itself by the adjusted data protection principles that the LED mandates (which should also be met by the PNR Directive),[102] as opposed to those applicable in a processing of personal data governed by the GDPR. [103]

Having adequate data protection standards, particularly in security-related processing, can favour both human rights and security interests. On the one hand, data protection standards entail safeguards for fundamental rights, thereby boosting citizens' trust in how data are used and made available in security. On the other hand, strong human rights protection reinforces trust in international cooperation, leading to a more efficient performance of security duties. Therefore, both directives seem to play a relevant role in the balance between security and fundamental rights by enshrining individual rights without frustrating the exigencies of competent authorities.

Despite their similarities, however, a major difference between the two should be acknowledged, relating to their focus. While the LED is devoted to the protection of personal data in law enforcement processing, the core of the PNR Directive is to regulate the use of specific data (i.e. PNR data) for the fight against particular crimes (i.e. terrorist offences and the serious crimes). This seems to suggest that the EU PNR Directive is a *lex specialis* to the LED, which is more general as to the data and activities it regulates.

IV. The right of access as a pillar of citizen empowerment in general processing and in security[104]

The right of access is one of the subjective rights granted to data subjects in data protection legislation, including the LED, and it is also incorporated in the PNR Directive by virtue of its data protection clause.[105] In recent years, an impressive body of work has been generated by scholars investigating the effects of the right of access, mostly in the context data processing in the private and public sectors (not including law enforcement or security authorities).[106] In essence, those studies have regarded the right of access as

[100] For instance, in Declaration 21, annexed to the final act of the intergovernmental conference to adopt the Treaty of Lisbon (which provided the legal basis for the adoption of the most recent data protection reform). That declaration acknowledges to adopt specific data protection rules for the law enforcement sector because of the specific nature of security-related activities.

[101] De Hert and Papakonstantinou (n 71).

[102] See PNR Directive, rec. 36.

[103] Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European Data Protection Law Review 367, 369.

[104] See also the theoretical underpinnings of the empirical study on the LED and the PNR Directive referred to earlier (Vogiatzoglou and others [n 1]).

[105] PNR Directive, art. 13(1).

[106] Many of those publications even include an empirical account of their findings. See Keith Spiller, 'Experiences of Accessing CCTV Data: The Urban Topologies of Subject Access Requests' (2016) 53 Urban Studies 2885; Antonella Galetta, Chiara Fonio and Alessia Ceresa, 'Nothing Is as It Seems. The Exercise of Access Rights in Italy and Belgium: Dispelling Fallacies in the Legal Reasoning from the "Law in Theory" to the "Law in Practice"' (2016) 6 International Data Privacy Law 16; Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer International Publishing 2017); Mahieu, Asghari and van Eeten (n 9); Ausloos and Dewitte (n 9); Mariano Di Martino and others, 'Personal Information Leakage by Abusing the GDPR "Right of Access"', *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* (2019); Mahieu and Ausloos (n 9); however, recent scholarship

a tool that enables data subjects to exercise control over their personal data.[107] By the same token, the right of access has the potential to work as an empowerment mechanism for citizens in security as well (as argued in this section).[108]

1. The right of access as a pillar of citizens' empowerment

In its recent report on the two years since the introduction of the GDPR, the European Commission highlighted the role of 'data protection as a pillar of citizens' empowerment'.[109] Amongst the data protection rights granted to data subjects, the right of access seems to occupy a prominent place. This is what the CJEU seems to suggest in cases where it said that the right of access is a precondition for the exercise of other data subject rights.[110] The European Court of Human Rights (ECtHR) seems to follow a similar path when ruling that not granting individuals access to information is a way of depriving them of the opportunity to refute that information.[111]

Current literature has widely investigated the diverse roles played by the right of access. To begin with, the right of access is considered as a tool that enables data subjects to exercise more control over their data.[112] In particular, it 'is a vital safeguard against informational power asymmetries in an increasingly datafied society'.[113] Moreover, it is the first mechanism against data protection violations envisaged in data protection law as it enables individuals to examine the legality of the processing and take action in case of data protection breaches. It is also an instrument to make data-driven practices more scrutable and to monitor whether data protection breaches have been effectively remedied. Furthermore, the right of access empowers individuals to have a direct impact on policies and legislative initiatives.[114] This could be particularly effective when individuals join forces to address power imbalances between data subjects and

---

shows a growing interest in the right of access in a security context as well. See comprehensive analysis on the right of access under the LED in Dimitrova and De Hert (n 10); see also empirical study on the right of access under the LED and PNR Directive, reported in JIPITEC: Vogiatzoglou and others (n 1).

[107] See, among others, L'Hoiry and Norris (n 9) 7; Ausloos and Dewitte (n 9); Mahieu, Asghari and van Eeten (n 9) 3–4; Mahieu and Ausloos (n 9) 2.

[108] However, De Hert and Papakonstantinou argue that the limitations for the exercise of data subject rights might curtail their effectiveness. See De Hert and Papakonstantinou (n 71) 12–13.

[109] European Commission, 'COM(2020) 264 Final Communication from the Commission to the European Parliament and the Council - Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation' (European Commission 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264> accessed 4 July 2020.

[110] According to the CJEU's ruling in Case C-553/07 *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* [2009] ECR I-3889, paras 51-52. This standpoint has been confirmed by the Court in subsequent rulings. See for instance Joined Cases C 141/12 and C 372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* [2014] EU:C:2014:2081, para 57; Case C434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C:2017:994, para 57.

[111] As the Court stated in *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987) para 48 and *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000) para 46.

[112] 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) 5 <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> accessed 20 June 2020.

[113] Mahieu and Ausloos (n 9) 2.

[114] As illustrated by the success stories relating to the privacy activist Max Schrems, who has pursued privacy campaigns that started by a data subject access request. L'Hoiry and Norris (n 9) 2.

controllers.[115] In addition, the right of access does not only help to redress informational power asymmetries, but it is also a crucial component of the 'ecology of transparency'.[116]

As suggested by existing case law and literature, the right of access arguably grants data subjects 'informational power',[117] and may be considered to serve various purposes (outlined above). Therefore, it can be concluded that the right of access is, at least in theory, a key component of the data subjects' empowerment.[118]

Despite the wide acceptance of the right of access as an empowerment mechanism, not all scholars support this view. For instance, Koops[119] claims that data subject rights are theoretical and not meaningful in practice, and thus cannot grant individuals actual control over their personal data. He suggests that not even the success stories of the exercise of data subject rights seem to hint at the effective control of data subjects over the processing of their data. He also states that the complexity of data protection rules compounds the problem of controller compliance. Hence, in Koops' view, 'informational self-determination is unenforceable'.[120]

Lazaro and Le Métayer[121] also question whether the right of access can work as an empowerment mechanism. They suggest that the assumption that data protection law provides 'control' results from a flawed view of privacy and data protection theories.[122] Similarly, Van der Sloot[123] raises doubts about whether more subject access duties and rights could be effective or even feasible. In addition, Cormack[124] disputes the practical significance of the right of access, and even asks whether this right poses potential threats to privacy.

Another issue to consider is the potential risks that the right of access may create. For instance, the exercise of the right of access lends itself to abuse and wrongdoing, as evidenced by an empirical study revealing flaws in the management of subject access requests.[125] Those flaws could lead to personal data leakages and might eventually result in identity theft.[126]

Some argue that data protection law in general and the right of access in particular empower individuals, while others argue that they do not. For the sake of simplicity, this paper assumes that they do. Also, regardless of the potential misuse of

---

[115] Mahieu, Asghari and van Eeten (n 9).
[116] Mahieu and Ausloos (n 9) 2–5.
[117] Ausloos, Veale and Mahieu (n 9) 296.
[118] Norris and others (n 9) 1; see also Ausloos and Dewitte (n 7).
[119] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 251–253.
[120] ibid 252.
[121] Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed <https://script-ed.org/article/control-over-personal-data-true-remedy-or-fairy-tale/> accessed 27 July 2020.
[122] For a similar argument, see Leiser and Custers (n 103).
[123] Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307, 324.
[124] Andrew Cormack, 'Is the Subject Access Right Now Too Great a Threat to Privacy?' (2016) 1 European Data Protection Law Review 15.
[125] See Di Martino and others (n 106).
[126] ibid.

data protection rights, this contribution views the right of access as a tool intended to serve the greater good (a goal that it seems to achieve, more often than not). On that premise, it is possible to further investigate the right of access and its role in a security context.

2. Scope of the right of access under the LED and the PNR Directive

The informational power of data subjects (*supra*) may be found in the LED and the PNR Directive. Article 14 of the LED (integrated in the PNR Directive through its Article 13) grants data subjects the right to be informed whether personal data concerning them are held by the controller and to receive certain supplementary details (including the purposes of and legal basis for processing, the categories of personal data concerned, and the envisaged period for which the data will be stored). The manner of exercising the right of access is regulated in Articles 12 and 17 LED: through direct request by the data subject and, if restricted, through the competent supervisory authority (see *infra*).

Under the LED, a controller is to be understood as a law enforcement agency in its performance of law enforcement tasks (i.e. the exercise of the security powers of the state). In other words, it appears that under the LED controllers in the private sector are beyond the scope of the right of access (at least in theory),[127] even when assisting competent authorities in their security duties.[128] This means that, for example, when Google discloses data (e.g. the browsing history of data subjects) to the police, that processing operation (i.e. data disclosure) is also governed by the GDPR, similar to other processing activities by the company.

The PNR Directive does not refer to the notion of 'controller' as such. Yet, it requires Member States to set up a specific entity (the PIU) responsible for collecting and analysing PNR data. The PNR Directive also requires EU countries to adopt a list of competent authorities entitled to request or receive PNR data.[129]

Amongst the information that competent authorities have to provide to data subjects is the legal basis for the processing. This requirement of the LED (and thus also the PNR Directive) evidences some of the differences between the general data protection regime and the one applied in a security context. While the GDPR provides a list of legitimate grounds for processing,[130] the LED does not. Instead, the latter requires that the processing of data is based on EU or Member State law, and that it is necessary for the performance of a law enforcement task by a competent authority.[131] Also, unlike under the GDPR,[132] data subjects' informational rights in a security context do not appear to include the right to have a copy of the data being processed. The LED seems to be more nuanced, stating that 'it is sufficient to provide a full summary of those data (…)

[127] Dimitrova and De Hert (n 10) 116.
[128] This reasoning seems to be confirmed by the recent CJEU case law. See, to that effect, *Privacy International* (n 25), para 46, and *La Quadrature du Net* (n 25), para 101.
[129] PNR Directive, art. 7(1). The wide variety of competent authorities that Member States notified to the European Commission (according to art. 7[3] PNR Directive) is noteworthy (see Vogiatzoglou and others [n 1] 284).
[130] GDPR, art. 6.
[131] LED, art. 8.
[132] Art. 15(3).

[which] could also be provided in the form of a copy of the personal data undergoing processing.'[133] It is thus not evident that data subjects are entitled to a copy of their personal data under the LED and the PNR Directive.

In addition, although the LED requires controllers to inform data subjects of the envisaged storage period, or at least the criteria to determine it, the purpose for processing might change. Since the change of purpose does not form part of the information obligations imposed on controllers,[134] the data could potentially be stored for longer than initially envisaged (and thus for longer than the data subject might expect). This limitation of the right of access under the LED reveals the higher level of discretion of the state in a security context.[135]

3. Effect of the right of access in a security context: a mechanism to achieve a better balance?

The more citizens are aware of flourishing surveillance practices, the more citizens can somehow monitor those, or at least to request a restriction or modification of data collection initiatives.[136] Assuming that the right of access can grant data subjects control over their data, it could also become a powerful tool for citizens with regard to security-related processing. In the same manner as the right of access is said to operate as a tool for data subjects' empowerment, it may also be instrumental in scrutinising the activities undertaken by competent authorities and encouraging more transparent security-related processing.[137] In other words, the right of access can help citizens monitor whether competent authorities are acting in conformity with the law.

This reasoning seems to be endorsed by the CJEU and the ECtHR. For instance, in *Rijkeboer*[138] the CJEU stressed that the right of access enables individuals to exercise the right to remedy data protection violations. The ECtHR has come to analogous findings in cases such as *Leander* and *Rotaru*.[139] Another relevant case is *Khelili*,[140] which shows the importance for citizens to have tools to access data held by competent authorities to detect unlawful data processing practices.

Further, in *Leander,*[141] the ECtHR alluded to the importance of access rights for the balance between competing and conflicting interests. The Court applied a similar reasoning in *Gaskin v UK*.[142] Moreover, the ECtHR seems to suggest[143] that the denial of access rights may be considered as a disproportionate and thus illegitimate interference with fundamental rights if the decision in question fails to strike a fair balance between

---

[133] LED, rec. 43.
[134] LED, art. 13.
[135] See Antonella Galetta and Paul De Hert, 'A European Perspective on Data Protection and the Right of Access' in Norris and others (n 9) 27.
[136] Lyon (n 51) 38.
[137] As it enables the verification of legitimacy of data practices. Mahieu, Asghari and van Eeten (n 9) 3; European Union Agency for Fundamental Rights (n 21) 124.
[138] (n 110), para 52.
[139] See section IV.I above.
[140] See *Khelili v Switzerland* App no 16188/07 (ECtHR, 18 October 2011) paras 68-71.
[141] (n 111), paras 59-63.
[142] *Gaskin v. the United Kingdom* App no 10454/83 (ECtHR, 7 July 1989) paras 43 and 49.
[143] At least implicitly (see Galetta and De Hert [n 135] 31).

competing interests.[144] The ECtHR also refers to the importance of information empowerment for data subjects to become aware of data protection violations, thus giving effect to the remedial system put in place by the data protection framework. A case in point is *I v Finland,*[145] where the Court found that the 'practical and effective protection to exclude any possibility of unauthorised access' to the data was not ensured, thereby leading to a data protection violation.

Information empowerment tools for citizens become even more important in security situations considering the power imbalance that characterises citizen-state relations. This is indeed the case as the information empowerment of individuals does not always entirely match the nature of the public sector interests.[146] The problem with information asymmetry and imbalance of power is that they may make it more difficult for individuals to detect or prove abuses of power. For example, it might be hard for citizens to demonstrate that their personal data have been unlawfully collected or unduly processed, particularly as data-gathering and data-processing techniques are becoming ever more sophisticated (as illustrated by Snowden's revelations).[147]

Also, its importance in security also relates to the secrecy that tends to characterise crime-fighting practices (particularly on the use of technology).[148] Secrecy can be an obstacle for citizens seeking to hold competent authorities to account, let alone to question the tools being used for security purposes. For instance, it can prove difficult to be removed from a secret police database, or even to question its management, if the individual is not aware that he or she has been (unduly) included.[149]

The positive impact of the information empowerment of citizens is also relevant in this context in view of the potential life-altering decisions that may result from security-related processing. An example of this would be the improper and excessive collection and processing of personal data by the police, without legitimate purpose, proportionality or sufficient guarantees (e.g. the storage of inaccurate or unnecessary information during a criminal investigation). This could potentially lead to the wrongful arrest, imprisonment, and conviction of individuals.

Against this background, the LED and the data protection provisions in the PNR Directive create some of the conditions that are needed to balance the information-driven power asymmetry between citizens and the state. The right of access can be a way

---

[144] In light of the *Haralambie v. Romania* ruling App no 21737/03 (ECtHR, 27 October 2009) paras 86 and 96.

[145] App no 20511/03 (ECtHR, 17 July 2008) para 47.

[146] Koops (n 119) 253.

[147] One of the lessons learned from the information revealed by Snowden is that it is crucial for citizens to fully comprehend the interplay between the protection of fundamental rights (such as privacy) and the advancement of security-related practices in order to set appropriate limits to the security powers of the state.

[148] Ferguson (n 50) 53.

[149] ibid. See also comment in the opinion of the Belgian data protection authority on a draft text of the national transposition of the GDPR and the LED, Commissie voor de bescherming van de persoonlijke levenssfeer, 'Voorontwerp van Wet Betreffende de Bescherming van Natuurlijke Personen Met Betrekking Tot de Verwerking van Persoonsgegevens (CO-A-2018-026)' (2018) Advies nr. 33/2018 para 213 <https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-33-2018.pdf> accessed 13 February 2021.

for citizens to know and control the data trails they leave behind in their everyday actions and that are eventually collected, accessed or processed by competent authorities. Moreover, it can be used to enforce or encourage accountability. If competent authorities know that they will be held accountable for intrusive data-driven security processing, they may be less inclined to proceed with such operations. In that way, the right of access can be a way for citizens to 'police the police'. This is even more important in a data-driven culture as those informational imbalances are expected to worsen in a big data environment.[150]

4. A right subject to limitations, but indirect access as additional avenue for redress

Despite the foregoing, it is important to bear in mind that the right of access is not absolute. For instance, it does not entail the right to access any record containing personal data, as not all information concerning the data subject is to be considered personal data. Think of the legal analysis in an administrative document about the data subject, which cannot be classified as 'personal data' within the meaning of data protection law.[151]

Moreover, the LED (and thus also the PNR Directive) contemplates the possibility to restrict the exercise of the right of access wholly or partially, subject to conditions and procedures.[152] Considering how broadly these restrictions are phrased, controllers seem to have a wide margin of appreciation to use exemptions, which could potentially curtail the positive effect of the information empowerment of citizens.[153]

Nevertheless, in cases where the right is fully or partially restricted, the data subject may turn to the relevant supervisory authority to exercise what is known as the 'indirect access'.[154] In that case, the competent supervisory authority, acting on behalf of the data subject, should make the necessary verifications on different aspects, including which data of the data subject are processed, the lawfulness of the processing, and the accuracy of the data. Subsequently, the supervisory authority should inform the data subject at least that the necessary verifications or review have taken place and that the data subject may seek a judicial remedy.[155] It might seem to follow that additional information may also be provided.

On first impression, indirect access may appear to have little or no effect on the citizen empowerment. A closer examination, however, shows that the exercise of the right of access through the competent supervisory authority offers an additional means of redress. Competent supervisory authorities do not only act on behalf of data subjects

---

[150] European Data Protection Supervisor (n 67) 8.

[151] As the CJEU said in a judgement bringing some clarity about scope of the right of access under the data protection regime. See *YS* (n 110), para 48.

[152] LED, art. 15. This provision sets out the four conditions to be met for the restriction, namely: (i) based on a legislative measure adopted by the state; (ii) for as long as it is necessary and proportionate; (iii) with due regard for the fundamental rights and legitimate interests of data subjects; and (iv) in the pursuit of at least one of the legitimate purposes listed in the LED (e.g. avoid prejudicing law enforcement tasks or protecting public security). It is worth noting that restrictions to the right of access are not unique to security situations: similar limitations apply under the GDPR, as per its art. 23.

[153] De Hert and Papakonstantinou (n 71) 12.

[154] See LED, art. 17.

[155] LED, art. 17(3).

to make the necessary verifications on the lawfulness of the processing, but they also take action where necessary. In this way, indirect access may entail the possibility for a data subject to have his or her personal data removed from a police database where those are unduly kept, for example.[156] For an individual, that action can mean the difference between being offered a job or not due to certain data included in his or her criminal record for longer than necessary.[157]

The verifications by supervisory authorities as part of indirect access requests become particularly important in security considering that 'data subjects usually do not know whether, let alone why, their personal data are processed in a [security] database'.[158] Yet, it has been reported that, when carrying out the necessary checks on behalf of data subjects, the relevant supervisory authorities have encountered many instances of erroneous data in security-related databases.[159] Crucially, these findings provide compelling evidence that indirect access operates as a counterweight to the restrictions laid down in the LED and offers an additional avenue for redress in security situations. Moreover, these results also highlight the role played by national supervisory authorities in the 'ecology of transparency'.[160]

V. Conclusion

In this paper, it has been argued that the information empowerment of data subjects, in the shape of access rights, may help to counterbalance the security powers of the state enhanced by modern processing capabilities. Starting from the premise that 'data is power', it can be said that states' increased data processing capabilities threaten to alter the balance between security and fundamental rights. As the findings of this study show, recent improvements in the data protection law focus on empowerment and control by data subjects. A key element of that empowerment is the right of access, which allows data subjects to learn more about how their data are collected and processed.

---

[156] Even data about individuals that had not been accused of any crimes are sometimes retained by competent authorities for longer than could be expected, with all the potential consequences that this can have. For some examples of this, see Commission Nationale de l'Informatique et des Libertés (CNIL), '39e Rapport d'activité 2018' (2019) 49 <https://www.cnil.fr/sites/default/files/atoms/files/cnil-39e_rapport_annuel_2018.pdf> accessed 13 February 2021.

[157] This is one of the examples that illustrate the importance of indirect access, which may be found in the 2019 yearly report of the French data protection authority (the latest at the time of writing). See Commission Nationale de l'Informatique et des Libertés (CNIL), '40e Rapport d'activité 2019' (2020) 87 <https://www.cnil.fr/sites/default/files/atoms/files/cnil-40e_rapport_annuel_2019.pdf> accessed 13 February 2021.

[158] Commissie voor de bescherming van de persoonlijke levenssfeer (n 149) para 213.

[159] See for example the annual activity report 2005 by the French data protection authority, where it is indicated that errors were found in at least 40% of the files inspected. See Commission Nationale de l'Informatique et des Libertés (CNIL), '26e Rapport d'activité 2005' (2006) <https://www.cnil.fr/sites/default/files/atoms/files/20171116_rapport_annuel_cnil_-_rapport_dactivite_2005_vd.pdf> accessed 13 February 2021. Considering the 1.760 indirect access requests received during that year (a number that has more than doubled in the last five years, according to the figures in the annual activity report 2019 [see n 149 above]), it can be reasonably assumed that many data protection violations can be effectively remedied by supervisory authorities in this way.

[160] For a comprehensive analysis of the ecology of transparency and its components, see Mahieu and Ausloos (n 9) 2–12.

The main point of this contribution is that the information empowerment of data subjects, in the shape of access rights, may be instrumental in addressing informational power asymmetries. In that way, the right of access, as one of the rights granted to data subjects in the LED and the PNR Directive, can be expected to foster greater transparency of the data processing activities performed for security. Also, it can act as a safeguard against the disproportionate and unaccountable exercise of security powers. Moreover, the right of access may serve as a tool to remain vigilant, to identify and stop abuse before it happens, as well as to advocate for more accountability in security-related data processing practices. As such, the right of access is instrumental in making data-driven security practices more scrutable and, thus, can enable citizens to 'watch the watchers'.

The right of access under the LED and the PNR Directive brings hope, but it is certainly not a panacea for all ills. The question remains whether it will serve all the purposes discussed above. Another open question is whether it can operate as a tool for transparency that provides the average citizen meaningful information about data-driven security practices. Hence, further research is needed to test the boundaries of Article 14 LED and other informational rights in security-related instruments to assess the reach of citizen's empowerment in this context.