UtrechtLawReview

Real Transparency and Real Oversight of Law Enforcement Data. The ECHR and the Lack of Accountability of Indirect Access Procedures

ARTICLE

DIANA DIMITROVA
PAUL DE HERT
*Author affiliations can be found in the back matter of this article

ABSTRACT

The present paper looks at the right of access to one's data, especially in the law enforcement sector, as developed by the European Court of Human Rights (ECtHR) with regard to the right to private life (Article 8) and to effective remedies (Article 13) in the European Convention on Human Rights (ECHR). Can this right to directly access one's data be (entirely) replaced, as happens with the practice of 'indirect access', by a system of independent oversight by administrative (data protection) authorities? If yes, under what conditions would such a system be rights compatible? The ECtHR has recently defined stricter requirements on effective oversight by the supervisory authorities which oversee the cases of restrictions on direct access, especially as concerns their powers to check the legality of the data processing and the restrictions on access, and to communicate the results of their checks to the concerned individuals. The paper then demonstrates that 'indirect access' procedures in three EU Member States – Belgium, France and Germany – are likely to be in breach of the rights provided under Articles 8 and 13 ECHR. Although these procedures are the result of an implementation of EU law (Article 17(3) Directive 2016/680), they restrict the powers of the supervising authorities both with regard to review and subsequent communication about the review to individuals.

CORRESPONDING AUTHOR:
Diana Dimitrova
FIZ Karlsruhe – Leibniz Institute for Information Infrastructures GmbH, Germany; Vrije Universiteit Brussel, LSTS Group, Belgium
diana.dimitrova@fiz-Karlsruhe.de

KEYWORDS:
right of access; independent oversight; human rights; ECHR; law enforcement directive

TO CITE THIS ARTICLE:
Diana Dimitrova and Paul de Hert, 'Real Transparency and Real Oversight of Law Enforcement Data. The ECHR and the Lack of Accountability of Indirect Access Procedures' (2025) 21(1) Utrecht Law Review 49–69. DOI: https://doi.org/10.36633/ulr.905

1 INTRODUCTION: THE CHALLENGES OF STUDYING THE RIGHT OF ACCESS UNDER THE ECHR

As police powers have expanded over the years, including the processing of increasing amounts of personal data, the issue of when and under what conditions individuals can access their own data has become increasingly important. The right of access has been regulated in the EU legal order in the law enforcement field since the entry into force of Directive 2016/680 (Law Enforcement Directive (LED)).[1] By contrast, the right of access to one's data under the European Convention on Human Rights (ECHR) and in the case law of the European Court of Human Rights (ECtHR) has remained more elusive, despite the fact that Convention 108(+), Council of Europe Recommendation (87)15 and the Council of Europe Guidelines on data protection in the police sector clearly include a right of access to one's data.[2]

Although the legal instruments of the Council of Europe 'push' towards transparency and accountability, they remain vague about limitations to access to personal data collected by law enforcement authorities. At the level of EU law, the LED contains two procedures for the exercise of the right of access. First, the 'direct access' procedure contained in Article 14 LED. The individuals can turn directly to the law enforcement body with questions about their personal data. This law enforcement authority ('the controller'), as the direct recipient of the access request from the concerned data subject, is perfectly situated to handle the request and if possible to disclose to the individual all the information provided for in the LED. Secondly, there is the Article 17(3) LED procedure. Here, there is no direct access and no disclosure of data to the individual. Under this 'exceptional' procedure, the controller decides to impose a (partial) restriction on the right of access pursuant to the respective provisions of the LED.[3] The right of access is then replaced by a verification procedure by a data protection authority (DPA) overseeing the law enforcement authorities in a given Member State.[4] This second procedure is commonly, but not quite accurately, referred to as 'indirect access'. In a previous paper, we identified two shortcomings in the implementation laws of France, Belgium and Germany. Contrary to the text and spirit of the LED, these laws severely restrict the powers of the DPAs to conduct a review of the data processing *and* to communicate their findings to the concerned data subjects.[5] We concluded that the discussed implementations are likely to be in breach of the LED and also of the Charter of Fundamental Rights of the EU (CFREU), especially the requirement for independent supervision over the right to data protection in Article 8(3) CFREU.[6] This finding was confirmed by a recent judgement of the European Court of Justice (CJEU) *Ligue des droits humains ASBL, BA v L'organe de contrôle de l'information policière* in relation to the Belgian system of indirect access.[7]

What is lacking in the literature is a human rights accountability-approach complementing the foregoing (EU law-based) analysis. How compatible with human rights is the replacement of the

1 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89, Art 14.

2 Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM (2018) 2 final, 128th Session of the Committee of Ministers (Elsinore, Denmark, 17–18 May 2018), Ad hoc Committee on Data Protection (CAHDATA), (Convention 108+); Council of Europe Committee of Ministers Recommendation No. R (87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, 17 September 1987; Council of Europe, 'Practical Guide on the use of personal data in the police sector', T-PD(2018)01. In the present paper, however, we will not discuss the right of access under these instruments; we will focus on the relevant case law only.

3 LED, Art 15.

4 LED, Art 17(3).

5 Diana Dimitrova & Paul De Hert, 'The LED's right of access to one's data: Loopholes on proper access, legality review and data protection authority Accountability' (2024) 15(1) *New Journal of European Criminal Law,* 12 (hereinafter 'Dimitrova & De Hert 2024A'). The paper also shows why we focused on the three selected EU Member States (Belgium, France and Germany).

6 Diana Dimitrova & Paul De Hert, 'DPA independence and 'indirect' access – illusory in Belgium, France and Germany?' ([2024) 31(1) *Maastricht Journal of European and Comparative Law*, 82 (hereinafter 'Dimitrova and De Hert 2024B').

7 Case C-333/22, *Ligue des droits humains ASBL, BA v L'organe de contrôle de l'information policière* [2023] ECLI:EU:C:2023:874.

DOI: 10.36633/ulr.905

right to directly access one's data by a system of independent oversight by administrative (data protection) authorities? We will study this question in the light of ECtHR case law on the right of access under Article 8 ECHR (private life) and under Article 13 ECHR (effective remedies). This human rights perspective offers instructive guidance on interpreting the powers of the DPAs set up in states in and outside the EU to help citizens protect their data. The ECtHR has a rich and longstanding case law, offering an ad hoc interpretation of the different types of restrictions on transparency and of the powers which (administrative) supervisory authorities should have. As we will demonstrate in the following sections, this case law requires, inter alia, that restrictions on transparency should be accompanied by independent judicial or administrative oversight (analogous to the DPA role under the LED). These authorities need effective powers to review the law enforcement authority's data processing and to communicate their findings to the individuals. In its recent case law the ECtHR has tended to require more accountability to the individual data subjects by the supervisory authorities which examine the restrictions on transparency and the legality of data processing, in contrast to its earlier case law, whose weaknesses we criticise in the sections below.

This paper is structured as follows. First, we will demonstrate that, in the ECtHR case law concerning Articles 8 and 13 ECHR respectively, there is no absolute right for the concerned individual to have access to their data, as there is likewise no absolute right to be notified of the collection of personal data on them (Sections 2-4). We will nonetheless examine the prevailing trends in case law regarding access rights, exercised by individuals upon request, and the notification obligation of the respective data processing authority, wherein data is provided proactively by the controller. Our goal is to extract the transparency rights granted by the ECtHR, specifically identifying the types of information individuals are entitled to know about the processing of their data by law enforcement authorities.

Then, we will demonstrate that the ECtHR has been concerned less with the question as to what information individuals should obtain about the processing of their data than with the question as to whether the restrictions on the right of access and/or notification have been accompanied by appropriate safeguards such as independent oversight. We will argue that there is an evolution in the ECtHR's case law as concerns the potential replacement of transparency rights with a system of independent external supervision, whether via a data protection authority or via other, similar means. We will demonstrate that the earlier case law (e.g. *Leander*) did not question the effectiveness of this safeguard, which we will do (Section 5). The problems with this surrogate safeguard for access are clearly felt in more recent surveillance case law (*Kennedy, Centrum för Rättvisa, Ekimdzhiev II*). The ECtHR is no longer satisfied just with an oversight system, but now looks more attentively at the added value of such a system, its powers to review and make public its findings (Section 6.1). We argue that the ECtHR has indicated that, when oversight authorities check the legality of the data processing and/or of the restriction of the disclosure, they should communicate the outcome of their review to the concerned data subjects. This trend to check the powers of oversight bodies, especially when they are deemed to replace data subject rights like access and notification, is also visible in other areas of case law, especially case law concerning data held by the ex-Communist regimes (e.g. in *Haralambie, Szulc, Tudor*, etc) (Section 6.2).

Having identified the level of accountability required by human rights law with regard to independent (administrative) supervision, the paper turns to existing indirect access procedures as implemented under Article 17(3) LED in certain EU Member States.[8] These restrictions on the right of access are not only problematic in terms of EU law, but also in terms of human rights law (Section 7). Most important in this regard is Belgium's general and indiscriminate refusal to allow direct access and the restricted decision-making powers of the DPAs in terms of disclosure of data to the concerned data subjects and the potential restrictions on effective judicial review in all three Member States. We end with presenting the legal questions posed in a pending case on 'indirect access' raised against France (*Emmanuel Bodinier et 16 autres requêtes*) (Section 8) and a summary of our findings about the human rights problems associated with 'indirect access' as an alternative in many legal systems to direct access (Section 9).

8 For the details on these national laws, see Dimitrova & De Hert 2024A (n 5).

2 THE RIGHT OF ACCESS UNDER ARTICLE 8 (RIGHT TO PRIVACY)

2.1 THE RIGHT OF ACCESS UNDER ARTICLE 8 ECHR: SECTORAL RECOGNITION WITH DIFFERENCES

Access to data fosters transparency, which is a prerequisite for accountability. Notification duties that inform citizens that their data is collected equally contribute to more transparency (see more below, in particular Section 4). As evident from the ECtHR case law, the text of the ECHR provides no explicit and general right of access to one's personal data.[9] As a consequence, there are no substantive or procedural requirements on the right of access to be found in the ECHR. This enters into conflict with the EU legal order, in particular with the General Data Protection Regulation (GDPR) and the LED (detailed provisions), and Article 8(2) CFREU (general recognition of a right to access).[10]

The silence of the ECHR explains why the right to access has remained open to development and definition by the ECtHR. However, it is difficult to discern a pattern as to the cases in which the ECtHR will recognise such a right, especially in the law enforcement field, and as to the acceptable restrictions to it. This could be partially attributed to the fact that Article 8 ECHR has a broad scope of application: it encompasses the law enforcement field, the national security field and areas not covered by either of these fields, e.g. health.

In non-law enforcement or security related sectors, the ECtHR has more directly and explicitly acknowledged a right to access to one's data, e.g. with regard to information on one's childhood, origins or health, or abolished totalitarian regimes.[11] The rationale for recognising this right in specific contexts beyond law enforcement appears to be the acknowledgement of its significance for private life, as safeguarded by Article 8 of the European Convention on Human Rights (ECHR). A prime example is *Gaskin v the UK* (1989).[12]

As concerns information about one's collaboration with former Communist regimes, the ECtHR has created obligations for the respondent Member States to give access to

> all relevant and appropriate information which would allow that party to effectively counter any allegations of his or her collaboration with the security services […] The procedure should equally provide for a possibility to correct any erroneous entries in the relevant files.[13]

9 Lee Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 (3) *International Journal of Law and Information Technology*, 247–284; Paul De Hert, 'Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955–1997' [Human Rights and Data Protection. European Case-Law 1995–1997], in *Jaarboek ICM 1997* (Antwerp: Maklu, 1998), 40–96.

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016,p. 1, Art 15; LED, Arts 14–15; European Union, Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391, Art 8(2).

11 E.g *Gaskin v the United Kingdom*, App. no. 10454/83 [1989] ECtHR*; Yonchev v Bulgaria*, App. no. 12504/09 [2017] ECtHR; *Joanna Szulc v Poland*, App. No. 43932/08 [2012] ECtHR; *Jarnea v Romania*, App. no. 41838/05 [2011] ECtHR; *Rotaru v Romania,* App. no. 28341/95 [2000] ECtHR; *Haralambie v Romania*, App. No. 21737/03 [2009] ECtHR.

12 *Gaskin v the United Kingdom* (n 11). The case concerned the applicant's request for access to the documents concerning his time in foster care as a child with different families, as kept by the Social Services Department of Liverpool City Council (para 12). The case is emblematic, because it seems to be the first acknowledgement of the right of access outside the law enforcement and national security fields. Gaskin requested access in order to learn more about the alleged abuse he had suffered in foster care. However, under the applicable law at the time, if some of the contributors to the report refused to grant their consent for the disclosure of certain documents, then these documents were not subject to disclosure. The applicant claimed that this represented a violation of his private life under Article 8 ECHR. The ECtHR agreed with the applicant and recognized the right of access to the documents in question, because of their importance for the applicant's private life: '… persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their childhood and early development.' (ibid, para 49).

13 *Joanna Szulc v Poland* (n 11), para 87; *Haralambie v Romania* (n 11), , paras 85–86; *Jarnea v Romania* (n 11), para 50. Note that the quoted cases concern access to files compiled by the ex-Communist regimes. See also *Yonchev v Bulgaria* (n 11), concerning access to the psychological assessment of an applicant's fitness to participate in an international police mission (para 53). See also *Roche v the United Kingdom*, App. no. 32555/96 [2005] ECtHR, para 162, concerning information on health risks. Also see *Gaskin v the United Kingdom* (n 11), para 49.

In its case law concerning former Communist regimes and topics such as health and one's childhood, at a procedural level, the ECtHR seems to implicitly favour direct access (meaning access granted by the party holding the data) as the default setting.

By contrast in the law enforcement and national security sectors, the ECtHR has been more hesitant about establishing that a right of access exists per se.[14] When examining a certain case, it has never denied its advantages for the data subject. One learns from the facts of different cases and the ECtHR's reasoning that accessing the information held by law enforcement and security authorities might help to curb misuse of the data, *inter alia* because access enables the data subject to rebut the contested information.[15] It is also seen as a means to 'rectify' the informational asymmetry between the authorities and individuals.[16] To achieve these purposes, the ECtHR has established that the right of access encompasses access to personal data included in law enforcement/secret police database files and the individual data elements included in files. It has also been broadly read to include access to documents, including access to a whole police file.[17]

The ECtHR's acknowledgement of the existence of the right of access to one's data, especially in the national security field, has been implicit rather than explicit, in the sense that it acknowledged that a restriction on access constitutes an interference or was part of the interference with Article 8 ECHR. For example, in *Segerstedt-Wiberg and Others v Sweden* (2006), the ECtHR explicitly acknowledged the restriction on access as a separate interference with Article 8 ECHR.[18] The ECtHR postulated that '[it] [...] finds it established that the impugned refusal to advise the applicants of the full extent to which information was being kept about them on the Security Police register amounted to interference with their right to respect for private life.'[19]

In most other cases, the reasoning has been even more implicit. In these cases, the ECtHR does not always acknowledge the restriction on access as a separate restriction to Article 8 ECHR.[20] *Leander v Sweden* (1987), also one of the older cases on access, concerned the issue of a national security check in the employment context.[21] The ECtHR noted that the refusal to grant access to the applicant's file constituted an element of the interference with Article 8 ECHR,[22] but it did not analyse this refusal separately or as a separate interference.

2.2 THE THIN LINE BETWEEN 'NATIONAL SECURITY' AND 'LAW ENFORCEMENT'

We note that Article 8 ECHR regulates, amongst other things, the grounds for restricting the right to private life as provided for in that same Article, including the disclosure of data to the concerned individual. As evident from Section 2.1, two of these grounds are 'national security' and 'the prevention of disorder or crime' (or law enforcement, in other words).[23] What is also evident is that the ECtHR normally allows Member States a broader margin of appreciation in

14 European Court of Human Rights, 'Guide to the Case-Law of the European Court of Human Rights: Data protection', 31 August 2022 ('ECtHR Guide on data protection'), 60.

15 E.g. *Amann v Switzerland*, App. no. 27798/95 [2000] ECtHR; *Martin v Switzerland*, App. no. 25099/94 [1995] ECtHR.

16 Evelien Brouwer, *Digital Borders and Real Rights Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff, 2008), 201.

17 See the summary of the ECtHR's case law in ECtHR Guide on data protection (n 14), 59–60.

18 *Segerstedt-Wiberg and Others v Sweden*, App. No. 62332/00 [2006] ECtHR. As to the facts of the case, the five applicants – Swedish nationals four of whom were politically active on the left scene and one was a journalist – complained of the lack of (full) access to information stored about them by the Security Police (paras 9–37).

19 ibid, para 99. See also *Martin v Switzerland* (n 15).

20 E.g. *Dalea v France*, App. no. 964/07 [2010] ECtHR; *Leander v Sweden*, App. no. 9248/81 [1987] ECtHR.

21 The check had resulted in the applicant not obtaining his security clearance and the ensuing termination of his employment for that reason.

22 *Leander v Sweden* (n 20), para 48.

23 Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950 (ECHR), Art 8(2).

national security matters as compared to other contexts.[24] We interpret this to mean that if the ECtHR has ruled in individual cases that non-disclosure of information to the concerned individuals constitutes an interference with Article 8 ECHR in the national security field, it can be hardly argued that it does not constitute an interference in the law enforcement field.

The question remains as to how to draw the line between national security and law enforcement for the purposes of establishing trends about the transparency which the ECtHR allows in relation to these two contexts.[25] As observed by other academics, there is no single definition of national security across the different EU Member States and hence the delineation between national security and law enforcement matters is not always straightforward.[26] Amongst the clear-cut distinctions one could cite spying for a foreign government as a national security matter as against the theft of a bag as a law enforcement matter. However, a lot of cases are not so clear-cut. For example, terrorism is considered by EU law (including in the interpretations provided by the Court of Justice of the EU (CJEU))[27] and by the ECtHR to be both a national security and law enforcement concern.[28]

The above discussion bears relevance for our paper in two major aspects: (i) because of the fluid separation between the two concepts, it is reasonable to examine the ECtHR case law on national security matters and transparency and apply it to transparency in law enforcement matters, where possible, bearing in mind the fact that (ii) the ECtHR has established limits on the restrictions on the right of access even in national security cases. This means that a fortiori it might be the case that the ECtHR is even stricter on the restrictions on transparency in cases of (minor) crimes.

3 THE RIGHT OF ACCESS UNDER ARTICLE 13 (RIGHT TO AN EFFECTIVE REMEDY)

As seen from the two Swedish examples, in *Segerstedt-Wiberg* and *Leander* discussed in Section 2.2, as well as from *Gaskin* (see Section 2.1), when the ECtHR acknowledges that a refusal of access constitutes (part of) an interference with Article 8 ECHR, the ECtHR examines whether the respondent Member State provided enough safeguards when imposing restrictions on access to one's data or documents, e.g. whether the refusal was accompanied by legal channels for an independent review or remedy. This examination is sometimes performed directly under Article 8 ECHR[29] or separately under Article 13 ECHR, or both. A prime example of the examination under Article 13 ECHR is *Segerstedt-Wiberg v Sweden*.[30]

---

24 E.g. *Segerstedt-Wiberg and Others v Sweden* (n 18), para 104.

25 National security falls outside the scope of EU law, including the LED (LED, Art 2(3)(a) and 4(2) Treaty on the European Union).

26 Didier Bigo et al, 'National security and secret evidence in legislation and before the courts: exploring the challenges', Study for the LIBE Committee at the European Parliament 2014, PE 509.991, https://www.europarl.europa.eu/RegData/etudes/STUD/2014/509991/IPOL_STU(2014)509991_EN.pdf, see Section 1.6 (last visited 3 March 2025).

27 E.g. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others* [2016] ECLI:EU:C:2016:970, paras 119 and 103.

28 European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence', updated on 31 August 2022, 131.

29 In cases where Article 13 ECHR is not invoked by the claimant or checked by the ECtHR, the notions of 'effectiveness' and 'remedy' are incorporated in one way or another in the ECtHR's analysis of Article 8 ECHR requirements either of 'legality' or 'proportionality'. See Paul De Hert & Gianclaudio Malgieri, 'One European Legal Framework for Surveillance: The ECtHR's Expanded Legality Testing Copied by the CJEU' in Valsamis Mitsilegas & Niovi Vavoula (eds.), *Surveillance and Privacy in the Digital Age. European, Transatlantic and Global Perspectives* (Oxford: Hart, 2021), 255–295.

30 In passing, we also note that an even more explicit right of access to investigatory and evidentiary materials concerning one's (pre-)trial has been acknowledged as a part of the human right to fair trial (Article 6 ECHR), especially as an aspect of the equality of arms between defendants and the prosecution: *Matanovic v Croatia*, App. no. 2742/12 [2017] ECtHR, para 159. However, we note that the LED right of access to one's data is more universal in the sense that it applies to the whole cycle of personal data processing, including before someone is even charged with a crime and before the right to fair trial is at stake. Hence, we decided to examine the right of access to law enforcement materials/data beyond the framework of fair trial and more as a private life aspect. We note that in access cases where Article 13 ECHR is invoked, the issue is whether the contested restrictions on the right to private life under Article 8 ECHR fulfil the requirements of the right to effective remedies under Article 13 ECHR.

As the ECtHR established in *Segerstedt-Wiberg and Others v Sweden*, refusals of access to one's data normally trigger the applicability of the right to effective remedies.[31] When Article 13 ECHR is applicable, it confers on individuals, according to the ECtHR's case law, a right of access to a national authority having competence to examine whether this Convention grievance was justified or not.[32] To perform its examination, this authority should have access to all the necessary information and offer adversarial proceedings, allowing the concerned individual to contest the decisions of the competent (law enforcement) authorities.[33] The authority does not always have to be a judicial authority.[34] What is important are its powers.[35] This distinction between judicial and non-judicial review, remedy or oversight is more than just a trifle. Opening the doors for non-judicial oversight as a way for human rights compliance has triggered many cases.

The cases reveal that the ECtHR has not always required a judicial review of the interferences with the rights protected under Articles 8 and 13 ECHR. This means that, as evidenced by its case law, it has also extensively examined the safeguards provided by administrative authorities such as the DPAs in the EU Member States.[36] These are the same authorities which are entrusted by EU law with carrying out the 'indirect' access procedure under the LED. Thus, the ECtHR case law on the requirements about the powers of these authorities becomes relevant in interpreting the 'indirect' access procedure.[37]

4 NOTIFICATION IN SURVEILLANCE CASES AS A MEANS TO TRANSPARENCY

Notification of (secret) surveillance or processing is, like access, instrumental for transparency towards the concerned individual. As such, it has an important role in data protection laws.[38]

31 *Segerstedt-Wiberg and Others v Sweden* (n 18), para 116: 'the applicants' complaints under Article 8 of the Convention about (…) the refusal to advise them of the full extent to which information on them was being kept may, in accordance with its consistent case-law (…), be regarded as "arguable" grievances attracting the application of Article 13.' See similarly *Leander v Sweden* (n 20), para 79.

32 European Court of Human Rights, 'Guide on Article 13 of the European Convention on Human Rights: Right to an effective remedy' 30 April 2020, 54; Partly Dissenting Opinion of Judge Ryssdal in *Leander v Sweden* (n 18), para 6; *Al-Nashif v Bulgaria*, App. no. 50963/99 [2002] ECtHR, para 137.

33 ECtHR Guide on Article 13 (n 32), 54; *Centrum för Rättvisa v Sweden*, App. no. 35252/08 [2021] ECtHR, para 362. Note that for the effective oversight or review to be performed, the applicant's access to the documents and/or data, which are supposed to be subject to contestation, is presupposed, so that the concerned individual can state their case in court or in front of other (quasi) judicial authorities. A prime example is *Amann v Switzerland* (n 15), where the ECtHR found that the fact that Mr Amann had had access to his file (card) allowed him to exercise his right to an effective remedy in Article 13 ECHR. (*Amann v Switzerland*, para 89). The case concerned police surveillance for security purposes of the telecommunications between the applicant and a member of the Russian diplomatic service. After it became known to the public that the security authorities had been intercepting the telecommunications of many presumably innocent individuals, Mr Amann requested access to his file and was granted partial access to his card. In addition, he was able to challenge the tapping, the creation and storage of the card with the domestic courts, even though the courts did not rule in his favour. Hence, it is not surprising that the ECtHR found that the fact that he had had access to his file (card) allowed him to exercise his right to an effective remedy in Article 13 ECHR.

34 *Segerstedt-Wiberg and Others v Sweden* (n 18), para 117. ECtHR Guide on Article 13 (n 32), 11.

35 Thus, in *Segerstedt-Wiberg and Others v Sweden* (n 18), the ECtHR found it sufficient that the refusal to advise individuals on the data stored about them in the Security Register could be challenged in front the administrative courts in Sweden (*Segerstedt-Wiberg and Others v Sweden*, para 119). On the other hand, it noted that the Swedish system lacked effective remedies against illegally stored data and thus the system overall did not offer effective remedies (ibid, paras 120–122).

36 E.g. *Ekimdzhiev and Others v Bulgaria*, App. no. 70078/12 [2022] ECHR (Ekimdzhiev II v Bulgaria), paras 198–204, 225–226, 346, 386, 410–412.

37 In recent judgements we see an increasing emphasis on the real added value of oversight in terms of powers and competences, regardless of the authorities performing it. We will discuss these below with regard to non-judicial oversight and apply it specifically to the EU DPAs, but we note in passing that the same trend is also present in the ECtHR's approach to judicial oversight. We will demonstrate that it is not sufficient to have a system of oversight, what is needed is a system of oversight (judicial, quasi-judicial, hybrid) that can provide an effective control of law enforcement and security authorities, supported by empirical checks in the national legal system at issue.

38 One of the elements of the right of access under the LED is a confirmation whether the data of the requesting individual are being or have been processed. Thus, the notification can be seen as a confirmation that the personal data of the concerned individual have been processed. Whereas the notification is supposed to be provided proactively by the authorities, without the individual having requested it, by contrast to the right of access, it is still the case that both convey partially the same information, namely an indication that data processing has taken place, with the right of access providing a further set of details: see Dimitrova and De Hert 2024A (n 5). Note how the ECtHR recently made a link between the notification in a secret surveillance context and the rights of information and access to one's data as transposed from the LED into Bulgarian national law in *Ekimdzhiev II v Bulgaria* (n 36), para 350.

Notification is a key guarantee, in particular in cases where governments or others engage in secret surveillance unknown to the citizen concerned. Notification, when possible, can then restore the balance. Both concepts—access and notification—are related: after notification the informed citizen can engage in an access request to know more about the data collected by others. It is not surprising to learn that the ECtHR case law on notification provides additional useful insights relevant to understanding the ECtHR's approach to the right of access to one's data.

Like access, notification is also lacking in the text of the ECHR, but it is sometimes recognised as an element or sub-right under Article 8 ECHR, similar to the right of access to one's data. The ECtHR case law does not always clearly distinguish between the right of access to one's data and/or files and the right to notification of surveillance. This could be partially explained by the fact that neither of them is officially recognised as a full (sub-) right under the ECHR.[39] Normally, it is understood that notification refers to the authorities proactively informing the concerned individuals that they have been subject to (secret) surveillance. The right of access, by contrast, refers to the individual requesting the authorities, be it national security or law enforcement ones, what information they have been processing in relation to them.[40]

The ECtHR normally accepts that the question of notification falls within the protection granted by Article 8 ECHR. At the same time, the ECtHR has consistently established that not notifying (all) individuals of (secret) surveillance does not automatically amount to a breach of the ECHR, as long as the concerned individuals may seek effective remedies against the surveillance without needing to prove that they have been surveilled, i.e. without the information provided by the notification. Hence, the ECtHR found little issue with the surveillance regimes in Germany in *Klass and Others v Germany* (1978)[41] and *Weber and Saravia* (2006)[42] or, in the UK, in *Kennedy v the United Kingdom* (2010),[43] but criticized the very limited or absent notification requirements under Russian and Hungarian laws, which prevented the concerned individuals from seeking (judicial) remedies in *Zakharov* (2015) and *Szabo and Vissy* (2016).[44]

These judgements demonstrate that transparency, in contrast to the right to effective remedies, is less of a concern for the ECtHR where national security is at stake. However, the ECtHR rarely accepts that the complete absence of notification even in national security cases could be compatible with the ECHR.[45] There is a development under way. Recently, individual

39 See, by contrast, the CJEU in C-350/21 *Spetsializirana prokuratura* [2022] ECLI:EU:C:2022:896, paras 68–76, where the requirement of notification is clearly linked by the CJEU to the right to information under Article 13 LED (and the right to effective remedies in Article 54 LED).

40 Thus, it can be argued that the right of access includes the information provided by notification, but also goes beyond it, as regulated by the applicable laws.

41 *Klass v. Germany*, App. no. 5029/71 [1978] ECHR.

42 *Weber and Saravia v Germany*, App. no. 54934/00 [2006] ECtHR, para 136.

43 *Kennedy v the United Kingdom*, App. no. 26839/05 [2010] ECtHR.

44 *Zakharov v Russia*, App. no. 47143/06 [2015] ECtHR, para 302: '[t]he effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.'; *Szabo and Vissy v Hungary, App. No. 37138/14* [2016] (ECtHR), para 36 (see the quoted case law there). The ECtHR deemed that the restrictions on notification were even more problematic in *Szabo and Vissy*, because the individuals could not receive any notification at any point (*Szabo and Vissy v Hungary*, para 86 ff), i.e. the restriction was absolute and individuals could not pursue any remedies. The rulings in *Zakharov* and *Szabo and Vissy* resonate also with the earlier case law in *Ekimdzhiev I, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* App. No. 62540/00 [2007] (ECtHR) and *Popescu v Romania*, App. no. 71525/01 [2007] (ECtHR), where the ECtHR found a violation of the ECHR, because the authorities did not provide any notification at any point, there was no possibility to seek remedies and thus no effective safeguards against abuse (see the brief summary in *Zakharov v Russia*, para 288).

45 *Malone v the United Kingdom*, App. no. 8691/79 [1984] ECtHR. The case dealt with the interception of phone conversations in which the applicant took part, on the basis of a judicial warrant in order to investigate a crime. In its ruling, the ECtHR barely touched upon the issue of the right of access to one's data by one of the suspects (Mr Malone). 'The requirement of judicial control over telephone interceptions does not flow solely from a concern rooted in a philosophy of power and institutions but also from the necessities of protecting private life. In reality, even justified and properly controlled telephone interceptions call for counter-measures such as the right of access by the subject of the interception when the judicial phase has terminated in the discharge or acquittal of the accused, the right to erasure of the data obtained, the right of restitution of the tapes' (Judge Pettiti's Dissenting Opinion in *Malone v the United Kingdom*). *A fortiori*, it could be argued that the ECtHR would be even more critical of the absolute restrictions on transparency in cases of minor crimes. As concerns the duration of the restrictions, the ECtHR acknowledges that national security requires more secrecy, even after surveillance is over. However, we note that it is commonly accepted that investigations into petty crime, which moreover end with the suspected and charged individuals being found innocent at the end, require less secrecy and thus more transparency, especially via the right of access to one's data, and thus the right of access might be justified.

DOI: 10.36633/ulr.905

ECtHR judges have begun emphasising that notification in the national security/intelligence sector should be provided whenever it would not jeopardise the fulfilment of the legitimate purposes behind the interception, even where individuals may exercise their right to effective remedies without such a notification.[46]

Further to enabling the right to effective remedies, notification has an additional function: to enhance the accountability of the national security agencies. In 2015, the Council of Europe Venice Commission, in a report on the oversight of signal intelligence agencies, paid special attention to the role of the supervisory authorities in controlling the refusals to notify those individuals who had been subject to this type of surveillance. Its approach demonstrates the importance of notifications and its understanding of the reality that national security, and in our opinion also law enforcement, authorities might abusively neglect their notification duties. Referring to the German legal system, where an external oversight body (the G 10 Commission) approves each non-notification of surveillance by the surveillance authorities to the concerned individual, the Venice Commission pointed out that such an independent oversight mechanism can be an essential safeguard in the framework of (secret) surveillance and identifies a new purpose to the notification system:

> Thus the notification requirement, even if it only rarely leads to actual notification, can still serve a useful function in curbing overuse, because the strategic surveillance agency knows that every time the content of the communications of a citizen or resident has been monitored, it must inform the oversight body of this *and convince it that its reasons for not subsequently notifying the person are justified*.[47]

Thus, a notification or access requirement, even when turned down by security or law enforcement authorities, still makes sense as a safeguard: in principle when it is elaborated in the right way (so that it forces these authorities to justify their decision to the oversight body), it has the advantage of making the security authorities more accountable towards the supervisory authorities and indirectly towards the citizens, when imposing restrictions.

This short discussion of the notification case law of the ECtHR, joined to Section 2 on access to law enforcement data, allows us a brief intermediate conclusion: despite the fact that the ECtHR has not established the rights of access and notification as self-standing rights, it has made it clear that unconditional restrictions on them are not compatible with Articles 8 and 13 ECHR and that where notification can be provided without jeopardising the concerned national security interest, it should ideally be provided.

5 INDEPENDENT OVERSIGHT INSTEAD OF ACCESS (OR NOTIFICATION): A CRITIQUE

5.1 THE UNASKED QUESTION RAISED BY THE TRUTH BEHIND *LEANDER*

In the case law discussed so far, the ECtHR has consistently established a requirement which influenced the rules on the right of access under the LED: restrictions on transparency, be it in the form of notification or the right of access, should be accompanied by the safeguard

46 Thus, in *Big Brother Watch*, Judge Albuquerque noted in his Partly Concurring and Partly Dissenting Opinion that: ‘Finally, *ex post* review of the use made of an interception order should also be triggered by notification to the targeted person. When nothing hinders the notification of the person whose communications have been intercepted, it would allow him or her to contest in a fair and adversarial judicial procedure the grounds for such interception. It is therefore highly speculative, to say the least, to pretend that a system which does not depend on notification of the intercept subject “may even offer better guarantees of a proper procedure than a system based on notification”. No one cares more for the interests of the intercept subject than the subject himself or herself’ (*Big Brother Watch and Others v the United Kingdom*, App. nos. 58170/13, 62322/14, 24960/15 [2021] ECtHR, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, para 27).

47 European Commission for Democracy through Law (Venice Commission), ‘Report on the Democratic Oversight of Signals Intelligence Agencies’, Study No. 719/2013, Strasbourg, 15 December 2015, 35 (emphasis added).

of independent oversight or even replaced by it in order to be compliant with the ECHR.[48] For example, in *Leander*, the ECtHR concluded that, all in all, the non-disclosure of the file to Mr Leander constituted a proportionate restriction to Article 8 ECHR, in particular because of the system of review and oversight which, according to the ECtHR, offered adequate remedies.[49]

This approach is not without risks. The ECtHR has sometimes been very superficial in examining the effectiveness and independence of the administrative supervisory authorities in its jurisprudence. We therefore question whether relying on supervisory bodies can be an adequate substitute for the direct right of access of the concerned individuals to the information (and documents) concerning themselves.

Illustrative for the effectiveness of the Swedish oversight system is *Leander* (1987) or, better, what we learned after *Leander*. Reportedly, a decade after the ruling, the Swedish Government 'admitted that their case at the European Court for Human Rights had been based on false information' and 'publicly declared that Leander was not and never had been a security risk',[50] in other words his registration and the associated data processing was illegal. More precisely, it was based on the expression of his political views as a teenager and treating people as a security threat for their political views was illegal under the Swedish Constitution.[51]

And here comes a hypothetical question: had the Swedish Government in 1987 been honest with the ECtHR, would the ECtHR have ruled otherwise and acknowledged the importance of access to one's file, either directly or through a security-cleared lawyer? The more disturbing question is: since the Government had engaged in illegal data processing, which was relatively straightforward and in practice not so difficult to detect, how had the oversight institutions not detected this abuse, and most importantly was the ECtHR wrong to conclude that the external control was really effective and independent *in casu*? Because if this is the case, then there is doubt as to whether effective supervision should be an unconditional alternative to an access right in principle, especially as a default procedure in law enforcement, and it can be questioned whether, in view of the risks, individuals should not have a vital interest in obtaining access to their file.

The circumstances of *Leander* do raise the question why the *Leander*-rule (non-access to the citizen can be remedied through a good oversight system) has been followed by the ECtHR in subsequent judgments. The reference to the *Leander* rule became so superficial that, at a certain point, the effectiveness and powers of the administrative supervisory authorities were not really examined.[52]

48 As noted by Sajfert and Quintel, this requirement influenced the design of the 'indirect access' procedure through the participation of the DPAs in the LED. See Juraj Sajfert & Teresa Quintel, 'Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873 (last visited 3 March 2025). This requirement was established as early as *Klass v Germany* (n 41), para 58; *Weber and Saravia* (n 42), para 136 and *Zakharov v Russia* (n 44), para 288. Non-disclosure should be an option only in exceptional cases, which are subject to independent judicial oversight and the concerned party should be represented by a lawyer (Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque in *Big Brother Watch* (n 46), para 28).

49 *Leander v Sweden* (n 20), paras. 67 and 78. *In casu*, the ECtHR paid special attention to the existence of 'National Police Board and to the supervision effected by the Chancellor of Justice and the Parliamentary Ombudsman as well as the Parliamentary Committee on Justice' (para 65). See similarly in *Segerstedt-Wiberg and Others v Sweden* (n 18). From the facts of *Segerstedt-Wiberg and Others v Sweden*, it becomes evident that these safeguards referred, inter alia, to a system of review of the legality of the data storage which includes a Data Inspection Board, the Records Board, the Parliamentary Ombudsperson and the Chancellor of Justice (paras 100–104).

50 Dennis Töllborg, 'Intelligent Suicide?', Gothenburg Research Institute, GRI-rapport 2008:5, 12. The Government had to apologize and pay Mr Leander damages.

51 ibid.

52 *Martin v Switzerland*, App. no. 25099/94, admissibility decision of 5 April 1995. It concerned a British journalist who was surveilled by the Swiss security and intelligence authorities when he was working in Switzerland. He requested access to his file under Article 8 ECHR, which was turned down and the Swiss safeguard system was considered to be sufficient because of the existence of administrative oversight bodies. In view of the situation with Mr Leander, it cannot be automatically presumed that, because these remedial instances existed, they managed to effectively detect and curtail potential abuse. Also in *Amann v Switzerland* (n 15), the ECtHR did not examine critically whether the Swiss courts had examined in detail the legality of this partial restriction. Thus, the effectiveness of the remedies, ensured through external judicial oversight, was not really questioned. This lack of examination of the safeguards' real value is also present in *Segerstedt-Wiberg and Others v Sweden*. When examining the complaints under Article 8 ECHR regarding the non-disclosure of information to the concerned data subject and the powers of the independent oversight authorities under Article 8(2) ECHR, the ECtHR did not explain how and why they were effective in relation to the refusal to grant full access to the concerned individuals to their files (*Segerstedt-Wiberg and Others v Sweden* (n 18), paras 100–104). Its examination of the effectiveness of the administrative courts which can deal with complaints about the refusal of access under Article 13 ECHR was also rather superficial (ibid, para 119).

5.2 *LEANDER'S* DÉJÀ VU AND THE POWERS OF THE FRENCH DATA PROTECTION SUPERVISORY AUTHORITY (CNIL)

This lack of profound scrutiny of powers and effectiveness of oversight bodies can be illustrated with *Dalea v France* (2010).[53] The applicant, a Romanian citizen, was refused a Schengen visa by France.[54] The ECtHR emphasized the presence of independent review in the French legal system, which was available through the indirect access procedure via the CNIL, as a safeguard in relation to the existence of the Schengen Information System (SIS) alert. In the ECtHR's own reasoning, such a review should offer the opportunity to the individual to refute the information processed by the authorities.

It is, however, unclear how the applicant could have realistically rebutted the information where no sufficient information was disclosed, *in casu* no information on the national security reasons for the inclusion in the SIS alert.[55] The ECtHR acknowledged that the CNIL had indicated that the security authorities had not disclosed the content of the file even to the CNIL, but did not explore the matter further.[56]

Dalea is interesting for two reasons: (i) the matter concerned the SIS, a system regulated by EU law in order to enhance the criminal law cooperation between the Member States, which in principle does not regulate national security matters as we mentioned in Section 2(2) above, but where nevertheless the EU Member States may enter alerts in relation to national security matters. This perfectly exemplifies the blurring of law enforcement and national security matters and the difficulty in delineating the transparency standards between the two; and (ii) *in casu*, the refusal to issue a Schengen visa could be treated as an implicit notification about an existing SIS alert, inviting Mr Dalea to exercise his right to administrative and/or judicial remedies. However, the case shows that this proved to be difficult without having access to the further information concerning the alert in the sense that Mr Dalea (and presumably his lawyers) could not refute the information contained in the alert by engaging in adversarial proceedings.

5.3 THE WEAKNESSES OF JUDICIAL REVIEW WHEN ADMINISTRATIVE REVIEW IS RESTRICTED

In this subsection we will briefly dwell on the question raised by our analysis of Dalea, namely whether judicial oversight, especially in cases of insufficient administrative oversight, is an adequate guarantee to protect the affected human right, in this case the right to private life. The problems of judicial oversight when information is not disclosed to the concerned data subjects are evident from the Regner v the Czech Republic ruling, concerning the lack of access to the reasons for the applicant's withdrawal of his security clearance, which was examined under the right to fair trial (Article 6 ECHR). The ruling itself had only a wafer-thin majority and gave rise to many dissenting and concurring Opinions, in which individual judges astutely raised the following points.

---

53 *Dalea v France*, information taken from the press release for the admissibility decision (Information Note on the ECtHR's case-law No. 127, February 2010). We note that the case was declared inadmissible.

54 He had been informed that this was because of an entry into the Schengen Information System (SIS) on national security grounds. Amongst the complaints submitted to the ECtHR on the basis of Article 8 ECHR, the applicant claimed that he had been refused access to the precise grounds for the SIS entry and had had access only to the factual data entered, e.g. his name.

55 'In particular, it must have the possibility of having the disputed measure reviewed by an independent and impartial body […]. Before this control body, the person concerned must benefit from an adversarial procedure in order to be able to present his point of view and refute the arguments of the authorities.' *Dalea v France*, Press release (n 53).

56 The ECtHR did not go into the question of whether the French 'indirect access' procedure guaranteed proper legality control, because of the limited access to the file which the CNIL as a supervisory authority had, and whether the CNIL could independently fulfil its role as an oversight authority. It also remains unclear why the CNIL could not make its decision on non-disclosure independently from the security authorities and demonstrate why and how it had reached its conclusions. This leaves the question open as to what powers of the data protection supervisory authorities the ECtHR is ready to accept as offering adequate safeguards and whether it is ready to accept deficiencies in their independence and effectiveness *as long as* there is judicial redress. The ECtHR apparently seemed to find a compensation for this state of affairs in the fact that the contested file could be transferred directly to the Council of State for judicial review (which was presumably done *in casu*) and that the Council of State concluded that the CNIL was right not to order the rectification or deletion of the data, meaning that proper judicial review seems to have been offered *in casu*.

DOI: 10.36633/ulr.905

Several judges argued that it is not the courts' role to be the individual's advocate and that if individuals do not have access to their data, then the courts might be misled by the security authorities which are in control of the information presented to the courts, whereas individuals cannot refute it.[57] In other words, the courts cannot act independently. As another judge noted, the courts are not independent when they act in the interest of the parties to only one side of the dispute, that is when they either perform reviews on behalf of the applicant or base their judgement only on the information provided by one party.[58] Even in the only Concurring Opinion, Judge Wojtyczek noted that 'certain forms of "inequality of arms" cannot be offset in this way [through 'the active role of the courts'].'[59]

This somehow challenges the established case law that as long as an independent authority exists for examining the refusal to grant access (be it an administrative or judicial one), then the individual has had access to effective remedies granted by an independent authority.[60] The observations on the role of the courts also raise questions as to whether indirect access procedures, where the DPAs may be more influenced by the law enforcement authorities, offer the opportunity for independent legality control. It remains to be seen whether these observations will be taken up by the majority of the ECtHR.

Based on the critical voices inside the ECtHR which reasonably question whether oversight should in principle replace direct access, even in national security cases, we argue that it might be problematic when a specific law enforcement legal system is based on an absolute ban on access and relies entirely on some version of external oversight as a safeguard, without proper powers to review and to give publicity to the findings to the concerned individuals.

6 ECtHR TOUGHER ON OVERSIGHT OVER NON-DISCLOSURES OF PERSONAL DATA

6.1 A SHIFT IN TOLERANCE TOWARDS STATE RELIANCE ON ADMINISTRATIVE OVERSIGHT SOLUTIONS

This subsection examines, in particular, the judgment in *Centrum för Rättvisa v Sweden*, which suggests that supervisory authorities should be more accountable to the concerned individuals about their findings on the legality of the restrictions on one's right to access and on the legality of the data processing by the national security or law enforcement authorities. A human rights-compatible system of administrative oversight is twofold: powers to review need to be complemented with powers to communicate about the review. Only then can the ideal of accountability towards citizens become a reality and indirect access legitimately be presented as an almost as good alternative to direct access.

The ECtHR, in *Centrum för Rättvisa v Sweden* ('*CFR*') (2021) – a case on the Swedish secret surveillance system – highlighted that individuals in Sweden could apply to an oversight body (the 'supervisory authority', or 'FII'), asking it to examine the legality of the processing of personal data concerning them and carry out, when needed, the necessary rectifying

57 Joint Partly Dissenting Opinion of Judges Raimondi, Sicilianos, Spano, Ravarani and Pastor Vilanova in *Regner v the Czech Republic*, App. No. 35289/11 [2017] ECtHR. The case was examined under Article 6(1) ECHR.

58 'A judge who has knowledge of evidence adduced by one party without the other party having knowledge of it and who bases his or her decision on that evidence and yet does not refer to it in the judgment cannot be considered to be objectively independent. A judge must refrain from any conflict between the parties and not give the impression that he or she is associated in any way with the subject matter or with one of the parties, even if his or her intention is to protect that party.

By leaning towards one or other side in these circumstances, any appearance of independence and impartiality of the domestic courts can be diminished or swept away: The domestic courts leaned (a) towards the side of the executive – since (i) they based their judgment on evidence provided by the Government which was detrimental to the applicant, without ever revealing that evidence to him, and (ii) deprived him of his right to equality of arms and to adversarial proceedings – and (b) towards the side of the applicant since they assumed the role of his advocate, although they left him in the dark as regards the circumstances of the case.' (Partly Dissenting Opinion of Judge Serghides in *Regner v the Czech Republic* (n 57), paras 108–109).

59 Concurring Opinion of Judge Wojtyczek in *Regner v the Czech Republic* (n 57), para 4, last subparagraph.

60 Similarly, Malgieri & De Hert have critically analysed the quality of judicial review and that it is not a 'panacea', e.g. because of the doubts on whether judges can act independently, whether their reviews can be really effective, and whether they are accountable in Gianclaudio Malgieri & Paul De Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but not Necessarily by Judges' in David Gray & Stephen Henderson (eds.), *The Cambridge Handbook of Surveillance Law* (New York: Cambridge University Press, 2017), 509–532.

measures. However, the concerned individuals were neither informed by the FII as to whether an interception had taken place, nor given a reasoned decision by the FII about whether infringements had been established.

The ECtHR was clearly not convinced by this state of affairs,[61] and made an interesting connection between this lack of transparency towards the individual by the oversight body and the overall effectiveness of the oversight body. The ECtHR pointed out that the supervisory authority might not always be encouraged to effectively check the legality of the processing, e.g. mistakes might be overlooked if the supervising authority is not required to be transparent about them.[62]

Further, the ECtHR ruled that reasoned opinions, including opinions on why data indeed may not be disclosed or why there is a finding of infringement of the legality of processing, might also have wider societal benefits:

> A reasoned decision has the undeniable advantage of providing publicly available guidance on the interpretation of the applicable legal rules, the limits to be observed and the manner in which the public interest and individual rights are to be balanced in the specific context of bulk interception of communications.[63]

Thus, the publicity of the supervisory authorities' findings could not only increase the effectiveness of the oversight system, but also increase the legal certainty, accessibility and foreseeability of the legal rules and contribute to the democratic debate on the work of the law enforcement and national security authorities, in addition to a more thorough control over the restrictions and transparency towards the individual concerned.

When discussing these advantages of making the reasoned opinions public in *Centrum för Rättvisa*, the ECtHR referred to its similar reasoning in *Kennedy v the United Kingdom* (2010). In that case the ECtHR had examined the powers of the Investigatory Powers Tribunal (IPT), a (quasi) judicial authority under British law.[64] The ECtHR positively noted, as a positive, that under British law the courts could decide to disclose 'information regarding the findings of fact in his case' where they deemed that no risk for national security exists.[65] This implies that the ECtHR assesses it as positive that the available remedies could result in disclosure to the data subject, including by informing the data subject about the findings of illegality of the processing of their data.

By contrast to *Kennedy*, the oversight body in *Centrum för Rättvisa* was a non-judicial supervisory authority (Inspectorate), which is mentioned alongside the Data Protection Supervisory Authority.[66] The combined approach of the ECtHR in *Centrum för Rättvisa* and *Kennedy* could signal that the ECtHR might be starting to impose higher standards on such supervisory

---

61 'With regard to the Swedish system, the Court notes that no details are communicated to the complainant as to the content and outcome of the investigation conducted by the Inspectorate and, hence, the Inspectorate seems to be afforded wide discretion' (*Centrum för Rättvisa v Sweden*, para 361). *Centrum för Rättvisa v Sweden*, App. No. 35252/08 [2012] ECtHR, paras 356–364. The concern was echoed in Judge Albuquerque's Concurring Opinion (para 17) and in his Partly Dissenting and Partly Concurring Opinion in *Big Brother Watch* (n 46), para 47. In addition, in *Centrum för Rättvisa v Sweden,* the ECtHR pointed out that the FII was not independent, because it was responsible for authorising the activities of the secret surveillance authorities and for supervising these activities. The ECtHR noted that, because of its dual role, the FII might have conflicts of interest when examining individual applications: 'It cannot be excluded that the dual role of the Inspectorate may generate conflicts of interest and, therefore, the temptation to overlook an omission or misconduct in order to avoid criticism or other consequences.' (ibid, para 359).

62 'In the conditions of secrecy, which legitimately characterise the relevant procedures, and failing a legal obligation for the Inspectorate to provide reasons to the individual concerned, there may be doubts as to whether the Inspectorate's examination of individual complaints in such situations affords adequate guarantees of objectivity and thoroughness' (ibid, para 359). The concerned individuals in Sweden may only be informed that an investigation (presumably a check or review) has taken place. This is exacerbated by the dual role of the Inspectorate as a supervisory and monitoring body, which may authorise certain operations of the surveillance authorities, and as an authority which should handle individual complaints, which might concern an activity authorized by the Inspectorate itself (ibid). See also Concurring Opinion of Judge Pinto De Albuquerque in *Big Brother Watch* (n 46), paras 16–19.

63 *Centrum för Rättvisa v Sweden* (n 63), para 361.

64 On that, see especially *Kennedy v the United Kingdom* (n 43), para 76.

65 ibid, para 189.

66 *Centrum för Rättvista v Sweden* (n 63), para 217. Further, '…the Court is satisfied that the Inspectorate's role is that of an independent control mechanism.' (ibid, para 346).

DOI: 10.36633/ulr.905

authorities and might expect them to perform like courts or other judicial authorities with their powers to review and render public the results of their review.[67] This approach suggests that non-judicial bodies that serve as oversight bodies need to be entrusted with powers to motivate and publish their decisions, even in the national security context. It remains to be seen whether this trend will continue. If this would become the case, then it would make it difficult to defend a system of 'indirect access', as we know it in the LED and data protection laws in Member States that do not allow any disclosure to any individual in any case by the supervisory authorities, even where it concerns a minor crime of a person not even charged with a crime.

New case law suggests that this trend, that started with *Centrum för Rättvisa v Sweden*, namely to look critically at the powers of non-judicial oversight mechanism,s is being continued. In *Ekimdzhiev II* (2022), concerning Bulgarian secret surveillance measures and their oversight mechanism, the ECtHR mentioned that one of the criteria for assessing the effectiveness of the supervisory authorities is 'the possibility of effective public scrutiny of those authorities' work'.[68] However, it did not specify what this public scrutiny means *in casu*, i.e. whether it involves the publication of its decisions where it found a violation of the lawfulness of a surveillance measure in a certain case and the refusal of the authorities to provide information to the concerned individuals. It did, however, pay attention to the number of actual notifications ordered by the supervisory authority and concluded that they were far too few, especially in comparison to the number of applications for access.[69]

This requirement that governments have to demonstrate the effectiveness of the oversight measures was already mentioned in *Zakharov* and *Szabo and Vissy*,[70] although even after *Ekimdzhiev II* it is still not clear what the ECtHR means with effectiveness in this context, e.g. does it also mean the opportunity for the supervisory authority to independently decide to disclose information to the concerned data subjects?

By way of a short conclusion, we would bring to mind the fact that the above powers of the administrative supervisory authorities were discussed in the framework of the notification of secret surveillance for national security purposes. We note that the notification 'only' reveals that a surveillance measure has taken place and hence keeping it secret might be essential for national security. By contrast, the right of access to one's data in the criminal law context is often requested once individuals are aware that their data have been processed for law enforcement purposes, for instance because charges have been raised against a certain individual who wants to have more details about the collected information. Depending on each individual case, providing the further information might or might not be critical for the effectiveness of the investigations and it could be argued that some cases might warrant more transparency about the data processing and the findings of the legality of the processing. It is exactly in examining the right balance in each individual case that the independent oversight authorities are needed and need to have effective powers.

6.2 CASE LAW ON COMMUNIST FILES (*HARALAMBIE, JARNEA, TUDOR* AND *SZULC*)

The importance of independent decision-making over the disclosure or restrictions on disclosure of information to the concerned data subjects was also pointed out by the ECtHR in a somewhat different context, namely access to one's file compiled by the former Communist regimes. Even though these were not designed to be remedial and supervisory authorities like the Member State DPAs under the LED, some of the points raised by the ECtHR in that context could also be relevant for these DPAs.

67 In *Centrum för Rättvisa v Sweden* (n 63) the ECtHR treated the problem of the transparency of the supervisory authority towards the concerned individuals and society at large only as one of the shortcomings of the Swedish system in the framework of Article 8 ECHR. Thus, it is not clear at which point the lack of transparency of the supervisory authority decisions could as such result in a violation of Article 8 ECHR or, in other words, what exactly justifies it and makes it proportionate. (ibid, para 364).

68 *Ekimdzhiev II v Bulgaria* (n 36), para 334.

69 ibid, paras 267 and 349. If criminal charges are raised against someone, then they are notified of the surveillance they had been subject to (ibid, para 266).

70 *Szabo and Vissy* (n 44), para 88; *Zakharov* (n 44), para 284. See Malgieri and De Hert (n 60).

As to the Romanian regime on disclosure of the Communist files, the ECtHR in *Haralambie* (2009), *Jarnea* (2012) and *Antoneta Tudor* (2013) indirectly criticized the lack of independence of the authority (National Council for the Study of the Archives of the *Securitate* (CNSAS)) tasked with providing access to individuals to their files. Since the files were initially held by the Security and Defence Ministries, these were supposed to provide the CNSAS with the requested files, which would then provide the concerned citizen access to these files. In practice, the security authorities would not always disclose the requested files to the CNSAS on time, which could then not fulfil its transparency obligations.[71]

The supervisory authority's need for unrestricted access to the information it supervises is essential for fulfilling its tasks effectively. This requirement has been emphasized by the ECtHR, particularly in the context of national security.[72]

In addition, in relation to the Romanian regime, the ECtHR criticized the fact that the affected individuals could not take the security services, *in casu* the Defence Ministry, to court for not disclosing the files to the CNSAS, as the Defence Ministry lacked standing in court under the applicable Romanian law.[73]

(Indirect) influence over the decision-making concerning information disclosure is another issue, as evident in *Szulc v Poland* (2012), about the Polish authorities' refusal, for more than ten years, to grant a woman – who denied any collaboration with the security services during the communist era – access to all documents about her collected by those services. The ECtHR held that the new post-communist regime had failed to put in place an effective procedure whereby interested parties could obtain access to security service documents concerning themselves.

The ECtHR observed that the abolished authoritarian regime in Poland had categorized the concerned persons into collaborator, informant, etc.[74] The oversight body (the Polish Institute of National Remembrance) responsible for examining access requests to the files had automatically taken over these classifications with the restrictions on access defined by the former regime.[75] Clearly the oversight body could not or did not want to decide independently on the restrictions.[76]

These judgments with regard to access by the concerned citizens to files compiled by the abolished Communist regimes confirm the new trend with regard to oversight as discussed in subsection 6.1 on surveillance case law: the ECtHR only accepts the guarantee of having an oversight body when certain minimum requirements are met with regard to their review powers, and their obligations with regards to the publicity of the outcome of their review, bringing to mind the requirement for independence of Member State DPAs.

7 A CRITICAL LOOK AT BELGIAN, FRENCH AND GERMAN INDIRECT ACCESS PROCEDURES

Let us now return to EU law and the three Member State laws which we examined in our two previous papers, as referred to at the beginning of the present paper. We argue that examining these against the background of the ECtHR is an important exercise, despite the fact that the three laws are the result of the implementation of the EU LED. *De jure*, challenges about the LED and the implementation laws should be raised before the CJEU with its powers to review

71 *Haralambie v Romania* (n 11), para 95; *Jarnea v Romania* (n 11), para 56; *Antoneta Tudor v Romania*, App. No. 23445/04 [2013] ECtHR, paras 35–6.

72 See *Hüttl v Hungary*, App. No. 58032/16 [2022] ECtHR concerning the framework of supervision over the application of national security measures which involve the processing of personal data.

73 *Jarnea v Romania* (n 11), para 58; *Antoneta Tudor v Romania* (n 71), para. 38; *Haralambie v Romania* (n 11), paras 41–43. These constituted elements of the violation of the State's positive obligation under Article 8 ECHR (*Haralambie v Romania*, para 96; *Jarnea v Romania*, para 60). This is without prejudice to the fact that, in addition, the CNSAS did not always disclose files on time even if it was in possession of the said files.

74 Only the information concerning specific categories of persons could be disclosed to the concerned individuals.

75 'Certain practices of the Institute, such as the reliance on the classifications adopted by the totalitarian security services, were disapproved by the Constitutional Court …'. (*Joanna Szulc v Romania* (n 11), para 93).

76 This was one of the grounds on the basis of which the ECtHR found a violation of the positive obligations of the State under Article 8 ECHR (ibid, para 94).

DOI: 10.36633/ulr.905

implementing acts, but this does not exclude a subsequent procedure before the ECtHR, i.e. after the CJEU has given its preliminary ruling on the subject matter and the highest national court has rendered a final judgement.[77] An individual who is not satisfied with such a ruling and who strives for more transparency by a certain DPA, could challenge the DPA's refusal to grant them access to their data based on the Member State LED implementing law, in front of the ECtHR,[78] which could result in damages being paid to the applicant. Thus, in this section we will apply the above case law on the restrictions, to the powers of the DPAs in Belgium, France and Germany to conduct their legality review and communicate their findings to the concerned data subjects under the Article 17(3) LED 'indirect access' procedure, which, as we argued in our earlier work, has been envisaged to be the exception under the LED, the default procedure being direct access as directly provided by the law enforcement authority to the requesting data subject.

In Belgium, the legal system is based on a general ban on direct access to personal data processed by the police. This ban applies to the disclosure both by the police authorities and by the supervisory data protection authority ('COC').[79] In effect, the COC may not disclose any data to the requesting data subjects, nor even confirm that the data of the individual are being processed. The direct access procedure is simply non-existent and automatically replaced by the possibility of turning to the COC. This 'indirect access' procedure is formally supposed to fulfil the ECtHR requirement of independent oversight. However, we argue that this is not quite the case. Indeed, the ECtHR 'approved' a system in which direct access is replaced by independent oversight. However, it did so in particular in the national security context, whereas the implementing law in Belgium makes no distinction between national security matters and more trivial police matters. In addition, the law does not allow a distinction to be made between the individual cases, in the sense that it does not require an assessment to be performed on the individual risk posed by the potential disclosure of the personal data of a specific individual, e.g. in the context of minor crimes or of acquitted individuals.

On a related matter, the ECtHR 'gave the green light' to the replacement by independent oversight especially when it comes to notification (of secret surveillance). As we noted in Section 2 above, in the law enforcement sector, when individuals are charged with crime, for instance, they are essentially notified of the data processing and it might be the case that disclosing further information about the data processing, depending on the case, might not be critical. The fact that the ECtHR has acknowledged that, even in certain national security cases, a notification can be provided means that it cannot be deemed proportionate that in all law enforcement matters no notification or further access to the data can be provided, especially by an independent authority which is supposed to independently balance the competing interests at stake. Another disturbing observation is that this general ban on the COC is not restricted in time, such as for the duration of an ongoing investigation.

We note that these absolute and indiscriminate restrictions on the right of access apply to the independent supervisory authority (COC). Thus, we can safely conclude that its decision-making power at this point is illusory. The disturbing fact is that the COC does not have to balance the interests of the law enforcement tasks and those of the concerned individuals, nor is the COC obliged to justify its decisions, even to inform innocent individuals that their data have been processed illegally and have been deleted, where it has found the data processing illegal. This might make its control over the police more lenient and less accountable to the concerned individuals and the public, a problem which has been criticized by the ECtHR in more recent case law, in which the ECtHR looked more closely at the effectiveness of the

77 This is because the ECtHR may examine the compatibility of national implementing laws with the ECHR, e.g. those implementing Article 17 LED, especially where a Member State exercises its margin of appreciation in implementing EU acts (see A-I Kargopoulos, 'ECHR and the CJEU. Competing, Overlapping, or Supplementary Competences?' (2015) 3 in *Eucrim*, Focus: European Criminal Law and Human Rights, p. 96; F Cherubini, 'The Relationship Between the Court of Justice of the European Union and the European Court of Human Rights in the View of the Accession' (2015) 16 *German Law Journal* 6, 1375.

78 See, as an example, how the ECtHR examined the French indirect access procedure as applicable in the context of the then applicable Schengen Information System (SIS) provisions in *Dalea v France* (n 53).

79 Belgian Act on the protection of natural persons with regard to the processing of personal data of 30 July 2018, Belgian Official Journal, 5 September 2018 ('Belgian Data Protection Act'), Art 42(2). See discussion in Dimitrova and De Hert 2024A (n 5).

independent (administrative) oversight.[80] The situation also implies that *de facto* and *de jure* the police authorities are not obliged to justify the refusal of access to the COC, which in turn cannot assess the legality of the restriction and grant transparency when no law enforcement interest can be prejudiced by the disclosure.[81]

Furthermore, we saw that the ECtHR pays serious attention to the right to effective remedies in general. Indeed, it tended to find restrictions on the right to notification in national security cases, i.e. in very limited cases, where individuals could seek effective remedies, compatible with the ECHR. It remains questionable whether the restrictions on the transparency of the COC in the law enforcement field offer an effective judicial review. Assuming that individuals may formally turn to the courts and theoretically challenge the data processing by the law enforcement authority, we argue that it is difficult to contest the information and the legality of its processing if the concerned individuals have not been granted access to the data as processed by that authority.[82] We saw that effective judicial review is a consistent requirement by the ECtHR, especially in cases where individuals do not obtain full access to the requested information, but there are unanswered questions on important details. How the ECtHR would reason on this in theory, can therefore not be claimed with certainty. Doubts about effective non-judicial and effective judicial review in Belgium exemplify our criticism that the mere existence of oversight mechanisms cannot be an effective safeguard if the oversight authorities are not independent from the law enforcement authorities and do not have any possibility of granting actual access to the data (see Sections 5 and 6).

Contrary to the situation in Belgium, the indirect access procedures in France and Germany are not phrased in law as the only procedure for access, but problematic aspects under the ECHR and the case law of the ECtHR remain. This is mostly due to the fact that the DPAs in both Member States might not always be able to overturn the decision to refuse access taken by the law enforcement authorities, which signals a lack of detachment from the law enforcement authorities with which they operate. In most cases, the DPAs are allowed to disclose information to the concerned data subjects about the processing of their data only after the authority which processes the data has given its approval for the disclosure, lacking criteria when such 'approval' may be withheld.[83] As a result, the DPAs are not able to effectively address the grievances of the data subject in relation to the non-disclosure, especially where the non-disclosure is assessed as illegal by the DPAs. Also, they might become too influenced by the opinions of the law enforcement authorities and may end up simply rubber-stamping their refusals, acting in the interest only of these authorities, which has been deemed problematic by ECtHR judges.[84] Similar to what we noticed in the Belgian case, we observe that the restrictions on the effective supervision and accountability of the DPAs about their supervisory work to the concerned individuals are quite indiscriminate and might lead to unjustified restrictions on transparency, again where no law enforcement interest would be prejudiced by the disclosure and no national security interest is at stake. The situation creates a *déjà vu* with *Leander* (see Sections 2.1 and 5.1 and 5.2), where the mere existence of administrative supervisory bodies did not manage to curb abuse, consisting in the illegal processing, which remained in the dark for years.

We argue that the situation created by the French and German laws also has parallels with the situation with the (non)-disclosure of the Communist files in Romania and Poland, where the administrative bodies tasked with deciding on the disclosure were prevented from effectively

80 *Centrum för Rättvisa v Sweden* (n 63) and *Ekimdzhiev II v Bulgaria* (n 36). As seen in the previous sections, even in the national security context the ECtHR was critical when national laws did not offer any possibility at least for a confirmation of the data processing or when this possibility was severely restricted, e.g. only when the individual's guilt had not been proven, as in *Zakharov* (n 44).

81 See by contrast the recommendations of the Venice Commission (n 47).

82 As the CJEU ruled recently on the Belgian law, where the provision of information would not prejudice a legitimate law enforcement task and the said information is necessary for the exercise of the fundamental right to judicial remedies, it should be provided (see Case C-333/22, *Ligue des droits humains ASBL, BA v L'organe de contrôle de l'information policière* [2023] ECLI:EU:C:2023:874, paras 65–66).

83 German Federal Data Protection Act, § 57 para 7, 6th sentence; Article 108 French Law Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, as amended on 1 June 2019. See discussion in Dimitrova and De Hert 2024A (n 5).

84 This is aggravated by the fact that the DPAs are not obliged by law to provide much more information than a confirmation that the necessary checks have been carried out and thus their transparency powers are not enabled by the laws.

doing so, even where disclosure should have been granted, because of the lack of cooperation from the authorities which were supposed to give their approval.

We also cannot be sure that the German DPAs can effectively hold the German law enforcement authorities accountable for their non-compliance with the data protection laws, because of the provision in German law that sometimes the data may not even be provided for review to the DPAs if the highest national security authority blocks this disclosure.[85] We notice that the provision refers to national security, where in general the ECtHR has been more lenient on the restrictions to transparency. However, a common sense argument is that this situation does not lead to effective administrative supervision over the processing of personal data when these are exchanged between the police and the national security agencies. We are worried, however, that in light of *Dalea*, the ECtHR might be 'pacified' if effective judicial redress is available.

In general, when discussing judicial redress, we doubt whether the French and German courts, similar to the DPAs, can be truly impartial if the individuals cannot state their case for which they would need additional information via the right of access to their data.[86] We would draw attention here to the opinions of individual judges that, in such situations, the courts risk taking sides, either because they are influenced by the law enforcement authorities which dispose of more information, or because they decide to act as the lawyers of data subjects to rectify the information asymmetry. The other problem, which has emerged in practice in Germany, is whether the courts can perform a proper judicial review, especially if the courts do not always obtain the necessary information from the law enforcement authorities to examine a certain case.[87]

The previous analysis of indirect access procedures in these three countries demonstrates that exceptions to transparency for the data subjects, including via the intermediary of the DPAs, are broadly phrased and do not allow the DPAs to independently decide, on a case-by-case basis, what level of transparency about the data processing and about the findings about the legality of the processing should be granted to the data subjects. DPAs are simply not free to assess the impact of these restrictions on the human rights of the concerned data subjects and to be the effective safeguard which the ECtHR has claimed they should be. Unfortunately, we note that only recently has the ECtHR paid closer attention to the effectiveness of the oversight and it remains to be seen which path it will take in the future: whether it will pay more attention to the effectiveness of oversight, or whether it will find it compatible with the ECHR if such authorities simply exist. It also remains to be seen what criteria the ECtHR will develop for the 'effectiveness' of the supervisory authorities and what limits to their effectiveness/independence will be deemed compatible with the ECHR. Hence, we are careful about establishing the ECtHR as a standard on effective supervision over the restrictions on transparency. Nevertheless, we can claim with certainty that the discussed implementing laws are highly likely to be problematic under the ECHR.

8 CHALLENGING DATA PROTECTION AUTHORITIES AS EFFECTIVE OVERSIGHT BODIES BEFORE THE ECtHR

Recently, the French legal provisions on 'indirect access' triggered 17 joint complaints with the ECtHR.[88] The subject of the challenge was the 2015 French law on indirect access to the

85 German Federal Data Protection Act, § 57 para. 7, 3rd sentence.

86 See criticism on the *Conseil d'Etat* rulings on transparency, which are seen as restrictive, because they prevent disclosure of information to the data subject which might be necessary to prove or challenge the legality of the processing of the data: 'Accès aux données : Le Conseil d'Etat et le droit d'accès indirect', 8 November 2019, http://libertescheries.blogspot.com/2019/11/acces-aux-donnees-le-conseil-detat-et.html (last visited 3 March 2025).

87 Case C-481/21, *TX v Bundesrepublik Deutschland* (unfortunately struck out and hence it will not be known how the CJEU would have ruled on it, but the facts of the case still exemplify the problem of effective judicial review within the Member States). Effective redress might be made even more ineffective where a national security authority, to which the LED is not applicable, might withhold its approval to the disclosure of the data by the law enforcement authorities and/or the DPAs, e.g. as is possible in Germany and France. The problem emerges where the decision of the national security authority might not be challenged in court because of the lack of standing of such authorities, a situation criticized by the ECtHR in connection with of the Romanian legal framework on access to the Communist files (see Section 6.2).

88 See the questions raised in each of the 17 cases: Emmanuel Bodinier contre la France et 16 autres requêtes. (voir liste en annexe) communiquées le 14 avril 2021, Requête no 40377/17. Although it is not clear whether the complaints refer to the French provisions implementing the LED (as the case refers to a 2015 French law, which might or might not have been amended after the entry into force of the LED) or whether they refer to purely national security provisions which fall outside the scope of the LED, we find that the questions raised are equally relevant for the indirect access procedure under the LED and might bring more clarity about the interpretation of indirect access under the LED.

DOI: 10.36633/ulr.905

files concerning national and public security and defence.[89] The complaints can be broadly summarized as referring to the impossibility or difficulty for the applicants to obtain access to their data as collected by the French law enforcement/security authorities.[90]

Three applicants in particular challenged in a straightforward way the French indirect access procedure, as made possible under the LED, claiming its incompatibility with Articles 8 and 13 ECHR,[91] because the legality check by the supervisory body in France (the CNIL) does not guarantee an effective procedure for the legality control over the processing, since only the concerned data subjects are in a position to assess the accuracy of the processed data.[92]

The applicants also claimed that the French legal framework does not offer any access, rectification and contestation opportunities as concerns the data to which access was sought in breach of Article 8, and also of Articles 6 and 13 ECHR.[93] On the point of judicial remedies, the question was raised as to what scope the judicial review by the Council of State should have: should this administrative court be able to examine the classification of the information as secret and examine the authorities' decision not to disclose the information to the data subject and be able to order the de-classification of the information?[94]

We note that the answer to this last question could also clarify the question of what an effective remedy in non-disclosure cases, especially where the indirect access procedure applies, under Article 13 ECHR should look like, as this is not very evident from the ECtHR's case law.[95] Although the European Court of Human Rights (ECtHR) has determined that, in principle, the right to effective remedies should provide adversarial proceedings,[96] it is debatable whether the protection of this right can be guaranteed if individuals do not have access to the necessary information to present their case.[97] Additionally, concerns arise when domestic courts are unable to grant relief, including the disclosure of information for a proper assessment of restrictions, due to limitations within the legal framework that prohibit such disclosures.

It will be interesting to see whether the ECtHR in these French cases will be strict in assessing the role of the domestic courts in non-disclosure cases, especially whether the courts can act as an effective and neutral safeguard against abusive restrictions.

9 CONCLUSION: 'INDIRECT ACCESS' POSES HUMAN RIGHTS PROBLEMS

With the expansion of the data processing network of law enforcement authorities and the increasing interest of individuals in obtaining access to the data stored about them by these authorities, it remains important to understand what the right of access to one's personal data actually constitutes and under what conditions it may be (entirely) replaced by a system of independent administrative oversight.

89 According to the applicable French procedure, the data subjects must turn to the French Data Protection Authority (CNIL), which is allowed to disclose to them the information as processed in one or more of those files only if the controller does not oppose the disclosure. If they oppose the disclosure, then the individuals may seek remedies with a special chamber in the Council of State (one of the highest French courts), whose members should be granted access to the contested files.

90 The different claims are based on Articles 6, 8 or 13 ECHR, or a combination of these provisions.

91 *Alexandrov v France*, see also *Polloni v France* (see *Bodinier v France* (n 88)).

92 *Bodinier v France* (n 88), concerning Articles 8 and 13 ECHR.

93 Amongst the other complaints, the applicants claimed that indirect access does not offer equality of arms and access to the court files in breach of Article 6 ECHR, including amongst other things because the CNIL did not disclose any information to the concerned applicant. Another issue raised under Article 6 ECHR was that the procedure offers the affected individuals no opportunity to seek effective remedies if they do not know whether their data are processed or not.

94 See from the application in *Bodinier v France* (n 88): 'La formation spécialisée du Conseil d'État peut-elle vérifier si la classification des informations par le responsable du traitement du fichier était justifiée et peut-elle se livrer à l'examen des raisons invoquées par celui-ci pour ne pas communiquer les informations? Est-ce que, si elle l'estimait nécessaire, la formation spécialisée du Conseil d'État peut demander au responsable du traitement du fichier la levée du caractère secret de certaines des informations classifiées?'.

95 *Segerstedt-Wiberg* (n 18), para 116 confirms that partial disclosure of information about oneself can trigger the applicability of Article 13 ECHR.

96 European Court of Human Rights, 'Guide on Article 13 of the European Convention on Human Rights: Right to an effective remedy' 30 April 2020, 54.

97 On granting of a relief which is *de jure* and *de facto* 'effective', *Segerstedt-Wiberg* (n 18), para 117.

DOI: 10.36633/ulr.905

We studied the applicable case law of the ECtHR on the right of access and its requirements on notification in surveillance cases, including on the requirements on independent oversight when access and notification are restricted. This paper thus adds, with its comprehensive analysis of human rights law, to our previous work which provided a holistic reading of the LED and EU primary law on the topic. The analysis in the present paper reveals that there are small but meaningful developments in the case law of the ECtHR. Also, there are developments with regard to a duty of governments to notify an individual, at a certain point, that there has been surveillance or other kind of data collection. The right of access to one's data has a longer standing in the case law but complementing it with a right for the concerned individuals to be notified when the security or law enforcement interests allow it, is more than welcome. More precisely, the ECtHR has indicated that it is important to notify individuals of the surveillance measures when the notification cannot prejudice the concerned national security interest. There is no longer any room in recent case law for a system of absolute restrictions on information to be provided to the concerned data subjects (e.g. *Centrum för Rättvisa, Ekimdzhiev II,* and *Kennedy*). Together, access and notification as sub-rights of Article 8 (one could equally defend the thesis that both are sub-rights or even essential components of the Article 13 right to an effective remedy) contribute to more transparency for the individual and for society. We saw that this transparency is not beneficial for its own sake only: it can also contribute to a higher level of legality of personal data processing through the increased accountability of the law enforcement and security authorities.

Access and notification, however, are not absolute (sub-) rights. For practical reasons, access (and notification) might often be refused, for instance for the fulfilment of legitimate law enforcement purposes. However, the requirement to inform a supervisory body that can review the decision of security and law enforcement authorities not to disclose the requested information makes more sense and contributes to an accountable set of safeguards with an individual and collective dimension, as does the power of oversight bodies to communicate to the individual and to society about their findings after review.

One of the central questions in this paper is whether oversight should replace transparency rights such as access (and notification): can a right, such as the right to access, always and, if so, under what conditions, be replaced by an oversight mechanism of independent supervisory authorities? This question is relevant both under the EU legal order under the LED and under the ECtHR because both legal orders envisage to different degrees such a 'replacement'.

Older case law of the ECtHR, such as *Leander*, seems to be re-oriented by more recent case law showing more nuance and less naiveté (especially in *Centrum för Rättvisa v Sweden* and *Ekimdzhiev II)*. Oversight procedures need to have real added value, especially when they replace direct transparency between law enforcement (or security) authorities and the individual. To a degree, this new sensitivity plays out for both non-judicial and judicial review: no access by an oversight body to the data, no powers to demand data and no powers to (independently decide whether to) communicate about the findings of the legality review to the concerned individuals weakens the position of the oversight body both under Article 8 and Article 13 ECHR. It also weakens the position of the concerned individuals, who might be left 'at the mercy' of the law enforcement and supervisory authorities if they are not informed at least of the findings of the legality check and cannot state their case in courts in order to have their claims examined by a court in adversarial proceedings where the courts remain neutral and are not disproportionately influenced by the party holding the data which thus possesses more information than the individuals.

Three lessons can be learned when the human rights *acquis* on access as constructed by the ECtHR is applied to indirect access procedures in Belgium, France and Germany. First, absolute restrictions on 'direct' access, as is the case in Belgium, are hardly acceptable under the ECtHR case law. Second, the provisions in the laws of the three examined Member States which either completely ban the supervisory authority from disclosing any information on the legality check (Belgium) or making this communication dependent on the law enforcement and national security authorities (France and Germany) are clearly problematic for the ECtHR. This is especially so because the supervisory authorities might become too lenient towards the law enforcement authorities and rubber-stamp their decisions. In addition, the supervisory authorities might be too influenced by the law enforcement authorities, whereas the individuals who do not have access to the data to contest it might remain unrepresented. Third, we quoted examples from the legal framework and practice in the three countries which pose doubts as to whether individuals may exercise their right to effective judicial remedies in relation to their right of access.

Considering that many access requests to personal data in the law enforcement context are likely to involve minor crimes and not pose issues for national security, unlike most of the national security cases cited above, and noting that Member States have a smaller margin of appreciation in the law enforcement field compared to national security, it is anticipated that the ECtHR's critical stance on these issues will be upheld. The ECtHR may even establish additional conditions regarding the effectiveness and independence of administrative oversight, particularly concerning minor crimes, when examining the strict necessity of the restrictions.

Finally, the present contribution has not gone into the matter of comparing judicial oversight with administrative oversight. In terms of independence, the former is superior but there might be reasons in a specific case to work with the latter or with a combination of the two.[98]

COMPETING INTERESTS

Paul De Hert contributed to the present paper in the framework of his participation into the iBOF Project (Future-proofing human rights. Developing thicker forms of accountability). The paper has also been inspired by Diana Dimitrova's PhD dissertation at the Vrije Universiteit Brussel (Diana Dimitrova, 'Data Subject Rights: The Rights to Access and Rectification in the Area of Freedom, Security and Justice', VUB PhD Dissertation, 2021).

AUTHOR AFFILIATIONS

Diana Dimitrova orcid.org/0000-0003-4732-7054
FIZ Karlsruhe – Leibniz Institute for Information Infrastructures GmbH, Germany; Vrije Universiteit Brussel, LSTS Group, Belgium

Paul De Hert orcid.org/0000-0003-4084-6898
Vrije Universiteit Brussel, Belgium; Tilburg University, Netherlands

TO CITE THIS ARTICLE:
Diana Dimitrova and Paul de Hert, 'Real Transparency and Real Oversight of Law Enforcement Data. The ECHR and the Lack of Accountability of Indirect Access Procedures' (2025) 21(1) Utrecht Law Review 49–69. DOI: https://doi.org/10.36633/ulr.905

Published: 01 September 2025

Utrecht Law Review is a peer-reviewed open access journal published by Utrecht University School of Law.

98 'The authorisation of such powers could be subjected to judicial confirmation, whether as an alternative or in addition to oversight by other bodies. This could enable close, independent scrutiny providing a robust method of oversight.' (Genevieve Lennon, 'Stop and search powers in UK terrorism investigations: a limited judicial oversight?' (2016) 5, *The International Journal of Human Rights*, 634–648, 643). There is also the practical difficulty of the consequences of judicial decisions which apply to all similar cases and could adversely affect a huge number of individuals, whereas administrative decisions are more focused on individual cases.