20

Standards for Independent Oversight

The European Perspective

NICO VAN EIJK

I. ABSTRACT

There are many ways to approach the question of government access to private-sector data. Much of the recent public debate has focused on access in the context of national security and traditional law enforcement, with respect to both targeted and untargeted access to data collected and processed by third parties. As more and more data is collected and stored by the private sector ("big data"), the amount of data that can be retrieved by governments is steadily increasing. A new "third domain" has emerged, where data is used for social security and tax surveillance and other types of non-traditional law enforcement. The *Digital Rights Ireland* case is the point of departure of this chapter. Next, two recent judgments by national courts are described, in which national data retention rules were tested against the ruling in the *Digital Rights Ireland* case and the necessity of independent oversight was discussed in further detail. This chapter draws from a recent study by the Institute for Information Law (IViR) to formulate standards for independent oversight. These standards are based on a broader analysis of the relevant jurisprudence of the European Court of Justice—including the *Digital Rights Ireland* case—and of the European Court of Human Rights (ECtHR). The analysis is also based on selected studies, reports, resolutions, and recommendations.

II. INTRODUCTION

There are many ways to approach the question of government access to private-sector data. Much of the recent public debate has focused on access in the context of national security and traditional law enforcement, with respect to both targeted and untargeted access ("bulk collection" or "mass surveillance") to data collected and processed by third parties. As more and more data is collected and

Bulk Collection. Fred H. Cate and James X. Dempsey.

stored by the private sector ("big data"), the amount of data that can be retrieved by governments is steadily increasing. Traditional impediments, such as storage and processing costs, no longer apply. Moreover, data collected privately is increasingly used not just for national security and traditional law enforcement purposes. A new "third domain" has emerged, where data is used for social security and tax surveillance and other types of nontraditional law enforcement. For lack of a better term, we call this third category "public task surveillance."[1]

Government access to private data implies the deployment of government power. In a classic rule of law tradition this requires an explicit basis in law and a carefully crafted system of checks and balances: special powers require special guarantees. Independent oversight is an undeniably crucial element of such a system of checks and balances.

The major preconditions for independent oversight can be found in the judgment of the European Court of Justice (ECJ) in the *Digital Rights Ireland* case,[2] which annulled the European Data Retention Directive (DRD).[3] Particularly, the Court took the view that the Directive did not comply with Article 7 (Privacy) and Article 8 (Data protection)[4] of the Charter of Fundamental Rights of the European Union (the Charter).

The *Digital Rights Ireland* case is the point of departure of this chapter.[5] Next, two recent judgments by national courts are described, in which national data

1. Readers of this chapter are encouraged to come up with a better name. Access for other types of use, such as statistical analysis, fall outside the scope of this essay. However, we note that several similar questions are at stake. For example, the collection of statistical data can be based on a legal obligation. In such a case, questions arise on the existence of free consent, proportionality, function creep, etc.

2. Judgment of the Court (Grand Chamber) of 8 April 2014 (requests for a preliminary ruling from the High Court of Ireland (Ireland) and the Verfassungsgerichtshof (Austria))—*Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12)*, (Joined Cases C-293/12 and C-594/12.

3. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Pb. L 105/54, 13 April 2006.

4. Article 7 (Respect for private and family life): "Everyone has the right to respect for his or her private and family life, home and communications." Article 8 (Protection of personal data): "1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority."

5. The Data Retention decision of the ECJ was an important element in the Safe Harbor decision, which annulled the agreement between Europe and the United States on the transfer of

retention rules were tested against the ruling in the *Digital Rights Ireland* case, and the necessity of independent oversight was discussed in further detail.

We draw from a recent study by the IViR to formulate standards for independent oversight.[6] These standards are based on a broader analysis of the relevant jurisprudence of the European Court of Justice—including the *Digital Rights Ireland* case—and of the European Court of Human Rights (ECtHR).[7] The analysis is also based on selected studies, reports, resolutions, and recommendations.

In the IViR study and in this chapter, we use a broad definition of the term "oversight" to include the various ways of holding government agencies accountable before the public and the government: internal oversight by the responsible minister, parliamentary oversight, judicial oversight, and external independent oversight. In the surveillance context, oversight can focus on specific instances in which surveillance measures are implemented against a particular target, on bulk interception of electronic communications, or on the overall functioning of a system of secret surveillance and data collection.

III. THE EUROPEAN DATA RETENTION DIRECTIVE

As a result of the 2004/2005 bombings in Madrid and London, the so-called Data Retention Directive (DRD) came into effect in 2006. This Directive was based on general powers under the EU-treaties to harmonize rules in the European Union. It did not concern national security as such, as the European Union does not have any powers in this domain. National security is the sole responsibility of the Member States. The European Union does have some authority with respect to traditional law enforcement, but in this domain, too, the role of the Member States is decisive to a large extent.

data (European Court of Justice (*Schrems v. Data Protection Commissioner*), Case C-362/14, 6 October 2015).

6. Sarah Eskens, Ot van Daalen & Nico van Eijk, "10 Standards for Oversight and Transparency of National Intelligence Services," 8 *J. Nat'l Security L. & Pol'y*, no. 3, (2016) pp. 553–594, http://jnslp.com/wp-content/uploads/2016/07/10_Standards_for_Oversight__Transparency.pdf.

This chapter focuses on the oversight elements of the study.

7. The European Court of Human Rights in Strasbourg—applying the European Convention on Human Rights—has a rich tradition of jurisprudence on surveillance. This jurisprudence is also applicable to the European Union. The Charter makes this explicit in article 52, par. 3: "In so far as this Charter contains rights which correspond to rights guaranteed by the European Convention on Human Rights, the meaning and scope of those rights shall be the same as those laid down by said Convention. This provision shall not prevent Union law providing more extensive protection." Recently, the European Court of Human Rights issued two important decisions confirming and deepening its earlier jurisprudence on surveillance (Case of *Roman Zakharov v. Russia* (Application no. 47143/06, Strasbourg, 4 December 2015) and Case of *Szabó and Vissy v. Hungary* (Application no. 37138/14, Strasbourg, 12 January 2016).

Therefore, the Directive was intended to harmonize the laws of Member States concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data that is generated or processed by them, in order to ensure that the data would be available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law. The scope of the Directive included both location and traffic data, but content fell outside the Directive. It should be noted that if topics fall outside the scope of a directive, they can still be subject to regulation. Member States are entirely free to step in (or have regulation in place already).

The Directive provided only a framework for national laws, as shown not only by its short length but also by the general nature of its provisions on access, retention duration (between six months and two years), data storage and security, and oversight. Detailing these aspects was left to the Member States.

A. European Court of Justice Declares Directive Invalid

As soon as the Directive entered into effect, it was challenged on fundamental grounds. Consequently, its implementation was blocked completely or partly by national courts in several countries, for instance in Bulgaria (2008), Romania (2009), Germany (2010), and Cyprus (2011).

In the *Digital Rights Ireland* case, the Directive was eventually submitted to the European Court of Justice (ECJ).[8] In his preceding opinion, the Advocate-General concluded that the Directive was not in compliance with the Charter, but that some room should be allowed for repair.[9]

The Court found no such room and declared the entire Directive invalid. Such a step is very unusual. Declaring a directive invalid is an extreme measure.

As to oversight, the Court based its judgment on Article 8 of the Charter, in which data protection is guaranteed as a fundamental right. Paragraph 3 of Article 8 provides that "compliance with these rules shall be subject to control by an independent authority." The paragraph doesn't allow exceptions. The Court stated "In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an

8. In an earlier case, the ECJ had decided that the EU treaty as such provided sufficient ground for the Directive (Case C-301/06, *Ireland v European Parliament and Council of the European Union*). However, the ECJ made explicit that it was not looking into the substance: "It must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24."

9. Opinion 12 December 2013 (ECLI:EU:C:2013:845).

independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits."[10]

Noting another consideration, the Court completed its reasoning with respect to independent oversight by stating: "the directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data."[11]

Additionally, the Court made one other comment that is relevant to the question of oversight when it noted that the Directive did not make any distinction concerning the collection of data concerning individuals (such as lawyers) who are bound by a duty of professional secrecy: "Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services (. . .). Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."[12] With this, the Court seemed to indicate that independent oversight in the case of 'professional secrecy'—and perhaps with regards to other uniquely sensitive matters as well—requires special attention and safeguards.

B. National Courts Follow ECJ Decision

After the judgment of the European Court of Justice, various national courts have had to rule on the consequences of the judgment for national legislation. After all, the cancellation of a directive does not automatically mean that the national implementation is invalid. A directive allows Member States some leeway for further specification by which the national regulations might be in compliance with the preconditions. The countries where the implementation of the judgment of the Court has been tested include the Netherlands, Belgium, Slovenia, and the United Kingdom. In each of these countries, the national implementations of the Data Retention Directive were annulled after judicial review. In the Netherlands and the United Kingdom, the Court explicitly focused on the independent oversight issue.

10. ¶ 62.

11. ¶ 68.

12. ¶ 58.

1. The Netherlands

On March 11, 2015, a district court in the Netherlands annulled the Dutch implementation of the Directive.[13] The Netherlands had implemented the Directive via a special law, the Wbt (Act Data Retention Telecommunication Services). With respect to oversight, the court concluded that independent oversight was not provided for in the Dutch implementation: "The foregoing is all the more important considering that the Wbt and related regulations do not require a prior authorisation by a judicial authority or independent administrative body in order to access the retained data. Different from that which is argued by the State, the office of public prosecution cannot be considered an independent administrative body. That the Court[14] has considered this as a compelling objection can be derived from the words 'above all' in consideration 62 of the judgment."[15] The decision of the district court was not challenged pending an upcoming review of the Dutch Intelligence and Security Services Act.

In an October 2015 decision, the same court dealt with the lack of restrictions on the surveillance of lawyers.[16] Because no special EU legislation or regulation is applicable to lawyers, the court did not use the EU Charter as a reference but relied instead on Article 8 of the European Convention on Human Rights (the Convention), which provides for protecting privacy and has been used in several cases dealing with surveillance. The court was of the opinion "that the breaching of journalists' and lawyers' privilege has serious consequences for the principles of a democratic state governed by the rule of law."[17] The court continued: "The mere possibility of breaches of lawyers' privilege affects the confidentiality of communications between lawyers and their clients and thus the right to an effective defence and the availability of lawyers. So in a sense this breach is also irreversible. Having regard to the serious consequences of (possible) breaches of lawyers' privilege and given that in individual cases abuse is potentially easy, the judge considers that, in accordance with the reasoning of the ECtHR in para. 98 of the *Telegraaf* case,[18] it is highly desirable that there should be independent oversight of the exercise of special powers, such that the oversight body must possess inter alia the power to prevent or to terminate the exercise of special powers."[19] The decision forced the Dutch government to implement an

13. ECLI:NL:RBDHA:2015:2498. Unofficial translation: http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf

14. The ECJ in the *Digital Rights Ireland* case.

15. ¶ 3.11.

16. ECLI:NL:RBDHA:2015:7436, no translation available; the Hague court of appeal upheld the verdict ECLI:NL:GHDHA:2015:2881. Unofficial translation of the decision by the Hague court of appeal: http://www.advocates.org.uk/media/1912/dutchspyingruling.pdf.

17. ¶ 4.10.

18. Case of *Telegraaf Media Nederland, Landelijke Media bv and others v. The Netherlands* (Application no. 39315/06), 22 November 2012.

19. ¶ 4.10.

exective order introducing a first form of ex ante independent oversight. A special independent committee assesses the proposed orders and can block them.[20] The order only deals with lawyers and the protection of journalists' sources.

2. United Kingdom

In response to the Data Retention Directive being declared invalid in the *Digital Rights Ireland* case, the United Kingdom immediately adopted a new act, the Data Retention and Investigatory Powers Act 2015 (DRIPA), in an effort to address the gaps in the Directive identified by the ECJ and thus provide an adequate basis for data retention. The act was fast-tracked through Parliament and adopted within three days. In a High Court ruling of July 17, 2015, however, the act was declared invalid.[21] The complainants argued that the act violated Articles 7 and 8 of the Charter, and the Court agreed. With respect to prior independent oversight the Court referred to the considerations noted by the ECJ in the *Digital Rights Ireland* case and tested the UK legislation against them. The High Court pointed out that "the provisions of RIPA, as applied by DRIPA, require (as we have noted above) that an application for access to communication data must be considered by a senior person who is independent of the investigation. There is already a need for there to be a written request for approval. The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome [. . .]; but if EU law requires independent approval, as we are satisfied it does, that must be put in place. It is not for us to devise the appropriate system."[22]

It is interesting that the British Court paid close attention to the same subject that had been dealt with earlier in the second Dutch case, that is, the special position of lawyers—but others are added as well—and stated: "However, communications with practising lawyers do need special consideration. The same in our view can properly be said to apply to communications with MPs." As far as oversight is concerned, it concludes: "As to the question of what level of consideration should be given to applications involving access to data involving communications with lawyers, Members of Parliament, or journalists, that too is not for us to determine. We only observe that such cases do require special consideration."[23]

20. The order by the ministers of the Interior and of Defence, responsible for national security, is named "Tijdelijke regeling onafhankelijke toetsing bijzondere bevoegdheden Wiv 2002 jegens advocaten en journalisten" (no translation available) and was published in the Official Journal of 23 December 2015 (No. 46477).

21. [2015]EWHC 2092 (Admin), Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014, dd. 17/7/2015.

22. ¶ 98.

23. Ibid.

Finally, the High Court emphasized that it was distingusihing in its analysis between access and retention: "We add the important proviso that the requirement of prior approval relates to access, not to retention. We see no reason why the exercise of the power to retain should need prior independent approval, and we do not understand the CJEU to have held that it does."[24]

IV. STANDARDS FOR INDEPENDENT OVERSIGHT

The *Digital Rights Ireland* decision of the European Court of Justice forms a core element in our IViR study *Ten Standards for Oversight and Transparency of National Intelligence Services*. In this study, we formulate generally applicable standards for independent oversight. These standards are based on the jurisprudence of the European Court of Justice and the European Court of Human Rights, including what can be deduced from that jurisprudence as best practices, and our assessment of the direction future case law is likely to take. In order to further substantiate the standards, the study draws from a selection of reports and soft law measures that have been issued in Europe and the United States.

The following list from the study relates to oversight of intelligence services, especially in the context of communication interception using the sophisticated technologies now associated with untargeted ("mass") surveillance. The standards should be read in combination—one would not work without the others. For example, independence in oversight will only be effective if oversight is supported by adequate resources. No references are included but can be found in the report.

A. Intelligence Services Need to Be Subject to Oversight That Is Complete

Under this standard, oversight should be complete in three respects: (1) The oversight *bodies themselves*: the government, parliament, the judiciary, and a specialized (non-parliamentary, independent) commission should all play a role in oversight. (2) The *moment* of oversight: oversight should include prior oversight, ongoing oversight, and oversight after the fact. (3) *Mandate*: the oversight bodies' mandate should encompass review of both lawfulness and effectiveness.

Disclosures in the media have demonstrated that there is a need for enhanced oversight, even in countries where oversight appears to be quite comprehensive. The overall blend of oversight mechanisms for national intelligence services is important. In the end, oversight encompassing all of the above elements is essential to ensure that adequate and effective guarantees against abuse and arbitrary use of secret surveillance and data collection powers are in place. Because the effectiveness or ineffectiveness of intrusive measures is relevant to the

24. ¶ 99.

proportionality test, we deduce from the jurisprudence that courts can address both lawfulness and effectiveness.

B. Oversight Should Encompass All Stages of the Intelligence Cycle

Surveillance occurs in stages, including the collection, storage, querying, and analysis of data. As each of these stages amounts to an interference with the right to privacy, each should be subject to oversight to a certain degree. In practice, this means that not only collection and selection stages should be subject to prior independent oversight, but also the analysis itself.

C. Oversight of the Intelligence Services Should Be Independent

Some of the oversight bodies must be independent of the intelligence services and the government. For example, public prosecutors in most political systems cannot be regarded as independent of the government. Similarly, government ministers cannot provide for independent oversight, as they are part of the government that is both the tasking body and the customer of the intelligence services. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to entrust oversight of secret surveillance and data collection to a judge, as is already the case in certain jurisdictions. However, the independence of judicial-like bodies is not a given. However, the fact that some courts in the past "rubber-stamped" government requests or took quite long in making their decisions is not an argument against judicial oversight as such. Rather, such concerns merely underline that adequate resources are essential to guarantee the independence and effectiveness of oversight bodies.

The independence of a specialized commission can be guaranteed by having its members appointed by parliament using an open and transparent selection and nomination procedure, where the voting power should not depend on parliamentary size, but where, for example, each political party including the opposition gets a vote. Furthermore, a standing parliamentary committee specializing in oversight of the intelligence services can be regarded as independent only if its members represent the opposition as well as the ruling parties, and the member's voting power does not depend on its parliamentary size. The procedure for dismissing members of an oversight body should also guarantee independence. Preferably, national law or the national constitution should provide that specialized commissions and parliamentary committees cannot be subject to instructions from the government.

There is some overlap between oversight by parliamentary committees and specialized (parliamentary-appointed) commissions, in the sense that both are independent and democratically legitimized. Nevertheless, there are advantages in having both of them. A parliamentary committee is in a better position to defend itself vis-à-vis parliament as a whole and the public, whereas a specialized commission allows for greater expertise in oversight.

To summarize: independence is reflected in several elements, including: (1) transparent and objective procedures for the nomination of the members of oversight bodies, (2) no governmental interference with the activities and decisions of the institution performing the oversight, (3) effective powers, and (4) adequate resources and budgetary independence.

D. Oversight Should Take Place prior to the Imposition of a Measure

In the field of secret surveillance of communications, especially using the sophisticated technologies now associated with untargeted surveillance, the risk of abuse is high, and abuse can have harmful consequences not only for individual rights but also for democratic society as a whole. Therefore, prior judicial oversight of the application of surveillance and collection powers is strongly preferred. Furthermore, the transfer of personal data to third countries requires prior approval by the competent supervisory authority. As an alternative to prior judicial oversight, a system of ministerial orders combined with prior oversight by an independent, specialized commission, after-the-fact oversight on the overall functioning of the system of surveillance by a parliamentary committee, and the possibility for individuals to complain before an independent body could also be compliant with human rights standards. Regardless of the structure, effective oversight will only exist if the body performing prior oversight has adequate powers (see the next Standard).

It should be noted that prior oversight is not at odds with ministerial responsibility: in a system of prior oversight, the minister gives an order for surveillance, and the oversight body merely has the power to block this order. Where—due to exceptional circumstances—it is not possible to wait for a decision by the oversight body because of the urgent nature of the order, the order should be subject to oversight as soon as possible. In addition, the oversight body should have sufficient resources to handle orders quickly. Political responsibility and optimizing the protection of fundamental rights are different topics.

E. Oversight Bodies Should Be Able to Declare a Measure Unlawful and to Provide for Redress

Bodies providing prior and ongoing oversight for intelligence services should have the power to prevent or end a measure imposed by intelligence services, and oversight bodies should have the power to declare a measure unlawful after the fact. In all cases, the oversight body should have the power to order the purging of personal data. Obviously, oversight powers will be effective only if combined with the power to make legally binding decisions and to provide for redress of the unlawfulness of a measure. Given the gravity of the decision to block or end use of a particular surveillance measure, the minister should simultaneously have the power to appeal such descisions to a court. Initial orders to conduct

surveillance should contain sufficient reasoning to allow oversight bodies and appellate courts to evaluate the lawfulness of the measure.

F. Oversight Should Incorporate the Adversary Principle

Where there is no prior judicial oversight, oversight mechanisms have survived the ECtHR's scrutiny under Article 8 of the European Convention on Human Rights only if they included an adequate complaint procedure. In such a procedure, the individual concerned can challenge the lawfulness of measures of secret surveillance and data collection directed against him after the fact. In recent case law, the Court also implied that it should be possible to provide some form of adversarial proceeding prior to approval of a surveillance measure, albeit one where the proceedings are secret. There is some overlap between the Court's interpretation of Article 8 in cases about secret surveillance and data collection for the purpose of national security and cases about deportation for the purpose of national security. In the context of the latter, the Court expressly requires "some form of adversarial proceedings."

This could mean involving a special advocate who defends the public interest (or the interest of affected individuals). This would introduce some form of adversarial proceedings without jeopardizing the secrecy of measures to be imposed. Where the surveillance is more general in nature, the special advocate would rather take on the role of an expert for the court, in order to allow the court to be in a better position to weigh the interests of the intelligence services against the interests of the public in not being subject to surveillance. Where the surveillance is more targeted, the special advocate would defend the rights of the individuals affected. In its 2007 report, the Venice Commission was critical of special advocates, but in its 2015 update of the report it argues for the involvement of privacy advocates as regards searching data obtained by strategic surveillance.[25] One of the most important recommendations of the United States Privacy and Civil Liberties Oversight Board called for the establishment of special advocates before the FISA Court.[26]

25. Report on the democratic oversight of the security services, adopted by the European Commission for Democracy through Law (Venice Commission), Venice, 1–2 June 2007 (CDL AD(2007)016); Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies, adopted by the European Commission for Democracy through Law (Venice Commission), Venice, 20–21 March 2015 (CDL-AD(2015)006).

26. Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, PCLOB 215 Report (January 23, 2014), p. 185. In 2015, in the USA FREEDOM Act, Congress in fact authorized the appointment of special advocates in cases before the FISA Court, and the Court has since appointed advocates in several cases and designated a small pool of advocates who could be drawn upon in future cases.

G. Oversight Bodies Should Have Sufficient Resources to Perform Effective Oversight

For oversight bodies to function effectively in practice, it is critical that they have the resources to obtain the necessary equipment and staff as well as resources in terms of information[27] and technical expertise. Having adequate resurces will ensure that oversight bodies are independent of the intelligence services and the government. Without access to sufficient resources, oversight bodies cannot fulfil their mandate in a meaningful way. As the technological sophistication of intelligence services will only increase, oversight will become more complicated, and it is to be expected that a commensurate increase in resources for oversight bodies will be necessary.

V. ANALYSIS AND CONCLUSION

European courts consider independent oversight a "condition sine qua non" of government surveillance. Governments cannot access private data without sufficient guarantees, including independent oversight. Recent jurisprudence by the European Court of Justice in the *Digital Rights Ireland* case—annulling the Data Retention Directive—confirms this. It should also be noted that the Charter of Fundamental Rights of the European Union explicitly mentions independent oversight in Article 8 (on data protection), paragraph 3: "Compliance with these rules shall be subject to control by an independent authority." In most European countries, Data Protection Authorities (DPAs) are the independent authority. However, DPAs often have no or only limited authority in the domain of national security or law enforcement.

Access to data to prevent serious crime or terrorism requires an assessment by a judge or an independent body of similar qualifications. This assessment needs to be made before access takes place, but it also needs to be really independent and effective. To achieve this, several standards have been formulated. Not all of these standards are based directly on explicit requirements articulated in the jurisprudence: this is not possible because courts have not yet been in the position to deal with every situation and element. However, for a country that takes the rule of law seriously the implementation of these standards is unavoidable.

The constitutional framework as defined in Articles 7 and 8 of the Charter makes no distinction between the three domains (national security, law enforcement, public tasks). As a consequence, oversight needs to comply with the same standards whenever personal data is accessed for (mass) surveillance. The *Digital Rights Ireland* case makes clear that mass surveillance is worse than targeted

27. Transparency contributes to access to information. In the report, we have three standards on transparency: (1) intelligence services and their oversight bodies should provide layered transparency; (2) oversight bodies, civil society, and individuals should be able to receive and access information about surveillance; and (3) companies and other private legal entities involved in national surveillance should be able to impart information about their involvement.

surveillance but sets oversight standards that are at least similar to those applicable to targeted surveillance. This is why these oversight standards also apply to the third domain (public tasks). Having the same level of qualified independent oversight does not exclude that—by applying subsidiarity and proportionality tests—the allowed use of particular methods and practices can differ among the three domains.

Because the constitutional framework makes no distinction, independent oversight needs to cover not only collection (the acquistion and storage of data into government databases) but also querying the data stored in private systems. Particularly in Europe, it is very likely that governments will collect data autonomously by accessing data stored by private entities. Furthermore, once accessed, data will often move into government-controlled databases. Finally, EU Member States used the Data Retention Directive to oblige operators to collect and store data that they would normally not collect or store. There is only a thin line between collection and access as well as between "metadata" and content. In my view, these lines have no real value anymore from a European fundamental rights perspective.

The ECJ's Data Retention decision gave renewed attention to the special position of "persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy,"[28] requiring special attention in the context of oversight. The Court did not specify who falls within the category of persons subject to the obligations of professional secrecy, leaving it to the national legislator, nor did the Court say anything about what the repercussions should be in the oversight system. This issue is part of the first standard ("Intelligence services need to be subject to oversight that is complete"), and it will be interesting to see how the debate on the position of lawyers, judges, politicians, doctors, and journalists for instance will develop. The question might arise whether thin lines will make clear distinctions still possible.

28. ¶ 58.