10 Standards for Oversight and Transparency of National Intelligence Services

Eskens, S.J.; van Daalen, O.L.; van Eijk, N.A.N.M.

Published in:
Journal of National Security Law & Policy

10 Standards for Oversight and Transparency of National Intelligence Services

Sarah Eskens,* Ot van Daalen,** & Nico van Eijk***

EXECUTIVE SUMMARY

This report aims to enhance the policy debate on surveillance by intelligence services by focusing on two key components: oversight and transparency. Both oversight and transparency are essential to devising checks and balances in a way that respects human rights.

By offering this concise list of ten standards, we intend to provide practical guidance for those who seek further input for discussions, policymaking and the review of existing legislation. These standards are based on our analysis and interpretation of relevant jurisprudence, literature and selected policy documents.

Standard 1: Intelligence services need to be subject to oversight that is complete.

Oversight should be complete in terms of a) the oversight body: the government, parliament, the judiciary, and a specialized (non-parliamentary, independent) commission should all play a role in oversight; b) the moment of oversight: prior oversight, ongoing oversight, and after-the-fact oversight, and c) the mandate of oversight bodies: reviews of lawfulness and effectiveness.

Standard 2: Oversight should encompass all stages of the intelligence cycle.

Surveillance involves different stages, including the collection, storage, selection and analysis of data. As all these stages amount to an interference with the right to privacy, these separate stages should be subject to oversight.

Standard 3: Oversight of the intelligence services should be independent.

In this context, this means independence from the intelligence services and the government. Judicial oversight offers the best guarantees of independence. Therefore, it is preferable to involve the judiciary in the oversight on secret surveillance and data collection.

* Sarah Johanna Eskens (LLM) is a PhD candidate at the Institute for Information Law (IViR). Her bio can be found at: http://ivir.nl/medewerkerpagina/eskens.

** Ot van Daalen is a researcher in the field of privacy and security at the Institute for Information Law (IViR). His bio can be found at: http://ivir.nl/medewerkerpagina/daalen.

*** Nico van Eijk Nico van Eijk is Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam). His bio can be found at: http://ivir.nl/medewerkerpagina/eijk. This project has been carried out in full compliance with the Declaration of Scientific Independence of the Royal Netherlands Academy of Arts and Sciences. Funding included a grant from Google. The original report on which this contribution is based was finalized July 2015. For the original report see: http://www.ivir.nl/publicaties/download/1591.

Standard 4: Oversight should take place prior to the imposition of a measure.

In the field of secret surveillance of communications, especially by means of 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 on the application of surveillance and collection powers is essential.

Standard 5: Oversight bodies should be able to declare a measure unlawful and provide for redress.

Prior and ongoing oversight bodies 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 and provide for redress.

Standard 6: Oversight should incorporate the adversary principle.

The 'adversary principle' is a basic rule of law principle. Where secrecy is necessary, this can be implemented by the appointment of a special advocate who defends the public interest (or the interest of affected individuals). As a result, some form of adversarial proceedings would be introduced without the secrecy of measures to be imposed being jeopardized.

Standard 7: Oversight bodies should have sufficient resources to perform effective oversight.

This standard includes the attribution of the necessary equipment and staff, resources in terms of information and technical expertise. Having sufficient resources also contributes to their independence from the intelligence services and the government.

Standard 8: Intelligence services and their oversight bodies should provide layered transparency.

This means that: a) the individual concerned, the oversight bodies, and civil society are informed; b) there is an adequate level of openness about intelligence activities prior to, during and after the fact; and c) notification, aggregate statistics, working methods, classified and detailed information about operations, and general information about what will remain secret under all circumstances is provided.

Standard 9: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance.

This standard more or less mirrors the previous one. Clear legislation on receiving and access to information about surveillance must provide a framework for oversight and supports public scrutiny of the surveillance powers.

Standard 10: Companies and other private legal entities should be able to publish aggregate information on surveillance orders they receive.

Organizations should be able to disclose aggregate information publicly about orders they receive directing them to provide information to the govern-

ment. They should be able to make more detailed/confidential information available to oversight bodies.

INTRODUCTION AND METHODOLOGY

Revelations about the working methods of national intelligence services, most notably through the documents revealed by Edward Snowden, have raised substantial legal and policy questions. These services can be – and in fact have been – engaged in activities that go beyond their legal mandate. Snowden's leaks provide clear evidence that this is the case. These revelations have sparked a highly significant debate on the powers and the practices of intelligence services. In fact, momentum is growing for reform of intelligence service legislation, both in Europe and the United States.[1]

The issue of accountability is a central theme in these discussions. Effective accountability requires a carefully crafted system of checks and balances, allowing for monitoring the exercise of powers and serious measures to address the issue of overstepping legislative boundaries. Oversight and transparency are crucial elements in such a system of checks and balances.

Oversight ensures compliance with the law and can provide remedies in case intelligence services overstep legal boundaries. Transparency mechanisms support effective oversight and democratic control.

For oversight to be credible, it needs to meet the highest possible democratic standards, such as the guarantees and safeguards that are embedded in constitutions and instruments of international law. In a European context, norms for oversight of intelligence services have been developed in the past decades in the case law of the European Court of Human Rights (ECtHR) based on the European Convention on Human Rights as signed by the Member States of the Council of Europe, and the Court of Justice of the European Union (CJEU), addressing the fundamental rights as laid down in the Charter of Fundamental Rights of the European Union.

In this report, we first provide a concise list of standards for oversight and transparency of European intelligence services, focusing on interception of electronic communications, especially using the sophisticated technologies now associated with untargeted surveillance. Existing works that address oversight of intelligence services rely on good governance as a reference point,[2] set forth political rules,[3] or analyze new, relevant cases decided by the ECtHR and the

1. The enactment of the USA Freedom Act replacing the so-called Patriot Act is a first example. *See* USA Freedom Act, Pub. L. No. 114-23, 129 Stat. 268 (codified in scattered sections of 18 U.S.C. and 50 U.S.C.).

2. GENEVA CENTER FOR THE DEMOCRATIC CONTROL OF ARMED FORCES, OVERSEEING INTELLIGENCE SERVICES: A TOOLKIT (Hans Born & Aidan Wills eds., 2012).

3. *Report on the Democratic Oversight of the Security Services*, European Comm'n for Democracy through Law, CDL-AD(2007)016 (June 11, 2007) [hereinafter Venice Commission 2007]; *see also Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the*

CJEU.[4] In this report, we use a human rights perspective, make legal recommendations, and take into account recent developments in jurisprudence.

The following research question guides our report: '*What are recommendable standards for oversight and transparency of intelligence services, in particular for intercepting electronic communications, as guided by the human right to respect for privacy and freedom of expression?*'

In order to answer this question, we first analyze case law of the European Court of Human Rights. There have been many cases before the Court on the topic of secret surveillance and data collection by intelligence services, but in only a few of them did the Court devote substantive attention to oversight and transparency. In this report, we single out the leading cases.

The Court has not had the chance to review the sophisticated untargeted surveillance made possible by technological advances and applied in the past decade, as partly revealed by Snowden. There are some cases on the Court's docket which touch on this particular issue, but these have not been decided yet. It is safe to say, however, that the existing case law on targeted and untargeted communications surveillance by the Court already provides for minimum standards. And as surveillance since then has become more sophisticated and allows for monitoring more persons, the infringement on human rights has become even more significant. Our recommendations are partly based on this premise, and the Court will probably also impose higher standards on, or restrict untargeted surveillance carried out with these new technologies.

One particular sign that courts are adopting higher standards for these practices is the recent decision of the Court of Justice of the European Union on data retention.[5] The European Union has no authority on national security; as stated in Article 4(2) of the Treaty on the European Union (TEU), "national security remains the sole responsibility of each Member State." Nevertheless, the CJEU has given an important judgment related to (secret) law enforcement measures, which is also relevant for our purposes. Furthermore, the fact that the European Union has no authority on national security does not mean that case law created by the CJEU is irrelevant. The CJEU held that "the mere fact that a decision concerns State security cannot result in European Union law being inapplicable."[6] The European Parliament also "strongly rejects the notion that all issues related to mass surveillance programs are purely a matter of national

---

Democratic Oversight of Signals Intelligence Agencies, European Comm'n for Democracy through Law, CDL-AD(2015)006 (Apr. 7, 2015) [hereinafter Venice Commission 2015].

4. IAIN CAMERON, NATIONAL SECURITY AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2000).

5. *See* Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Nat. Res., ECLI:EU:C:2014:238 (Apr. 8, 2014).

6. Case C-300/11, ZZ v. Sec'y of State for the Home Dep't, ECLI:EU:C:2013:363, ¶ 38 (June 4, 2013); *see also* Case C-387/05, European Comm'n v. Italian Republic, 2009 E.C.R. I-11831, ¶ 45.

security and therefore the sole competence of Member States."[7] Thus, we also analyze relevant jurisprudence of the CJEU.

In addition, we look into a selection of policy documents, issued by European and U.S. institutions (see appendix). Furthermore, we have consulted an extensive amount of comments, articles, studies and academic papers in preparation of this report. Given the nature of the report and to enhance its readability, we have refrained from including detailed footnotes. Instead, a non-exhaustive list of recommended literature can be found in the appendices. Decisions are referred to by their abbreviated case name in the footnotes. The application and case numbers can be found in the appendix.

The topic of the report is oversight and transparency of intelligence services, in particular focusing on the interception of electronic communications in bulk. We acknowledge that the activities of intelligence services also raise other questions. For example, the preliminary question of the necessity of powers of surveillance (including bulk surveillance) is not discussed in this report but remains equally important, as lack of necessity (and consequently proportionality and subsidiarity) cannot be compensated by better oversight and transparency. Nor do we focus on other contexts where similar methods are used, and where oversight and transparency are equally relevant, such as surveillance in the context of law enforcement and social security. Nonetheless, it is to be expected that most of the analyses and conclusions in this report will be useful when applied to these other environments.

Lastly, it should be noted that the terminology used to describe the field of intelligence services is quite specific and differs somewhat per discipline. We have explained our use of the terminology in the next section.

This report concludes with practical guidance for policymakers, in particular those who are in the process of reviewing their national statutes. The ongoing revision of the Dutch Intelligence and Security Services Act (Wiv 2002) could be one of the first occasions in Europe where our recommendations can be taken into consideration and tested. As we aim to provide for practical guidance and keep the report concise, we limit our findings to ten standards that we consider the most important ones.

I. A FEW WORDS ON THE TERMINOLOGY USED IN THIS REPORT

As noted in the introduction, in this report we draw heavily on jurisprudence by the European Court of Human Rights and to a lesser extent by the Court of Justice of the European Union. In the past few decades, the ECtHR has used recurring terms to describe concepts relating to intelligence services, thus suggesting it gives them specific meanings. However, it actually defines these concepts only very rarely, and no uniform definitions exist in the literature

7. Report on the U.S. NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, EUR. PARL. DOC. (COM 139) ¶ 16 (Feb. 21, 2014).

either. It is therefore useful to provide definitions of the actors and actions that are relevant to the topic of oversight and transparency. In doing so, we take a functional approach rather than provide exhaustive definitions.

A. Intelligence Services

A concept central to the topic of this report is that of 'intelligence service.' This term at least covers all government agencies that collect, process, analyze, and disseminate electronic communications and other types of data for national security purposes.

On a national level, a division is often made between a general, or civil intelligence service and a military intelligence service. It is also customary to have a separate foreign intelligence service and a service for national intelligence. The latter might be called 'security service.' Intelligence for national security and law enforcement purposes is usually gathered by different agencies. Many governments have also set up a specialist intelligence service that is solely responsible for gathering signals intelligence (SIGINT), which refers to the interception of radio and cable-bound communications and of signals not directly used in communications, such as signals from radar or weapon systems. In some countries, the intelligence services are part of, or integrated into, law enforcement. In those countries, the intelligence services might therefore also possess general law enforcement powers. Additionally, the activities of intelligence services might not be restricted to 'national security' in a strict sense and include other domains.

Where we use the term 'intelligence service' in the discussion of case law, it can refer to all sorts of agencies as discussed in this paragraph. Nevertheless, our analysis and the formulated standards in particular address oversight for intelligence services that intercept electronic communications on national territories as part of more general programs of surveillance (see paragraph 2.3).

B. Secret Surveillance and Data Collection

A recurring concept in the jurisprudence of the European Court of Human Rights is 'secret surveillance.' The Court characterizes this as measures of "surveillance the existence of which remains unknown to the persons being controlled."[8] In the Court's case law, 'secret surveillance' for example concerns tapping telephone conversations or 'metering' incoming and outgoing phone calls.[9] With the term 'data collection' we refer to the collection and storage of data by intelligence services, without the need for them to resort to secret measures, or without interfering with the secrecy of communications. For example, open-source intelligence (OSINT) is derived from information in the

8. Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R., ¶ 36 (Sept. 6, 1978), http://hudoc.echr.coe.int/eng?i=001-57510.

9. *See, e.g.*, *id.*; Malone v. United Kingdom, App. No. 8691/79, Eur. Ct. H.R. (Aug. 2, 1984), http://hudoc.echr.coe.int/eng?i=001-57533.

public domain, such as social media profiles, newspapers, and academic journals. Intelligence services also collect information by requesting (bulk) data from public and private entities, such as telecom providers, social services, and financial institutions. Naturally, secret data collection is a form of secret surveillance, but using both terms is useful to preserve some nuance in the discussion of the case law of the European Court of Human Rights.

C. Individual Surveillance and General Programs of Surveillance

In the case law of the Court, a distinction is made between 'individual surveillance' and 'general programs of surveillance.' The *Klass* case and the majority of cases afterwards concerned individual surveillance, which is the surveillance of specific persons. This is also denoted as 'targeted surveillance.' On the other hand, 'more general programmes of surveillance' are programs for bulk interception of the content of telecommunications and metadata. In German law and the literature, this is known as 'strategic surveillance,' but the Court uses the term 'strategic monitoring.' Strictly speaking, bulk interception is not the same as untargeted surveillance, since one could collect data in bulk of a (very broadly defined) target, for instance 'all inhabitants of the Netherlands.' We use 'individual' and 'targeted' versus 'strategic,' 'bulk,' and 'untargeted' interchangeably.

At the date of publication of the report on which this contribution is based, the Court discussed strategic surveillance only twice, in the *Weber and Saravia* case and in the *Liberty* case.[10] Two more cases on this issue are pending before the Court: *Big Brother Watch v. United Kingdom* revolves around strategic surveillance by the GCHQ revealed by Edward Snowden, and in *Zakharov v. Russia* the applicant complains of unrestricted interception of all telephone communications by the Russian Federal Security Service (FSB) without prior judicial authorization.[11] Furthermore, the Hungarian Eötvös Károly Institute has announced it will turn to the European Court of Human Rights now that the Hungarian Constitutional Court has rejected their complaint about the Act on the Police.[12] This Act allows secret surveillance and data collection based on a ministerial order, without a court warrant.[13]

D. Oversight, Control and Transparency

In this report, we use a broad definition of the term 'oversight' to include the various ways of holding the intelligence services accountable before the public

10. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. 309; Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (July 1, 2008), http://hudoc.echr.coe.int/eng?i=001-87207.

11. Big Brother Watch v. United Kingdom, App. No. 58170/13, Eur. Ct. H.R. (Jan. 9, 2014), http://hudoc.echr.coe.int/eng?i=001-140713; Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R. (Oct. 20, 2006), http://hudoc.echr.coe.int/eng?i=001-159324.

12. Szabó v. Hungary, App No. 37138/14, Eur. Ct. H.R. (Jan. 16, 2016), http://hudoc.echr.coe.int/eng?i=001-160020.

13. Statement of Facts, Szabó v. Hungary, App No. 37138/14, Eur. Ct. H.R. (June 12, 2014), http://hudoc.echr.coe.int/eng?i=001-145320.

and the government: internal oversight by the responsible minister, parliamentary oversight, judicial oversight and external independent oversight. Oversight can focus on specific instances in which 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. We recognize the fact that third parties, including civil society and companies, are or can be involved in exercising oversight to some extent. Including them in this report would broaden the scope too much, although we address their role in the part on transparency.

We also use the term 'control,' which should be distinguished from 'oversight.' 'Control' is usually associated with the executive branch, and it includes the power to manage and direct an intelligence service. It is performed by the intelligence service over itself and/or by the responsible minister (including his staff). The entity exercising control could also exercise internal oversight. Although it is important that control and internal oversight processes are in place, they cannot be considered to be substitutes for *external* and *independent* oversight.

Oversight can be applied at three moments: when the surveillance is first ordered and authorized, while it is being carried out, and after it has been terminated. The European Court of Human Rights makes this distinction in the context of Articles 8 and 13 of the Convention.[14] In this report, we refer to these moments of intervention as 'prior' oversight, 'ongoing' oversight, and oversight 'after the fact' respectively. In this context, prior oversight means that a minister, judge, or independent body approves the use of surveillance against an individual, although the use of a method itself can also be subject to oversight, in addition to its application. It is highly uncommon that parliamentary committees perform prior oversight. Ongoing intervention allows for the suspension of surveillance if it is no longer necessary, or if it is performed in violation of the law. Oversight after the fact refers to the possibility of having certain practices declared (un)lawful, and to provide for remedies. It could focus on whether authorizations have been granted lawfully (formalities and substantive requirements), whether the measures have been implemented properly, and/or the overall functioning of the system. The term 'oversight powers' denotes the institutional competences and legal powers that oversight bodies are equipped with in order to perform their task. For example, an independent oversight commission can be entrusted to oversee certain aspects of the work of intelligence services, and to do so it can be empowered to request specific information from intelligence agencies.

Finally, we use a broad concept of 'transparency' in this report. In the context of the current debate, what first comes to mind are the transparency reports issued by telecommunication providers and companies delivering 'over-the-top'

14. With regard to Article 8, see Klass, *supra* note 8, at ¶ 55, and with regard to Article 13, see *Ekimdzhiev*, ¶ 99 (June 28, 2007), http://hudoc.echr.coe.int/eng?i=001-81323.

Internet services. Such reports are a tool to give the public some insight in the scope of secret surveillance and data collection and allow for a further assessment of the lawfulness and effectiveness of measures. However, it should be acknowledged that transparency, i.e. openness, is important at multiple levels and in different relations, for instance at the level of the judiciary, or in the relation between intelligence services and parliamentary oversight committees or forms of independent oversight. All of these institutions can contribute to transparency by reports, hearings and investigations. We will use this meaning of transparency in this report.

II. OVERSIGHT OF INTELLIGENCE SERVICES

In this report, we focus on oversight of the intelligence services in the context of the European Convention of Human Rights (the 'Convention') and the Charter of Fundamental Rights of the European Union (the 'Charter'). In this section, we analyze the relevant rights and jurisprudence regarding oversight in a thematic way. We discuss transparency in the next section.

A. Interference with Human Rights

Privacy and data protection in conjunction with the right to an effective remedy are the most relevant human rights issues related to the topic of this report. However, other rights, such as the freedom of expression and the freedom of assembly and association, can be affected too.

The right to privacy is set out in Article 8, first paragraph, of the Convention and Article 7 of the Charter. For those articles to apply, it should be established first that there is an *interference* with (or in the case of the Charter, *limitation of*) the right to privacy. For the sake of completeness, we first have to discuss under what circumstances such interference occurs.

The performance of secret surveillance and data collection, as well as the mere existence of legislation providing for such powers, interferes with Article 8 of the Convention according to the European Court of Human Rights.[15] The Court reads a right to data protection into the right to privacy. It finds that the collection, analysis, and dissemination of data relating to an individual's private life amounts to an interference within the meaning of Article 8 of the Convention.[16] It is irrelevant for the Court whether this concerns sensitive information, whether the applicants have been inconvenienced as a result of the use of the data, or whether the information has ever been consulted by a third party.[17] In fact, the Court established that the dissemination of data to and their use by

15. Klass, *supra* note 8, at ¶ 47; Malone, *supra* note 9, at ¶ 64; Weber v. Germany, 2006-XI Eur. Ct. H.R. 309, 331-332.

16. Leander v. Sweden, App. No. 9248/81, Eur. Ct. H.R., ¶ 48 (Mar. 26, 1987), http://hudoc.echr.coe.int/eng?i=001-57519; Amann v. Switzerland, 2000-II Eur. Ct. H.R. 245, 269; Rotaru v. Romania, 2000-V Eur. Ct. H.R. 109, 128.

17. *Amann*, 2000-II Eur. Ct. H.R. at 282.

other authorities constitutes a *further separate* interference.[18] Similarly, the Court of Justice of the European Union found that the obligation to retain data relating to a person's private life and to his communications constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.[19] It also found that access of the competent national authorities to the data constitutes a *further* interference with this right.[20] Such retention and access constitutes the processing of personal data and is therefore also subject to the right to protection of personal data, which is protected by Article 8 of the Charter as a separate fundamental right.[21] Like the ECtHR, the CJEU found that it does not matter whether the information is sensitive or whether the persons concerned have been inconvenienced in any way.[22] In any case, in so far as the Charter contains rights that correspond to rights guaranteed by the Convention, the meaning and scope of those rights shall be the same as those laid down by the Convention.[23] The European Court of Human Rights takes the view that even public information can fall within the scope of private life where it is systematically or permanently collected and stored in files held by the national authorities. This is the case in particular where the information concerns a person's distant past.[24] It is exactly for this reason "that files gathered by security services on a particular individual fall within the scope of Article 8 [of the Convention], even where the information has not been gathered by any intrusive or covert method."[25] It is also for this reason that we distinguish between 'secret surveillance' and 'data collection' (see above).

Once we have established that most surveillance and data collection by intelligence services will give rise to an interference, the next step is to see if the interference is justified. According to Article 8, second paragraph, of the Convention, any interference by public authorities with exercising the right to privacy should be: a) in accordance with the law; b) in pursuit of a legitimate aim (e.g. national security); and c) necessary in a democratic society for the pursuit of this aim. We will refer to 'in accordance with the law' as the 'legality' or 'lawfulness' requirement in line with literature on this topic. The requirement of a legitimate aim is more of a formal character, since the Court hardly ever doubts that an interference is in the interest of national security or law enforce-

18. *Weber*, 2006-XI Eur. Ct. H.R. at 332.

19. *Digital Rights Ireland*, *supra* note 5, at ¶ 34.

20. *Id.* at ¶ 35.

21. *Id.* at ¶ 36.

22. Österreichischer Rundfunk v. Austria, App. No. 35841/02, Eur. Ct. H.R., ¶ 75 (Dec. 7, 2006), http://hudoc.echr.coe.int/eng?i=001-78381; *Digital Rights Ireland*, *supra* note 5, at ¶ 33.

23. Charter of Fundamental Rights of the European Union, art. 53(3), Dec. 7, 2000, 55 O.J. 391 (entered into force Dec. 1, 2009).

24. *Rotaru*, 2000-V Eur. Ct. H.R. at 128; M.M. v. United Kingdom, App. No. 24029/07, Eur. Ct. H.R., ¶ 187 (Nov. 13, 2012), http://hudoc.echr.coe.int/eng?i=001-114517.

25. P.G. v. United Kingdom, 2001-IX Eur. Ct. H.R. 195, 218.

ment.[26] The Court will consider an interference to be 'necessary in a democratic society,' if it answers a pressing social need, is proportionate to the legitimate aim pursued, and if the reasons adduced by the government to justify it are relevant and sufficient.[27] The necessity requirement often boils down to a proportionality analysis. In the Court's approach, the *existence* of oversight normally is assessed under the heading of legality, whereas the *functioning* of such oversight is a question of necessity.[28] However, where the Court concludes that interference is not in accordance with the law, it will not proceed to examine aim and necessity.[29] It turns out that in the majority of cases, secret surveillance or data collection was not 'in accordance with the law,' due to unclear surveillance powers or a simple lack of regulation.

The Charter provides for a general limitation clause that resembles the logic of the limitation clauses in the Convention. Article 52, first paragraph, provides that any limitation on the exercise of the rights and freedoms recognized by the Charter must: a) be provided for by law; b) genuinely meet objectives of general interest or the need to protect the rights of others; c) be necessary (subject to the principle of proportionality); and d) respect the essence of the rights and freedom recognized by the Charter. Just like the ECtHR, the Court of Justice of the European Union has accepted without much discussion that measures introduced to fight international terrorism satisfied an objective of general interest.[30] Furthermore, the CJEU determined that the competent national authority has the task of proving that national security would in fact be compromised: "There is no presumption that the reasons invoked by a national authority exist and are valid."[31]

As noted, secret surveillance and data collection also affect the right to an effective remedy. Article 13 of the Convention establishes the right to an effective (domestic) remedy for the violation of a Convention right: "Everyone whose rights and freedoms as set forth in the Convention are violated, shall have an effective remedy before a national authority [. . .]." This right is also

---

26. Nevertheless, in the more recent cases of *Iordachi v. Moldova*, App. No. 25198/02, Eur. Ct. H.R. (Sept. 14, 2009), http://hudoc.echr.coe.int/eng?i=001-91245, and *Ekimdzhiev*, *supra* note 12, the Court is a bit more wary of the use of the term 'national security' in domestic law.

27. Handyside v. United Kingdom, App. No. 5493/72, Eur. Ct. H.R., ¶ 48-50 (Dec. 7, 1976), http://hudoc.echr.coe.int/eng?i=001-57499; Gillow v. United Kingdom, App. No. 9063/80, Eur. Ct. H.R., ¶ 55 (Nov. 24, 1986), http://hudoc.echr.coe.int/eng?i=001-57493; *Leander*, *supra* note 14, at ¶ 58. *See also* S. v. United Kingdom, 2008-V Eur. Ct. H.R. 167, 202.

28. Cameron 2005, p. 221. However, in at least two cases the Court also verified whether shortcomings in a legal system (such as a lack of formal oversight) had an impact on the actual operation of the system of secret surveillance. If statistical information showed that the system of secret surveillance was overused, the Court reasoned that this might in part be due to the shortcomings in the law, with the effect that interference had not been "in accordance with the law." *See Ekimdzhiev*, *supra* note 12, at ¶ 92-93; Iordachi, *supra* note 24, at ¶ 52-53.

29. *See, e.g.*, *Malone*, *supra* note 9, at ¶ 82.

30. *See, e.g.*, Kadi v. Council and Commission, ECLI:EU:C:2008:461, § 363; Al-Aqsa v. Council, ECLI:EU:C:2012:711, § 123; *Digital Rights Ireland*, *supra* note 5, at ¶ 42-44.

31. *ZZ*, *supra* note 6, at ¶ 61.

recognized in Article 47 of the Charter. In the context of immigration cases, the European Court of Human Rights stated that, given the overlap between the procedural safeguards under Articles 8 and 13, the former should be interpreted in a manner consistent with the latter.[32] It appears that the same holds true for Articles 8 and 13 in the context of secret surveillance and data collection.

B. The Margin of Appreciation

Traditionally, the European Court of Human Rights has accorded states a fairly wide margin of appreciation in the context of national security.[33] It fits in with the doctrine of the Court that this margin can be reduced, for example when the Court sees growing consensus between Member States on a particular topic or certain changes in society. In the *S. and Marper* case, the applicants complained that the permanent storage of their fingerprints, cellular samples and DNA profiles in a police database was a violation of their right to privacy.[34] The Court considered that the protection of personal data is of fundamental importance for the right to respect for private and family life. In reference to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the Court stated that "domestic law must afford appropriate safeguards to prevent any" use of personal data that would be a violation of the right to privacy.[35] The Court found the need for safeguards even greater where the personal data undergo automatic processing, especially when such data are used for police purposes,[36] and it noted strong consensus among the Convention parties to balance the competing public and individual interests carefully. Furthermore, the Court observed that "the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."[37]

---

32. I.R. and G.T. v. United Kingdom, App. Nos. 14876/12, 63339/12, Eur. Ct. H.R. ¶ 62 (Jan. 28, 2014), http://hudoc.echr.coe.int/eng?i=001-141330. In *Lambert v. France*, the Court considered the lack of an 'effective' remedy to challenge telephone tapping a violation of Article 8. App. No. 23618/94, Eur. Ct. H.R., ¶¶ 31-40 (Aug. 24, 1998), http://hudoc.echr.coe.int/eng?i=001-58219.

33. *Klass*, *supra* note 8, at ¶ 59; *Leander*, *supra* note 14, at ¶ 59; L. v. Norway, App. No. 13564/88, Eur. Ct. H.R. (June 8, 1990), http://hudoc.echr.coe.int/eng?i=001-718; Esbester v. United Kingdom, App. No. 18601/91, Eur. Ct. H.R. (Apr. 2, 1993), http://hudoc.echr.coe.int/eng?i=001-1537; Christie v. United Kingdom, App. No. 21482/93, Eur. Ct. H.R. (June 27, 1994), http://hudoc.echr.coe.int/eng?i=001-1870; Segerstedt-Wiberg v. Sweden, 2006-VII Eur. Ct. H.R. 87, 118; *Weber*, 2006-XI Eur. Ct. H.R. at 338.

34. *S.*, 2008-V Eur. Ct. H.R. at 174.

35. *Id.* at 203. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data was drawn up within the Council of Europe and opened for signature in Strasbourg on 28 January 1981 (Convention 108). It was supplemented with the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, opened for signature in Strasbourg on 8 November 2001 (Convention 181).

36. *S.*, 2008-V Eur. Ct. H.R. at 203; *see also Digital Rights Ireland*, *supra* note 5, at ¶ 55.

37. *S.*, 2008-V Eur. Ct. H.R. at 205.

These factors narrowed the margin of appreciation left to the respondent state.[38] As to the facts of the case, the Court concluded that the respondent state had failed to strike a fair balance and that there had been a violation of Article 8.[39]

The position of the Court was more recently confirmed by sweeping considerations on technological developments and oversight in *M.M. v. United Kingdom*.[40] In this case, the Court further develops the line of reasoning set out in the *S. and Marper* case. The applicant received a caution for child abduction, and the government refused to delete it from the police records after the retention time had lapsed. She complained in Strasbourg about the retention and disclosure of her caution data, in particular about the fact that it would be retained for life. The Court recalled previous surveillance cases and considered

> it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules [. . .]. There are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data. At each stage, appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments and prevent arbitrary and disproportionate interference with Article 8 rights must be in place.[41]

It added that "the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data."[42]

Another factor that militates in favor of a small margin of appreciation is when interference is particularly far-reaching. In the case of *Bernh Larsen Holding v. Norway* for example, a Norwegian tax office obtained all existing documents on a server, regardless of their relevance for tax assessment purposes,[43] and in *M.K. v. France* data was retained for twenty-five years.[44]

Finally, it can be argued that the state's margin of appreciation also depends on the risk or actual evidence of abuse or arbitrary use of surveillance powers. In the admissibility decision of *Remmers v. Netherlands*, the Commission considered that:

---

38. *Id.*; *see also Klass*, *supra* note 8, at ¶ 48, in which the Court took note of the technical advances made in the means of espionage and surveillance, and Khelili v. Switzerland, § 62.

39. *S.*, 2008-V Eur. Ct. H.R. at 208-209.

40. *See M.M.*, *supra* note 22.

41. *Id.* at ¶ 195.

42. *Id.* at ¶ 200.

43. Bernh Larsen Holding v. Norway, App. No. 24117/08, Eur. Ct. H.R., ¶¶ 159, 163 (Mar. 14, 2013), http://hudoc.echr.coe.int/eng?i=001-117133.

44. M.K. v. France, App. No. 19522/09, Eur. Ct. H.R., ¶¶ 42-43 (Apr. 18, 2013), http://hudoc.echr.coe.int/eng?i=001-119075.

> as regards the compatibility of rules on secret surveillance with Article 8, the Court has accepted that the possibility of improper action by a negligent official can never be completely ruled out whatever the system. Relevant for the purposes of Article 8 of the Convention are the *likelihood of such action* and the safeguards provided to protect against it" [emphasis added].[45]

In the absence of any evidence or indication that the actual practice followed is otherwise, the Court will assume that the intelligence services comply with the law.[46]

In its recent judgment in *Digital Rights Ireland*, the reasoning of the CJEU confirmed much of the case law of the ECtHR of prior decades in the field of surveillance, even though the disputed measure related to law enforcement. The judgment was given in joint cases of requests for a preliminary ruling from Ireland and Austria. Essentially, the referring courts were asking the CJEU to examine the validity of the Data Retention Directive – under which telecom providers are held to store traffic data in bulk for a period of 6 to 24 months – under Articles 7 and 8 of the Charter.

Echoing the ECtHR considerations on the margin of appreciation, the CJEU found that the discretion of EU legislature was limited, because of the extent and the seriousness of interference resulting from the disputed Directive.[47] In this respect, it was a relevant factor that the Directive covered, "in a generalised manner, all persons and all means of electronic communications as well as traffic data, without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime."[48]

Now that the stage has been set, we need to know which standards for oversight can be derived from the Court's jurisprudence.

C. Adequate and Effective Guarantees Against Abuse

The recurring central theme in all relevant case law is that powers of secret surveillance should be accompanied with adequate and effective guarantees against abuse of these powers. Oversight is one of the elements required to prevent such abuse, according to the Court.

The Court establishes the 'adequate and effective guarantee' criterion in the *Klass* case, one of its very first surveillance cases. Five German citizens complained that the Act on Restrictions on the Secrecy of the Mail, Post and Telecommunications of 1968 (the 'G 10') on phone interception interfered with their right to private life and correspondence. The Court found that the *mere*

45. Remmers v. Netherlands, App. No. 29839/86, Eur. Ct. H.R. (May 18, 1998), http://hudoc.echr.coe.int/eng?i=001-4258.

46. *Klass*, *supra* note 8, at ¶ 59; *see also Esbester*, *supra* note 31*;* Kennedy v. United Kingdom, App. No. 26839/05, Eur. Ct. H.R. ¶ 168 (May 18, 2010), http://hudoc.echr.coe.int/eng?i=001-98473.

47. *Digital Rights Ireland*, *supra* note 5, at ¶ 48.

48. *Id.* at ¶ 57.

existence of the legislation itself constituted interference.[49] In assessing whether this interference was justified by the terms of Article 8, second paragraph, the Court considered that powers of secret surveillance of citizens are tolerable under the Convention only in so far as *strictly necessary* for safeguarding the democratic institutions.[50] The Court of Justice of the European Union also takes the view that limitations to the right to respect for private life should be strictly necessary.[51] Notwithstanding the respondent state's margin of appreciation,[52] the ECtHR stated that "whatever system of secret surveillance is adopted, there [must] exist adequate and effective guarantees against abuse."[53] In the *Klass* case and a couple of subsequent cases, the Court considered the 'adequate and effective guarantees' criterion in the context of the necessity requirement.[54] In later cases, the Court tended to examine such guarantees as part of the legality requirement.[55]

However, most recently the Court appeared to apply this test again under the necessity requirement. In *Dragojević v. Croatia*, the Court stated that this criterion "in particular bears significance as to the question whether an interference was 'necessary in a democratic society' [. . .], since powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions."[56] If the Court examines oversight of secret surveillance under the necessity heading, it will determine whether the procedures for supervising the ordering and implementation of the surveillance measures are such as to keep the interference to what is "necessary in a democratic society."[57] For that matter, the fact that "the values of a democratic society must be followed as faithfully in the supervisory procedures if the bounds of necessity, within the meaning of Article 8, second paragraph, are not to be exceeded" is used as a guiding principle.[58] In this

49. *Klass*, *supra* note 8, at ¶ 41.

50. *Id.* at ¶ 42; *see also Rotaru*, 2000-V Eur. Ct. H.R. at 130, Segerstedt-Wiberg, 2006-VII Eur. Ct. H.R. 118; Volokhy v. Ukraine, App. No. 23543/02, Eur. Ct. H.R., ¶ 43 (Nov. 2, 2006), http://hudoc.echr.coe.int/eng?i=001-77837; *Kennedy*, *supra* note 44, at ¶ 153; Dragojević v. Croatia, App. No. 68955/11, Eur. Ct. H.R., ¶ 84 (Apr. 15, 2015), http://hudoc.echr.coe.int/eng?i=001-150298.

51. *Digital Rights Ireland*, *supra* note 5, at ¶ 52; *see also* Case C-473/12, Institut professionnel des agents immobiliers (IPI) v. Englebert, 2013 E.C.R. 715, ¶ 39.

52. *Klass*, *supra* note 8, at ¶ 49.

53. *Id.* at ¶ 50.

54. *See Klass*, *supra* note 8, at ¶ 48-49; *Leander*, *supra* note 14, at ¶ 60; *L.*, *supra* note 31, at ¶ 2; Esbester, *supra* note 31; Hewitt v. United Kingdom, 14 Eur. Comm'n H.R. Dec. & Rep. 657 (1992); *Lambert*, *supra* note 30, at ¶ 31; *eWeber*, 2006-XI Eur. Ct. H.R. at 338; *Kennedy*, *supra* note 44, at ¶ 153.

55. *Ekimdzhiev*, *supra* note 12, at ¶ 77; Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 22; Sefilyan v. Armenia, App. No. 22491/08, Eur. Ct. H.R., ¶ 127 (Oct. 2, 2012), http://hudoc.echr.coe.int/eng?i=001-113296.

56. *Dragojević*, *supra* note 48, at ¶ 84.

57. *Id.*; *see also Klass*, *supra* note 8, at ¶ 54; *Lambert*, *supra* note 30, at ¶ 31; Kvasnica v. Slovakia, App No. 72094/01, Eur. Ct. H.R., ¶ 80 (June 9, 2009), http://hudoc.echr.coe.int/eng?i=001-92879; *Kennedy*, *supra* note 44, at ¶ 154.

58. *Dragojević*, *supra* note 48, at ¶ 84.

connection, the Court consistently refers to the rule of law as being one of the fundamental values of a democratic society.[59] The question to be answered is then how the supervisory procedures can follow the values of a democratic society faithfully.

D. Judicial, Parliamentary, and Independent Oversight

One important factor relates to the bodies performing oversight. Another important factor relates to the moment oversight is performed. The European Court of Human Rights takes a holistic approach to this topic. In the *Klass* case, the Court stated that the 'adequate and effective guarantees against abuse' criterion of Article 8 of the Convention depends on the type of surveillance at issue, the requirements for a surveillance order, the authorities competent to authorize, carry out, and supervise such measures, and the kind of remedy provided for by the national law.[60] In its assessment, the Court adds up all the guarantees, safeguards, and remedies as provided for by the national legal system, before issuing a final determination on the system's compatibility with the Convention.[61] However, as the following sections show, the Court finds certain forms of oversight preferable and other forms even unacceptable in the light of this assessment.

1. Prior Judicial Oversight

Without any doubt, the Court considers it 'desirable' to entrust oversight on secret surveillance to a judge. In the *Klass* case, dated 1978, the Court had already considered: "In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."[62] The Court tied this consideration to the principle of the rule of law. This principle implies that an interference by the national authorities should be subject to "effective control." "Such oversight should normally be assured by the judiciary, at least in the last resort," because judicial oversight provides the "best guarantees of independence, impartiality and a proper procedure."[63]

---

59. *See id.*; *Klass*, *supra* note 8, at ¶ 55; *Lambert*, *supra* note 30, at ¶ 31; *Rotaru*, 2000-V Eur. Ct. H.R. at 132; Brinks v. Netherlands, App. No. 9940/04, Eur. Ct. H.R., ¶ 1 (Apr. 5, 2005), http://hudoc.echr.coe.int/eng?i=001-68816; *Volokhy*, *supra* note 48, at ¶ 52; *Kvasnica*, *supra* note 54, at ¶ 80; *Kennedy*, *supra* note 44, at ¶ 154.

60. *Klass*,*supra* note 8, at 50; *see also* Mersch v. Luxembourg, 43 Eur. Comm'n H.R. DR 34 (1985); *L.*, *supra* note 31; *Ekimdzhiev*, *supra* note 12, at ¶ 77; *Weber*, 2006-XI Eur. Ct. H.R. at 338; *Kennedy*, *supra* note 44, at ¶ 153; *Uzun*, 2010-VI Eur. Ct. H.R. at 22; Shimovolos v. Russia, App. No. 30194/09, Eur. Ct. H.R., ¶ 68 (June 21, 2006), http://hudoc.echr.coe.int/eng?i=001-105217; *Sefilyan*, *supra* note 52, at ¶ 127; *Dragojević*, *supra* note 48, at ¶ 84.

61. *See also* CAMERON, *supra* note 4, at 126-127.

62. *Klass*, *supra* note 8, at ¶ 56; *see also Kennedy*, *supra* note 44, at ¶ 167; Telegraaf Media v. Netherlands, App. No. 39315/06, Eur. Ct. H.R., ¶ 98 (Nov. 22, 2012), http://hudoc.echr.coe.int/eng?i=001-114439.

63. *Klass*, *supra* note 8, at ¶ 55; *see also Brinks*, *supra* note 57, at ¶ 1; *Rotaru*, 2000-V Eur. Ct. H.R. at 132; *Volokhy*, *supra* note 48, at ¶ 52.

2. Alternatives to Prior Judicial Oversight

In the *Klass* case, the Court accepted the exclusion of prior and ongoing judicial oversight, on the condition that "the [supervisory] procedures established themselves provide adequate and equivalent guarantees safeguarding the individual's rights."[64] The German system satisfied this criterion. It encompassed internal control, parliamentary oversight, independent oversight, and a complaint procedure before an independent body. Only a Federal Minister or the highest authority of one of the *Länder* could order surveillance measures. The minister was bound to provide the independent G 10 Commission (*G 10-Komission*) every month with an account of the measures he had ordered, before such measures were actually implemented. He could however, order the execution of the measure before having informed the Commission if there was a risk that a delay might frustrate the purpose of the measure. This meant that except in urgent cases, the minister obtained prior approval of the Commission. Furthermore, an official qualified for judicial office supervised the implementation of the measures ordered.[65] The Parliamentary Supervisory Board (*Parlamentarische Kontrollgremium*, PKGr) performed after-the-fact oversight. The competent minister had to report to the Board on the application of the G 10 at least once every six months, which enabled the Board to oversee the overall performance of the system.[66] The Court noted that the Parliamentary Supervisory Board and the G 10 Commission enjoyed sufficient independence of the authorities carrying out the surveillance, and were vested with sufficient powers and competences to exercise effective and continuous oversight. In particular, the Court noted that "the democratic character [was] reflected in the balanced membership of the Parliamentary Board," since the opposition was represented. Lastly, the Court noted that an individual who believed himself to be under surveillance had the right to complain to the G 10 Commission, and – when such complaint was without success – to seek recourse from the Constitutional Court. The Court concluded that the exclusion of prior and ongoing judicial oversight did not exceed the limits of "what may be deemed necessary in a democratic society."[67] In coming to this conclusion, it attached particular weight to the independence it assumed the supervisory bodies enjoyed.

The Court again endorsed this system in 2006, about three decades later. In the admissibility decision of *Weber and Saravia v. Germany*, two German citizens complained that the amended G 10 Act violated their right to respect for privacy. They alleged that the scope of the Federal Intelligence Service's power

64. *Klass*, *supra* note 8, at ¶ 55.

65. One could object that the 'qualification to hold judicial office' does not ensure independence. At least, in the context of Article 6 the Court has a narrower notion of when a court or tribunal is "independent." *See* Volkov v. Ukraine, App. No. 21722/11, Eur. Ct. H.R. (May 27, 2013), http://hudoc.echr.coe.int/eng?i=001-115871.

66. *Klass*, *supra* note 8, at ¶¶ 18-21, 23, 56; *Weber*, 2006-XI Eur. Ct. H.R. at 319-320, 327-328, 340.

67. *Klass*, *supra* note 8, at ¶ 56. As regards after-the-fact judicial oversight, this is a matter of subsequent notification and will be discussed in the section on transparency.

(*Bundesnachrichtendienst*, BND) to carry out strategic surveillance under the amended G 10 Act was far too wide.[68] Again the Court asked whether there were 'adequate and effective guarantees against abuse' in place.[69] The Court observed that the system of oversight approved in the *Klass* case essentially remained the same, and it saw no reason to reach a different conclusion about it in the present case.[70] The *Weber and Saravia* case thus shows that the Court imposes the same standards of oversight for targeted and strategic surveillance.

Leander v. Sweden, a case that followed soon after *Klass*, offers another example of a system in which 'adequate and effective guarantees against abuse' were in place,[71] even though prior judicial oversight was lacking in the Swedish system at that time. Mr. Leander was rejected for a government job after he had failed a personnel screening procedure. In Sweden, a special police service was responsible for the prevention and detection of offenses against national security, and they had intelligence powers for these purposes. The security department (the Security Police) within the National Police Board (*Rikspolisstyrelsen*) kept a secret police register in which it could enter information necessary for the special police service. The National Police Board released information about Mr. Leander from the secret police register to the government, for use in the personnel screening procedure.

The Swedish system made no mention of judicial oversight, yet it did provide for internal control by the Minister of Justice, parliamentary oversight, independent oversight, and the right to file complaints before an independent body. The Court attached particular importance to the presence of parliamentarians on the National Police Board and noted that this group included members of the opposition. In the view of the Court, the parliamentarians' direct and regular oversight with regard to the most important aspect of the register – the release of information – provided a major safeguard against abuse.[72] In addition, the Court noted that the Parliamentary Standing Committee on Justice (*riksdagens justitieutskott*) regularly scrutinized the activities of the Security Police, and that the Parliamentary Ombudsman (*justitieombudsmännen*) performed oversight.[73] Furthermore, the Chancellor of Justice (*justitiekanslerns*), a traditional Swedish institute, was tasked with supervising the public authorities and their employees in order to ensure that they exercised their powers in compliance with the law.[74] The Court acknowledged that in some matters the Chancellor was not independent of the government. However, the Court observed that the Swedish Parliament

68. *Weber*, 2006-XI Eur. Ct. H.R. at 339.
69. *Id.* at 338.
70. *Id.* at 341.
71. *Leander*, *supra* note 14, at ¶ 60.
72. *Id.* at ¶ 65. "Direct and regular" refers to the fact that the parliamentarians participated in all decisions regarding whether or not information should be released, and that each of them was vested with a right of veto. *Id.i; see also Klass*, *supra* note 8, at ¶ 56; *c.f. Ekimdzhiev*, *supra* note 12, at ¶ 87.
73. *Leander*, *supra* note 14, at ¶ 65.
74. *See id.* at ¶ 36.

(*riksdag*) had given the Chancellor his mandate to supervise the functioning of the personnel screening system, so that in practice, he did act independently of the government.[75] Lastly, the Court noted that the Chancellor of Justice and the Parliamentary Ombudsman could receive and examine complaints from individuals.[76] The Court concluded that the Swedish system for security vetting met the requirements of Article 8, second paragraph.[77]

As in the *Klass* case and the *Weber and Saravia* case, the Court again had to assess the Swedish system about three decades later and reached the same conclusion. In the case of *Segerstedt-Wiberg v. Sweden,* five Swedish nationals requested access to their records contained in the secret police register. A few applicants had their request refused and other applicants were allowed to inspect some records. Together they complained in Strasbourg about both the continued storage and the refusal to provide full access to their records. After the *Leander* case, the Records Board (*Registernämnden*) had replaced the National Police Board to monitor compliance with the Police Data Act, and the independent Data Inspection Board (*Datainspektionen*) had been introduced to monitor compliance with the more general Personal Data Act. The latter had the authority to receive complaints from individuals,[78] and in order to carry out its oversight function it had access to the personal data that was being processed, to additional information, and to the premises where the processing took place.[79] In regard to this, and to its findings in the *Leander* case, the Court deemed it established that the system met the requirement of Article 8, second paragraph.[80]

More recently, in *Kennedy v. the United Kingdom*, the Court concluded that the British system for secret surveillance, contained "adequate and effective guarantees against abuse."[81] Mr. Kennedy complained that the British regimen of intercepting internal communications on a targeted basis, established under the Regulation of Investigatory Powers Act 2000 (RIPA), did not comply with Article 8, second paragraph, of the Convention. As in the *Klass* case, the applicant could claim to be a victim of interference for the mere fact that RIPA existed.[82] Of course, the Court took into account the type of surveillance at issue,[83] the procedures for a surveillance order,[84] and the oversight mechanisms. As regards oversight of the RIPA regime, the Court observed that apart from internal control by ministers, the Interception of Communications Commis-

75. *Id.* at ¶ 65.
76. *Id.* at ¶¶ 36, 38.
77. *Id.* at ¶ 67. Nevertheless, Cameron points out that those oversight bodies approved by the Court were later shown to be ineffective. CAMERON, *supra* note 4, at 229-234.
78. *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 112.
79. *Id.*
80. *Id.* at 123. Note that the Swedish oversight system was recently renewed in line with current oversight trends.
81. *Kennedy*, *supra* note 44, at ¶ 153.
82. *Id.* at ¶¶ 124-129.
83. *Id.* at ¶ 160.
84. *Id.* at ¶¶ 159-164.

sioner as well as the Investigatory Powers Tribunal (IPT) exercised after-the-fact oversight. The Commissioner oversaw the overall functioning of the surveillance system and the authorization of interception orders in specific cases. The Court noted that the Commissioner was independent of the executive and the legislature and held or had held a high judicial office.[85] Furthermore, the Court was impressed by the role of the IPT.[86] The Court highlighted the "extensive jurisdiction of the IPT to examine any complaint of unlawful interception."[87] Any person who suspected that his communications had been or were being intercepted could apply to the tribunal. Therefore, the jurisdiction of the IPT did not depend on notification, and the Court marked this as an advantage over the German system. The Court emphasized "that the IPT was an independent and impartial body, which [had] adopted its own rules of procedure."[88] The members of the tribunal had to hold, or had previously held, high judicial offices or had to be experienced lawyers.[89] In regard to the procedures as well as to the safeguards offered by the supervision of the Commissioner and the review of the IPT, the Court concluded that interference was justified under Article 8, second paragraph.[90]

3. The Body Issuing Authorizations

Without any doubt, "the body issuing authorizations for interception should be independent and . . . there must be either judicial [oversight] or [oversight] by an independent body over the issuing body's activity," as the Court stressed in *Iordachi v. Moldova*.[91] This statement refers to *Dumitru Popescu v. Romania (No. 2)*.[92] A public prosecutor had ordered the Romanian intelligence services to intercept Mr. Popescu's telephone conversations. After the applicant had been arrested, he was found guilty in particular on the basis of this material. Mr. Popescu complained in Strasbourg that he had been convicted on the basis of unlawful evidence. In its assessment under Article 8, the Court noted that authorization of the telephone tapping had been left to the power of the public prosecutor, a body known not to be independent of the Romanian executive

85. *Id.* at ¶ 166.

86. *Id.* at ¶ 167. Note that many commentators are highly critical of the IPT. In its ruling of 5 December 2014 for example, it rejected complaints against TEMPORA, finding this program not to be in contravention of Articles 8 and 10 of the Convention. *See* Liberty v. Gov't Commc'ns Headquarters [2014] UKIPTrib 13/77/H (UK).

87. *Kennedy*, *supra* note 44, at ¶ 167.

88. *Id.*

89. *Id.*

90. *Id.* at ¶ 169; see also *Esbester*, *supra* note 31, and *Christie*, *supra* note 31, in which the Commission found oversight by the IPT in combination with the Commissioner to be sufficient. Nevertheless, in the latter the Commission did note that "the possibility of review by a court of involvement of Parliamentarians in supervision would furnish additional independent safeguards to the system." *Christie*, *supra* note 31, at ¶ 15.

91. *Iordachi*, *supra* note 24, at ¶ 40.

92. *Id.* at ¶¶ 70-71; Popescu v. Romania, App. No. 71525/01, Eur. Ct. H. R. (July 26, 2007), http://hudoc.echr.coe.int/eng?i=001-80352.

branch.[93] In a previous case against Romania, the Court had already found that the decisions of the public prosecutor could not be challenged before an independent and impartial judicial body, but rather only before the hierarchically higher superior prosecutor.[94] Therefore, authorization for telephone tapping was not subject to prior oversight by a judge or other independent body, either at their own initiative or after a complaint of the person concerned.[95]

4. After-the-Fact Oversight on the Authorization and the Overall Performance of the System

In the *Dumitru Popescu* case, the Court noted that there was no meaningful after-the-fact judicial oversight on the authorization process[96] because the law made it impossible for the Romanian court hearing the criminal charges against Mr. Popescu to review the validity of the authorization given by the prosecutor. This court had thus limited itself to reviewing compliance with the formalities for the actual interception.[97] In view of the Court, the theoretical possibility for an individual to complain before a parliamentary committee could not make up for the lack of prior and after-the-fact judicial oversight on the authorization procedure, since the person concerned had not been notified of the surveillance, and the parliamentary committee was not competent anyway to sanction unlawful surveillance.[98] There had been a violation of Article 8.[99]

The Court also holds the opinion that there has to be independent ongoing or after-the-fact oversight on the overall functioning of a system of secret surveillance and data collection. In *Ekimdzhiev v. Bulgaria*,[100] the applicants complained about the Bulgarian Special Surveillance Means Act (SSMA), referring to Article 8 of the Convention. They alleged it gave the intelligence services a broad power to use secret surveillance, and it failed to provide adequate and effective guarantees against abuse. The Court found that prior oversight on the authorization procedure provided sufficient safeguards.[101] However, the Court was not content with the oversight for the later stages. It noted that the SSMA did not provide for ongoing or after-the-fact oversight by an independent body that verified whether the intelligence services in fact complied with the warrants for authorizing the use of surveillance, whether they faithfully reproduced the original data in the written record, or whether the original data was in fact

93. *Popescu*, *supra* note 90, at ¶¶ 70-71; *see also Uzun*, § 72.

94. Rupa v. Romania, App. No. 58478/00, Eur. Ct. H.R. (Mar. 16, 2009), http://hudoc.echr.coe.int/eng?i=001-90222; *see also Popescu*, *supra* note 90, at ¶ 72.

95. *Popescu*, *supra* note 90, at ¶ 73.

96. *Id.* at ¶ 74.

97. *Id.* at ¶ 76.

98. *Id.* at ¶ 77; *see also* Ass'n '21 December 1989' v. Romania, App. No. 33810/07, Eur. Ct. H.R., ¶ 120 (May 24, 2011), http://hudoc.echr.coe.int/eng?i=001-104864.

99. *Popescu*, *supra* note 90, at ¶ 86; *see also* Bălteanu v. Romania, App. No. 142/04, Eur. Ct. H.R., ¶¶ 42-46 (July 16, 2013), http://hudoc.echr.coe.int/eng?i=001-122361.

100. *Ekimdzhiev*, *supra* note 12.

101. *Id.* at ¶ 84.

destroyed if the law provided for this.[102] On the contrary, these activities were all carried out by the Ministry of Internal Affairs.[103] The Court further noted that the overall control over the system of secret surveillance was also entrusted solely to the responsible minister, not to independent bodies.[104] The Court concluded that there had been a violation of Article 8.

Finally, the CJEU denounced that, under the Directive, access by the national authorities to the data retained was "not made dependent on a prior review carried out by a court or by an independent administrative body."[105] This comment has already found its way to national jurisprudence.

5. Prior and After-the-Fact Opportunities for the Individual

The Court's case law on the right to an effective remedy in particular stresses the fact that individual rights protection requires independent oversight after the fact on the lawfulness of measures of secret surveillance and data collection applied to an individual. Such oversight can exist in a complaint procedure. In the *Klass* case, the very fact that individuals believing themselves to be under surveillance had the opportunity to complain to the G 10 Commission and to the Constitutional Court and that they had recourse to various courts once they had been notified, ensured that the system satisfied the requirements of Article 13 of the Convention.[106] Similarly, in the *Leander* case the fact that individuals could complain before the Chancellor of Justice and the Parliamentary Ombudsman, that there was parliamentary oversight on individual cases, and that the entire Cabinet of the Government had looked into Mr. Leander's complaints, provided sufficient evidence that Article 13 had been complied with – although none of these remedies would be 'effective' on their own.[107] In the *Ekimdzhiev* case, the Court denounced that as a result of a lack of notification, "those concerned [were] unable to seek any redress in respect of the use of secret surveillance measures against them."[108] Moreover, the Bulgarian government had not provided its citizens with any information on remedies that could become available to the persons concerned.[109]

What is more, the *Ekimdzhiev* case signals that the Court is progressing towards an adversary principle for prior oversight proceedings. The Court found it obvious that when surveillance is ordered and while it is under way, i.e. when prior and ongoing oversight takes place, notification of the persons concerned is not possible, since such notification would jeopardize national security. The Court held that the persons concerned were therefore of necessity deprived of

102. *Id.* at ¶ 85.
103. *Id.*
104. *Id.* at ¶ 87.
105. *Digital Rights Ireland*, *supra* note 5, at ¶ 62.
106. *Klass*, *supra* note 8, at ¶¶ 70-72.
107. *Leander*, *supra* note 14, at ¶¶ 81-84.
108. *Ekimdzhiev*, *supra* note 12, at ¶ 101.
109. *Id.* at ¶ 102.

the possibility to challenge specific measures ordered or implemented against them. However, the Court considered that "this does not mean it is altogether impossible to provide a limited remedy – for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage."[110] As an example the Court referred to the *Klass* case, where individuals *believing* themselves to be under surveillance could file a complaint.[111] The Court concluded that Article 13 had been violated.

In the context of deportation cases for the purpose of protecting national security, the Court reads the right to 'some form of adversarial proceedings' into Article 8 of the Convention. The case of *Al-Nashif v. Bulgaria* concerned a father of two who was deported from Bulgarian territory on national security grounds.[112] Under Bulgarian law, an order concerning a matter of national security was not subject to judicial review. The father and his children complained that there had been arbitrary interference with their right to respect for their family life contrary to Article 8 of the Convention. The Court recalled classic surveillance cases such as *Klass*, *Amann*, and *Rotaru*[113] in that "there must be safeguards to ensure that the discretion left to the executive is exercised in accordance with the law and without abuse."[114] Furthermore, the Court inferred from the cases mentioned that:

> even where national security is at stake, the concepts of lawfulness and the rule of law in a democratic society require that measures affecting fundamental human rights must be subject to some form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence, if need be with appropriate procedural limitations on the use of classified information.[115]

This meant that the individual had to be able to challenge the government's assertion that national security is at stake, and that the independent body had to be able to review the government's interpretation of "national security."[116] The Court noted that under Bulgarian law the Ministry of the Interior was empowered to issue deportation orders without following any form of adversarial procedure, without giving any reasons, and without any possibility for appeal to an independent authority, and concluded there had been a violation of Article 8.[117]

---

110. *Id.* at ¶ 100.
111. *Id.*
112. Al-Nashif v. Bulgaria, App. No. 50963/99, Eur. Ct. H.R. (Sept. 20, 2002), http://hudoc.echr.coe.int/eng?i=001-60522.
113. *Id.* at ¶ 119.
114. *Id.* at ¶ 122.
115. *Id.* at ¶ 123.
116. *Id.* at ¶ 124.
117. *Id.* at ¶ 128.

E. Independence of the Authorities Carrying Out Surveillance

Regardless of the particular organization of oversight, one thing that becomes clear from the jurisprudence on the right to privacy is that there should be at least some form of 'independent' oversight on the lawfulness of the surveillance. To determine whether a body is independent, the European Court of Human Rights examines how the body exercises its functions, whether it acts upon its own rules, how its members are appointed, or if its independence is guaranteed in any other way.

For the purpose of Article 8 of the Convention, 'independent' oversight means independence of the intelligence services and the executive branch. In the *Klass* and *Weber* cases, the Court noted that the G 10 commissioners were completely independent in the exercise of their functions and could not be subject to instructions. Furthermore, the Commission drew up its own rules of procedure. Additionally, the members of the Parliamentary Board were appointed by parliament itself in proportion to the parliamentary groupings, the opposition being represented on the Board.[118] The Court concluded that the "Parliamentary Board and the G 10 Commission [were] independent of the authorities that carried out the surveillance,"[119] and it found no breach of Article 8.[120] Similarly, in the *Kennedy* case the Court expressly noted that the Interception of Communications Commissioner was independent of the executive and the legislature,[121] and it emphasized that the Investigatory Powers Tribunal was an independent and impartial body, which had adopted its own rules of procedure.[122] Another way to ensure independent oversight is by a way of a constitutional provision. In the *Segerstedt-Wiberg* case, the Court observed that the independence of the Records Board and the Data Inspection Board was guaranteed, *inter alia*, by the Swedish Constitution, which provided that neither Parliament nor the government could interfere with the manner in which the Boards oversaw particular cases.[123]

By contrast, in the *Dumitru Popesco* case the Court recalled that the Romanian Minister of Justice supervised all the members of the general prosecutor's department.[124] Since the public prosecutor – who oversaw telephone tapping – acted as a member of this department, it was not independent of the executive branch.[125] The Court found a violation of Article 8.[126] In *Commission v. Germany*, the Court of Justice of the European Union established that "in

118. *Klass*, *supra* note 8, at ¶ 21; *Weber*, 2006-XI Eur. Ct. H.R. at 341.
119. *Klass*, *supra* note 8, at ¶ 56.
120. *Id.* at ¶ 60.
121. *Kennedy*, *supra* note 44, at ¶ 166.
122. *Id.* at ¶ 167.
123. *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 11-112; *see also Leander*, *supra* note 14, at ¶ 36.
124. *Popescu*, *supra* note 90.
125. *Id.* at ¶¶ 70-71.
126. *Id.*; *see also Iordachi*, *supra* note 24, at ¶ 40; *Uzun*, 2010-VI Eur. Ct. H.R. at 24-25; *Ekimdzhiev*, *supra* note 12; *P.G.*, 2001-IX Eur. Ct. H.R. 195. *Khan v. United Kingdom* confirmed that 'independence' means the same for the purposes of Article 13. 2000-V Eur. Ct. H.R. 279, 296. In *M.M.*,

relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure."[127] It involves the lack of any instructions relating to the performance of their duties, so 'independence' does not concern exclusively the relationship between the supervisory authorities and the bodies subject to this supervision.[128] In *Commission v. Austria*, the CJEU added that 'functional independence,' where the respective party is not bound by instructions in the performance of its duties, is not by itself sufficient to protect a supervisory authority from all external influence.[129] For instance, the attribution of the necessary equipment and staff to supervisory authorities must not prevent them from acting independently,[130] and, at least in the context of the Data Protection Directive, the supervisory authorities and their decisions should remain above all suspicion of political partiality.[131]

F. Powers for Effective Oversight

The cases discussed above (*Klass*, *Weber and Saravia*, *Leander*, *Segerstedt-Wiberg* and *Kennedy*) contain clues on the particular powers an oversight body should have in the light of the Convention.

Most importantly, it can be induced from the Court's case law on Article 8 of the Convention that prior and ongoing oversight bodies should have the power to prevent or end a surveillance measure and to order the removal of personal data. As noted earlier, in the *Klass* case the Court attached importance to the fact that the Parliamentary Supervisory Board and the G 10 Commission were vested with sufficient powers to exercise effective oversight.[132] This conclusion was based on the fact that if the G 10 Commission declared any measures to be illegal or unnecessary, the Minister had to 'terminate' them immediately.[133] Similarly, in the *Leander* case the Court highlighted that each member of Parliament on the Swedish National Police Board was vested with a right of veto, the exercise of which automatically prevented the Board from releasing information to the Swedish government.[134] The Court explicitly re-approved both systems thirty years later in *Weber and Saravia* and *Segerstedt-Wiberg* respectively (under Article 8, but, as will be set out below, *Segerstedt-Wiberg*

---

supra note 22, at ¶ 206, the Court stressed the importance of independent review of a decision to retain or disclose data.

127. Case C-518-07, Comm'n v. Germany, 2010 E.C.R I-1897, 1908.

128. *Id.* at 1908, 1910.

129. Case C-614/10, Comm'n v. Austria, ECLI:EU:C:2012:631, ¶ 42 (Oct. 16, 2012); *see also* Case C-288/12, Comm'n v. Hungary, ECLI:EU:C:2013:816, ¶ 51 (Dec. 10, 2013).

130. *Comm'n v. Austria*, *supra* note 127, at ¶ 58.

131. *Id.* at ¶ 52.

132. *Klass*, *supra* note 8, at ¶ 56.

133. *Id.* at ¶¶ 21, 53.

134. *Leander*, *supra* note 14, at ¶ 65.

did not survive scrutiny under Article 13).[135] In the *Kennedy* case, the Court endorsed the fact that the IPT could, *inter alia*, quash any interception order, cancel a surveillance warrant and require the destruction of any records obtained under a surveillance warrant.[136]

Finally, in *S. and Marper* the Court disapproved of the fact that an acquitted individual had only limited possibilities to have the data removed from the national database or the materials destroyed.[137] Not only does the right to privacy require that authorities tasked with oversight are actually in a position to do something about surveillance measures, but, according to the Court, it also follows from the right to an effective remedy, protected by Article 13 of the Convention, that oversight bodies should be able to issue legally binding decisions against intelligence services. In the view of the Court in the *Klass* case, the 'authority' referred to in Article 13 is not necessarily a judicial authority in the strict sense; the main question is whether the powers are actually effective: "The powers and procedural guarantees an authority possesses, are relevant in determining whether the remedy [. . .] is effective."[138]

Meanwhile, the Court is mindful of limits to oversight potentially present in the context of national security: "An 'effective remedy' under Article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance."[139] Building on these considerations, the Court noted in the *Leander* case that the main weakness of the oversight afforded by the Parliamentary Ombudsman and the Chancellor of Justice was that both lacked the power to render a legally binding decision.[140] However, the Court observed that the opinions of the Ombudsman and the Chancellor commanded by tradition great respect in Swedish society and were usually followed in practice.[141] The Court also found it important that the Parliamentary members of the Swedish National Police Board considered each case where release of information was requested, in respect of which each of them was vested with a right of veto.[142] In the end, the Court concluded there was no violation of Article 13.[143]

However, the Swedish system that was approved in the *Leander* case was considered a violation of Article 13 of the Convention in the case of *Segerstedt-Wiberg*. This development in the case law can be explained by the fact that the principles of data protection had found their way into the Convention. In the

135. *See Weber*, 2006-XI Eur. Ct. H.R. 309; Segerstedt-Wiberg v. Sweden, 2006-VII Eur. Ct. H.R. 87.

136. *Kennedy*, *supra* note 44, at ¶¶ 80, 167; *see also Mersch*, *supra* note 58, at ¶ 118.

137. *S.*, 2008-V Eur. Ct. H.R. at 207.

138. *Klass*, *supra* note 8, at ¶ 67; *Leander*, *supra* note 14, at ¶ 77; *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 126.

139. *Klass*, *supra* note 8, at ¶ 69.

140. *Leander*, *supra* note 14, at ¶ 82.

141. *Id.* at ¶¶ 82, 37-38.

142. *Id.* at ¶¶ 82, 65.

143. *Id.* at ¶ 84.

Segerstedt-Wiberg case, the applicants complained that no effective remedy existed and in particular that they could not have their files destroyed.[144] The Court noted that the Records Board had "no competence to order the destruction of files or the erasure or rectification of information kept in the files."[145] In addition, the Court found it unproven that the Data Inspection Board, which in theory had the power to order a processor to stop processing the information other than for storage, functioned effectively in practice.[146] Individuals furthermore "had no direct access to any legal remedy as regards the erasure of the information" that had been released to them.[147] In the view of the Court, these shortcomings were not set off by any possibilities for the applicants to seek compensation, so the system was not consistent with Article 13.[148]

III. TRANSPARENCY OF INTELLIGENCE SERVICES

The European Court of Human Rights recognizes the fact that for an individual to exercise his or her right to privacy and freedom of expression, a certain degree of transparency is essential, even though the Court hardly ever explicitly mentions the term 'transparency' as such in its decisions on secret surveillance and data collection. In several instances, however, the Court points to the lack of 'public scrutiny' of interference with the right to privacy. This notion captures the importance of transparency. In addition, case law regarding the legality requirement of Article 8 underlines the need for transparency, notwithstanding the fact that the Court is not insensitive to the argument that publication of information about secret surveillance might reveal the working methods and fields of operation of the intelligence services and even possibly identify their agents.[149]

A. The Regulation of Intelligence Services

From the requirement that any interference with the right to privacy should be 'in accordance with the law' it follows that the scope of powers of secret surveillance and data collection should be transparent. The Strasbourg Court established this in *Malone v. the United Kingdom*. Mr. Malone complained that the police tapped and metered his telephone. With respect to the foreseeability condition that is contained in the legality requirement, the Court held that this could not mean that an individual should be able to foresee exactly *when* the authorities will use secret surveillance against him.[150] Nevertheless, the Court found the law must be sufficiently clear to give citizens an indication as to the

144. *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 93.
145. *Id.* at 127.
146. *Id.* at 127-128.
147. *Id.* at 128.
148. *Id.*
149. *See, e.g.*, *Klass*, *supra* note 8, at ¶ 55.
150. *Malone*, *supra* note 9, at ¶ 67.

circumstances in which and the conditions on which public authorities are empowered to resort to any measures of secret surveillance and the collection of the data.[151] Moreover, the Court determined that, since the implementation of secret surveillance is not open to 'public scrutiny,' it should be the law – as opposed to accompanying administrative practice – that indicates the scope of powers, to give the individual adequate protection against arbitrary interference.[152]

Parallel to this, the CJEU held that EU legislation for the retention of data should lay down clear and precise rules governing the scope and application of the measure and impose minimum safeguards so that the persons concerned are protected against the risk of abuse and against unlawful access and use of this data.[153] This condition was further worked out in *Liberty and Others v. the United Kingdom*. Liberty and two other civil liberties organizations complained that the existence of the Interception of Communications Act 1985 (IOCA), which provided for strategic monitoring of external communications, interfered with their right to privacy. The applicants contended that the law was not foreseeable, as the examination, use, storage, dissemination, and destruction of intercepted data were regulated in secret 'arrangements.'[154] In response, the government argued that publication of these procedures might damage the efficacy of the surveillance or give rise to a security risk.[155] First of all, the Court did "not consider there was any ground to apply different principles concerning the accessibility and clarity of the rules governing" individual and general surveillance.[156] Moreover, the Court observed that in Germany details about such procedures for strategic surveillance were public.[157] For that matter, the Investigatory Powers Tribunal (IPT) in the United Kingdom had also made public details about the rules to be observed for interception warrants. In the view of the Court, those examples suggested that "it is possible for a State to make public certain details about the operations of a scheme of external

151. *Id.*; *see also Weber*, 2006-VII Eur. Ct. H.R. at 335; *Ekimdzhiev*, *supra* note 12, at ¶ 75; *Uzun*, 2010-VI Eur. Ct. H.R. at 21; *Telegraaf Media*, *supra* note 60, at, ¶ 90. '. . . and the collection of data' was added only recently in *Shimovolos v. Russia*, App. No. 30194/09, Eur. Ct. H.R., ¶ 68 (June 21, 2011), http://hudoc.echr.coe.int/eng?i=001-105217.

152. *Malone*, *supra* note 9, at ¶ 68; *see also* Halford v. United Kingdom, App. No. 20605/92, Eur. Ct. H.R., ¶ 49 (June 25, 1997), http://hudoc.echr.coe.int/eng?i=001-58039; Kopp v. Switzerland, App. No. 23224/94, Eur. Ct. H.R., ¶ 64 (Mar. 25, 1998), http://hudoc.echr.coe.int/eng?i=001-58144; Copland v. United Kingdom, 2007-I Eur. Ct. H.R. 317, 329-330; Huvig v. France, App. No. 11105/84, Eur. Ct. H.R., ¶ 29 (Apr. 24, 1990), http://hudoc.echr.coe.int/eng?i=001-57627; Kruslin v. France, App. No. 11801/85, Eur. Ct. H.R., ¶ 30 (Apr. 24, 1990), http://hudoc.echr.coe.int/eng?i=001-57626; Remmers v. Netherlands, App. No. 29839/86, Eur. Ct. H.R. (May 18, 1998), http://hudoc.echr.coe.int/eng?i=001-4258; *Weber*, 2006-XI Eur. Ct. H.R. at 335-336; *S.*, 2008-V Eur. Ct. H.R. at 201; *Telegraaf Media*, *supra* note 60, at ¶ 90.

153. *Digital Rights Ireland*, *supra* note 5, at ¶ 54.

154. *Liberty*, *supra* note 10, at ¶¶ 45, 60.

155. *Id.* at ¶ 68.

156. *Id.* at ¶ 63.

157. *Id.* at ¶ 45.

surveillance without compromising national security."[158] The strategic surveillance had not been in accordance with the law.[159]

Statute law should indicate the procedures as well as existing mechanisms of oversight on secret surveillance and data collection. In *Shimovolos v. Russia*, the applicant complained with reference to Article 8 about the registration of his name in a so-called Russian 'Surveillance Database' (*Сторожевой контроль*) and the collection of personal data about him by the police. This database was linked to the databases of Russian railway and airline companies, so that whenever any of the persons listed bought a train or airplane ticket an automatic notification was sent to the police. In its assessment of the legality requirement, the Court recalled the *Liberty* case and added that statute law should also set out which authorities would be competent to permit, carry out and supervise the possible surveillance measures, and the kind of remedy provided for by national law.[160] In this case, a ministerial order governed the creation and maintenance of the Surveillance Database as well as the procedure for its operation.[161] This order was not published and was not accessible to the public.[162] The Court noted that as a result, neither the procedures nor the existing controls and guarantees against abuse were open to public scrutiny.[163] It concluded that interference had not been in accordance with the law.[164]

B. Notification

Transparency is a means to ensure accountability to the public at large, but in the context of secret surveillance and data collection it is also important for the reasons set out in the current and the next section. To begin with, an individual cannot challenge retrospectively the legality of the measures taken against him before a court, unless he is notified of the surveillance once the measure has ended, or otherwise learns of it (for example by a leak). Lack of notification thus hinders after-the-fact oversight, and has been discussed incidentally in the case law of the European Court of Human Rights in this context. The Court of Justice of the European Union has pointed out another disadvantage of not notifying (or not allowing third parties to notify), namely that this "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[165] First in the *Klass* case and then in the *Weber and Saravia* case, the Court inferred from the necessity require-

158. *Id.* at ¶ 68.
159. *Id.* at ¶ 69.
160. *Shimovolos*, *supra* note 58, at ¶ 68.
161. *Id.* at ¶ 60.
162. *Id.* at ¶¶ 60, 62.
163. *Id.* at ¶ 69.
164. *Id.* at ¶ 70; *see also Ekimdzhiev*, *supra* note 12, at ¶ 88; Hadzhiev v. Bulgaria, App. No. 22373/04, Eur. Ct. H.R., ¶¶ 45-47 (Oct. 23, 2012), http://hudoc.echr.coe.int/eng?i=001-114076; Savovi v. Bulgaria, App. No. 7222/05, Eur. Ct. H.R., ¶¶ 56-59 (Nov. 27, 2012), http://hudoc.echr.coe.int/eng?i=001-114767.
165. *Digital Rights Ireland*, *supra* note 5, at ¶ 37.

ment the condition that "as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should [. . .] be provided to the persons concerned."[166] In both cases, German law indeed provided for this, and this rendered after-the-fact judicial oversight possible.

As the *Klass* case concerned individual surveillance and the *Weber and Saravia* case concerned general programs of surveillance, it is apparent that the Court does not set different notification requirements for the two types of surveillance. Furthermore, in the *Weber and Saravia* case the Court also approvingly noted that the Federal Constitutional Court "prevent[ed] the duty of notification from being circumvented" (namely, if data was destroyed within three months without notification, this was only justified where the data had not been used before), and that the independent "G 10 Commission had the power to decide whether an individual being monitored had to be notified."[167] This all contributed to keeping interference resulting from the surveillance within the limits of what was necessary to achieve the legitimate aim of protecting national security.[168]

The Court also reads a notification condition into the right to an effective remedy. In principle, the Court finds that a lack of notification to the person concerned does not, of itself, entail a breach of Article 13.[169] Nevertheless, in the case of *Ekimdzhiev v. Bulgaria* the Court found a violation of Article 13, since Bulgarian law did not provide for notification at any point in time and under any circumstances. The Bulgarian Special Surveillance Means Act of 1997 (SSMA) provided that all persons who came across information about intelligence activities were under a duty not to disclose it. On the basis of this, the Bulgarian Supreme Administrative Court held that the refusal to provide information to a person on whether surveillance had been used against him was legitimate.[170] Furthermore, the Protection of Classified Information Act of 2002 (PICA) labelled information about special means of surveillance and intelligence obtained thereby as a state secret. Accordingly, the Supreme Administrative Court held that a refusal to inform a person of surveillance against him had been properly denied, because this information was a state secret.[171] Taking note of all this, the Court considered that Bulgarian law did not provide for notification of the persons concerned at any point in time and under any circumstances[172] and concluded that Article 13 had been violated.[173]

---

166. *Klass*, *supra* note 8, at ¶ 58; *Weber*, 2006-XI Eur. Ct. H.R. at 345; *see also Mersch*, *supra* note 58.

167. *Weber*, 2006-VII Eur. Ct. H.R. at 345.

168. *Id.*

169. *Klass*, *supra* note 8, at ¶ 69; *see also Leander*, *supra* note 14, at ¶ 78; *Mersch*, *supra* note 58. It should be noted that in making its decision the Court took into account the existence of a system of proper oversight.

170. *Ekimdzhiev*, *supra* note 12, at ¶ 49.

171. *Id.* at ¶ 50.

172. *Id.* at ¶ 101.

C. Access of Oversight Bodies to Information

Effective oversight requires that the oversight bodies themselves have access to relevant information, including information about specific operations and the personal data that is being processed.

The systems of secret surveillance and data collection in Germany, Sweden and the United Kingdom all guaranteed that the competent oversight bodies had access to information. As appears from the *Klass* and *Weber and Saravia* cases, the responsible minister for the intelligence services was bound by law to report on the application of the G 10 Act to the Parliamentary Board at least once every six months, and to provide the G 10 Commission every month with an account of the measures he had ordered.[174] Furthermore, a person who had unsuccessfully complained to the G 10 Commission could apply to the Constitutional Court. The Constitutional Court could request the Government to supply it with information or to produce documents. The authorities were bound to comply with such a request even if the information asked for was secret. It was then for the Constitutional Court to decide whether the information could be used in the complaint procedure.[175]

In order to carry out their oversight functions, the Swedish National Police Board/Records Board, the Chancellor of Justice, and the Parliamentary Ombudsman were entitled to have access to all files or other documents kept by the intelligence services. The services, as well as their employees, had to provide the oversight bodies with such information and reports as they requested. The Swedish Parliamentary Committee on Justice informed itself by holding hearings with spokesmen of the National Police Board and its Security Department as well as by regular visits. Members of the Committee had full access to the registers during their visits.[176] The Data Inspection Board was entitled to have access to the personal data being processed, to receive additional information pertaining to the processing of personal data and to access the premises where the processing took place.[177]

In the *Kennedy* case, the Court expressly endorsed the mechanism by which the British oversight bodies were provided with information. First of all, the Court considered it 'particularly important' that it was prescribed by law that intelligence services are to keep detailed records of interception warrants for which they had applied.[178] This ensured that the information needed by the oversight bodies would be available in the first place. With regard to this, the Court noted that both the Interception of Communications Commissioner and the IPT had access to all relevant documents, including closed materials, and

173. *Id.* at ¶ 103. The Court saw no reason to hold otherwise in *Hadzhiev*, *supra* note 97, at ¶¶ 53-56. For a similar case, see *Volokhy*, *supra* note 48.

174. *Klass*, *supra* note 8, at ¶ 53; *Weber*, 2006-VII Eur. Ct. H.R. at 320.

175. *Klass*, *supra* note 8, at ¶ 23.

176. *Leander*, *supra* note 14, at ¶ 36, 38, 40; *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 111.

177. *Segerstedt-Wiberg*, 2006-VII Eur. Ct. H.R. at 112.

178. *Kennedy*, *supra* note 44, at ¶ 165.

that all of those involved in intelligence activities had a duty to disclose to them any material they required.[179] In sum, those involved in carrying out secret surveillance had retention duties and those tasked with oversight had transparency entitlements. As to the facts of the case, the Court found the surveillance complained of justified.[180]

By contrast, in the *Ekimdzhiev* case the Court noted that the Bulgarian Special Surveillance Means Act of 1997 (SSMA) made no provision for acquainting the overseeing judge with the results of the surveillance.[181] This made his supervisory role irrelevant.

D. Positive Obligations Under the Right to Privacy

A right to access to information held by the government can be derived from the right to respect for private life and family life. This first represents the Court's view that transparency contributes to the realization of the individual's right to privacy. For example, in *Rotaru v. Romania* the Court held that storing personal information by a public authority, the use of it and the refusal to disclose this information to the person concerned amounted to interference with the right to respect for private life.[182] A stronger right to access to information can be found in cases where the government failed to ensure full access to files and was therefore in breach of a positive obligation flowing from the right to privacy. In the case of *Gaskin v. United Kingdom*, the applicant had been in the care of the Liverpool City Council in his youth.[183] The local authority had kept confidential records concerning him and his care. Mr. Gaskin claimed that the continuing lack of access to the whole of his case file held by the City Council was in breach of his right to respect for his private and family life under Article 8 of the Convention. The Court considered that, "as in the *Leander* case," there was a file "concerning details of Mr. Gaskin's personal history which he had no opportunity of examining in its entirety."[184] Accordingly, the Court found that the United Kingdom had not interfered with the applicant's private or family life but that it had "failed to act" by refusing him complete access to his case records.[185] The Court therefore examined whether the government was in breach of a positive obligation flowing from Article 8.

---

179. *Id.* at ¶¶ 166-167.

180. *Id.* at ¶ 169; *see also L.*, *supra* note 31 (the Court stressed multiple times that there was oversight by an independent Control Committee which could request all information necessary); *Amann*, 2000-II Eur. Ct. H.R. 245; *Rotaru*, 2000-V Eur. Ct. H.R. 109.

181. *Ekimdzhiev*, *supra* note 12, at ¶ 85; see also *Iordachi*, *supra* note 24, at ¶ 47, where the Court disapproved of the fact that Moldovan law made no provision for acquainting the overseeing judge with the results of the surveillance.

182. *Rotaru*, 2000-V Eur. Ct. H.R. at 129; *see also Halford*, *supra* note 150; *Lambert*, *supra* note 30; *Amann*, 2000-II Eur. Ct. H.R.; *Brinks*, *supra* note 57, at ¶ 1; *Telegraaf Media*, *supra* note 60.

183. Gaskin v. United Kingdom, App. No. 10454/83, Eur. Ct. H.R., ¶ 10 (July 7, 1989), http://hudoc.echr.coe.int/eng?i=001-57491.

184. *Id.* at ¶ 41.

185. *Id.*

In the proportionality requirement in Article 8, second paragraph, it is stipulated that an independent authority decides whether access to personal records has to be granted. In the *Gaskin* case, the Court weighed the "fair balance that has to be struck between the general interest of the community and the interests of the individual" to determine whether a positive obligation existed.[186] In the Court's opinion, persons in the situation of the applicant had an interest in receiving the information necessary to know and to understand their childhood and early development.[187] On the other hand, the Court considered that confidentiality of public records could be necessary for the efficacy of the system and for the protection of the contributors to the files.[188] In this respect, the Court found that the British system, which made access to records dependent on the contributor's consent, could "in principle be compatible with the [positive] obligations under Article 8."[189] However, the Court found that such a system will only be "in conformity with the principle of proportionality if it provides that an independent authority finally decides whether access has to be granted."[190] No such procedure was available, so there had been a breach of Article 8. Positive obligations under Article 8 also arise with regard to records created by intelligence services. In *Haralambie v. Romania*, the applicant alleged a violation of his right to privacy, because he was not granted access to the file made on him by the former intelligence services. The Court pointed out the relation between the issue and Convention 108.[191] The Court found the administrative procedure to access files ineffective, mainly because of unjustified delays.[192] In light of this, the Court found that the respondent state had not fulfilled its positive obligation to provide an effective and accessible procedure enabling the applicant to have access to all information.[193]

E. A Right to Access Information

In certain circumstances, citizens or legal entities can invoke a right to access information such as secret surveillance statistics, or information about unlawful activities of intelligence services.

To begin with, the Court has taken steps towards the recognition of a right of access to information contained in the right to freedom of expression, and it determined that both natural persons and legal entities could invoke such a right. The (non-surveillance) case of *Társaság a Szabadságjogokért v. Hungary*

186. *Id.* at ¶ 42.
187. *Id.* at ¶ 36.
188. *Id.* at ¶ 3.
189. *Id.* at ¶ 49.
190. *Id.* at ¶ 49; *see also* M.G. v. United Kingdom, App. No. 39393/98, Eur. Ct. H.R., ¶ 30 (Dec. 24, 2002), http://hudoc.echr.coe.int/eng?i=001-60642.
191. Haralambie v. Romania, App. No. 21737/03, Eur. Ct. H.R., ¶ 77 (Oct. 27, 2009), http://hudoc.echr.coe.int/eng?i=001-95302; *see also Amann*, 2000-II Eur. Ct. H.R. at 269; *Rotaru*, 2000-V Eur. Ct. H.R. at 128.
192. *Haralambie*, *supra* note 124, at ¶¶ 90-95.
193. *Id.* at ¶ 96.

gave the initial impetus. In this case, the Hungarian government had denied the Hungarian Civil Liberties Union access to information of public interest.[194] The association complained that the government's denial had constituted an infringement of its right to receive information of public interest, which was in breach of the right to freedom of expression. On the question whether there had been any interference, the Court recalled that it had consistently held that the public has a right to receive information of general interest, which is protected as part of press freedom.[195] However, the Court found that the creation of forums for public debate was not limited to the press, one of society's 'public watchdogs.'[196] It stated that an association could be characterized as a 'social watchdog,' where its activities are an "essential element of informed public debate."[197] Therefore, the activities of the Civil Liberties Union warranted similar Convention protection to that afforded to the press.[198]

The Court then fully recognized a right of access to information in *Youth Initiative for Human Rights v. Serbia*. Referring to Article 10 of the Convention, Youth Initiative for Human Rights complained that the intelligence agency of Serbia had refused to provide certain information, even though a body set up to ensure observance of the Freedom of Information Act 2004 had ordered that the information be made available to the applicant.[199] In its assessment, the Court stated that "the notion of 'freedom to receive information' embraces a right of access to information."[200]

In particular, Youth Initiative for Human Rights requested factual information about how many people had been subjected to electronic surveillance by the Serbian intelligence agency in 2005, and the Court found they had a right of access to this information. Referring to the *Társaság a Szabadságjogokért* case, the Court considered that the applicant NGO "was obviously involved in the legitimate gathering of information of public interest."[201] In this case, there had been a violation of Article 10, since the reluctance of the intelligence agency to comply with the order to make the information available was in defiance of domestic law and tantamount to arbitrariness.[202] Finally, the Court found, with reference to Article 46 of the Convention (binding force and implementation), that the best execution of its judgment would be to ensure that the intelligence agency of Serbia did provide the applicant with the information requested.[203]

---

194. Társaság a Szabadságjogokért v. Hungary, App. No. 37374/05, Eur. Ct. H.R., ¶ 3 (Apr. 14, 2009), http://hudoc.echr.coe.int/eng?i=001-92171.

195. *Id.* at ¶ 26.

196. *Id.* at ¶¶ 26-27.

197. *Id.* at ¶ 27.

198. *Id.*

199. Youth Initiative for Human Rights v. Serbia, App. No. 48135/06, Eur. Ct. H.R., ¶ 16 (June 25, 2013), http://hudoc.echr.coe.int/eng?i=001-120955.

200. *Id.* at ¶ 20.

201. *Id.* at ¶ 24.

202. *Id.* at ¶ 26.

203. *Id.* at ¶ 32.

The Court listed factors to determine the necessity of disclosing information about arbitrary interference and abuses by intelligence services. The applicant in *Bucur and Toma v. Romania* worked in the telephone interception department of a military unit of the Romanian Intelligence Service (RIS).[204] He was suspended for the fact that he gave a press conference disclosing that there were irregularities in the intelligence work and that a large number of journalists, politicians, and businessmen were tapped. The applicant complained in Strasbourg that his criminal conviction had interfered with his right to freedom of expression, in particular his right to impart information. The main issue before the Court was whether this interference was necessary in a democratic society. The Court recalled the factors regarding the protection of whistle-blowers who work in the public service, and found them useful for the case in hand: a) whether or not the applicant had other means of imparting the information; b) the public interest value of the information; c) the authenticity of the information; d) the damage done to the public authority as a result of the disclosure; and e) the good faith of the applicant.[205]

As to the second factor, the Court considered that the information disclosed was of public interest. The interception of telephone communications was particularly important in a society that had known close surveillance by the intelligence services during the communist regime. Moreover, the Court considered that civil society was directly affected by the information disclosed, since anyone's telephone calls might be intercepted.[206] The information the applicant disclosed related to abuses committed by high-ranking state officials and affected the democratic foundations of the state. For the Court there was no doubt that these were very important issues for the political debate in a democratic society, in which public opinion had a legitimate interest.[207] In this case, interference with its right to freedom of expression was not necessary in a democratic society.

CONCLUSION

In the previous two sections, we have analyzed European jurisprudence in order to develop recommendable standards for oversight and transparency of intelligence services that respect the human rights to privacy and freedom of expression.

Below, we list ten recommendable standards for oversight and transparency of intelligence services, especially in the context of communication interception using the sophisticated technologies now associated with untargeted surveillance. We base these on the jurisprudence (footnotes provide links to relevant

204. Bucur v. Romania, App. No. 40238/02, Eur. Ct. H.R., ¶ 7 (Jan. 8, 2013), http://hudoc.echr.coe.int/eng?i=001-115844.

205. *Id.* at ¶ 93.

206. *Id.* at ¶ 101.

207. *Id.* at ¶ 103.

paragraphs of the analysis in Section 3), our interpretation of it (including what can be regarded as best practices), and our expectations about the direction future case law might take. In order to substantiate our recommendations further, we draw from a selection of reports and soft law measures that have been issued in Europe and the United States.

These standards should be read in combination – one would not work without the other. For example, independence in oversight (Standard 3) will only be effective if oversight is supported by adequate resources (Standard 7).

Standard 1: Intelligence services need to be subject to oversight that is complete.

This means it should be complete in terms of:[208]

a) the oversight body: the government, parliament, the judiciary, and a specialized (non-parliamentary, independent) commission should all play a role in oversight;

b) the moment of oversight: prior oversight, ongoing oversight, and oversight after the fact;

c) the oversight bodies' mandate: review of lawfulness and effectiveness.

Disclosures in the media have demonstrated that there is a need for enhanced oversight,[209] even in countries where oversight appears to be quite comprehensive. The overall blend of oversight mechanisms for national intelligence services is important.[210] 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.[211] We deduct from the jurisprudence that both lawfulness and effectiveness are elements that can be addressed by the courts. Non-effective intrusive measures can fail the proportionality test.

208. *See* discussion *supra* Section II; Venice Commission 2007, *supra* note 3, at §§ 70, 72; Report on the U.S. NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, EUR. PARL. DOC. (COM 139) ¶ 16 (Feb. 21, 2014). Virtually all findings in this report are reflected in U.S. NSA surveillance program surveillance bodies in various Member States and impact on EU citizens' fundamental rights, EUR. PARL. DOC. (COM 230) §§ 21, 75 (2014) [hereinafter 12 March Resolution]. We only refer to the former separately where needed.

209. *See* discussion *supra* Section I; Committee on Legal Affairs and Human Rights, *Mass surveillance*, COUNCIL OF EUR. PARLIAMENTARY ASSEMBLY, Doc. No. 13734, § 114 (Mar. 18, 2015), https://ccdcoe.org/sites/default/files/documents/CoE-150318-MassSurveillanceReport.pdf. [hereinafter *Report on mass surveillance*]; EUR. PARL. ASS. RES. 2045(2015), *Mass surveillance*, § 13 (Apr. 21, 2015); 12 March Resolution, *supra* note 208, at § 9.

210. *See* discussion *supra* Section III.E; Venice Commission 2007, *supra* note 3, at § 79. All findings in this report are reinforced in Venice Commission 2015, *supra* note 3. We only refer to the latter separately where it contains additions to the original report.

211. *See* discussion *supra* Section III.C; Venice Commission 2007, *supra* note 3, at § 76.

Standard 2: Oversight should encompass all stages of the intelligence cycle.

Surveillance involves different stages, including the collection, storage, selection and analysis of data. As all these stages amount to interference with the right to privacy, these separate stages should be subject to oversight to a certain degree. In practice, this means that not only the collection and selection of surveillance measures should be subject to prior independent oversight, but also the analysis itself.

Standard 3: Oversight of the intelligence services should be independent.

In this context, this means independence of the intelligence services and the government.[212] Judicial oversight offers the best guarantees of independence.[213] Therefore, it is preferable to entrust oversight on secret surveillance and data collection to a judge, as is already the case in certain jurisdictions.[214] However, the independence of judicial-like bodies is not a given. For example, public prosecutors in most political systems cannot be regarded as independent of the government. Similarly, government ministers cannot provide for independent oversight, since they are part of the government that is also the tasking body and the customer of the intelligence services. The fact that some courts in the past 'rubber-stamped' decisions or took quite long in making a decision is not an argument against judicial oversight as such. This merely underlines that adequate resources are essential to guarantee the independence and effectiveness of oversight bodies (see Standard 7).

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. Furthermore, a standing parliamentary committee that specializes in intelligence services can also be regarded as independent if its members represent the ruling parties as well as the opposition, and the member's voting power does not depend on its parliamentary size. The dismissal procedure 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

212. *See* discussion *supra* Section III.E; Venice Commission 2007, *supra* note 3, at §§ 110, 205; 12 March Resolution, *supra* note 206, at § 79.

213. *See* discussion *supra* Section III.D.

214. Venice Commission 2007, *supra* note 3, at § 204; *Report on mass surveillance*, *supra* note 207, at §§ 113; 116; EUR. PARL. ASS. RES. 2045(2015), *Mass surveillance*, § 19.2 (Apr. 21, 2015); 12 March Resolution, *supra* note 208, at § 21.

specialized commission allows for greater expertise in oversight.[215]

To summarize: independence is reflected in several elements, including: a) transparent and objective procedures for the nomination of people, b) no governmental interference with the activities and decisions of the institution performing the oversight, c) effective powers (see Standards 4 and 5) and d) resources and budgetary independence (see Standard 7).

Standard 4: 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 for the application of surveillance and collection powers is essential.[216] Furthermore, the transfer of personal data to third countries requires prior consent by the competent supervisory authority.[217] 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 (see Standard 6).[218] In such a system, 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 unprecedented and 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 (see Standard 7). Political responsibility and optimizing the protection of fundamental rights are different topics.

Standard 5: Oversight bodies should be able to declare a measure unlawful and provide for redress.

Prior and ongoing oversight bodies 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 removal of personal data.[219] Obviously, oversight powers will only be effective if

215. Venice Commission 2007, *supra* note 3, at § 232.

216. Venice Commission 2007, *supra* note 3, at § 204; 12 March Resolution, *supra* note 208, at §§ 12, 75.

217. 12 March Resolution, *supra* note 208, at § 13.

218. *See* discussion *supra* Section III.D.

219. *See* discussion *supra* Section III.E.

combined with the power to make legally binding decisions which also provide for redress of the unlawfulness of a measure. Given the gravity of such decisions, the minister should simultaneously have the power to appeal against these before a court. Initial orders to conduct surveillance should contain sufficient reasoning to allow oversight bodies and appellate courts to evaluate the lawfulness of a measure.

Standard 6: Oversight should incorporate the adversary principle.

Where there is no prior judicial oversight, only oversight mechanisms that included a complaint procedure survived the Court's scrutiny under Article 8 of the Convention. In such a complaint 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 considered that it should be possible to provide for a prior remedy, for instance one where the proceedings are secret. In such considerations, the notion of 'some form of adversary proceedings' is implicit. Moreover, 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 jeopardzsing 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 courts to be in a better position to weigh the interests of the intelligence services against the interests of the public 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,[220] but in its 2015 update of the report it argues for the involvement of privacy advocates as regards searching data obtained by strategic surveillance.[221] One of the most important recommendations of the United States Privacy and Civil Liberties Oversight Board is in fact the establishment of special advocates before the FISA Court.[222]

Where there is no prior judicial oversight, only oversight mechanisms that included a complaint procedure survived the Court's scrutiny under Article 8 of the Convention. In such a complaint procedure, the individual concerned can

220. Venice Commission 2007, *supra* note 3, at §§ 215-216.

221. Venice Commission 2015, *supra* note 3, at § 17.

222. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 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 185 (Jan. 23, 2014) [hereinafter PCLOB 215 report]. The Board made similar findings in its REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014).

challenge the lawfulness of measures of secret surveillance and data collection directed against him after the fact.

Standard 7: Oversight bodies should have sufficient resources to perform effective oversight.

This includes the attribution of the necessary equipment and staff, resources in terms of information (see Standard 8) and technical expertise.[223] This contributes to them being independent of the intelligence services and the government (see Standard 3), and it is critical for oversight bodies to function effectively in practice. Without access to sufficient resources, oversight bodies cannot fulfill their mandate in a meaningful way.[224] 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.

Standard 8: Intelligence services and their oversight bodies should provide layered transparency.

This means that:

a) the individual concerned, the oversight bodies, and civil society are informed;

b) there is an adequate level of openness about intelligence activities prior to, and after the fact;

c) notification, aggregate statistics, working methods, classified and detailed information about operations, and general information about what will remain secret under all circumstances is provided.

Such an approach to transparency is essential to ensure that individuals can exercise their rights effectively, that oversight bodies can perform their tasks effectively, and that the public can hold their political representatives accountable. In sum, transparency contributes to oversight. States should not wait for leaks and unauthorized disclosures but instead ensure that everyone involved can access and receive the information necessary to perform the oversight related to their role, at a relevant time. A layered structure of transparency should be put in place. Such a structure would make the provisioning of information dependent on the level of confidentiality and/or aggregation. Such a layered system should be based on policies clearly laid down, rather than on arbitrary and unilateral decision-making.

223. *See* discussion *supra* Section III.E.

224. *Report on mass surveillance*, *supra* note 207, at § 101, Venice Commission 2007, *supra* note 3, at §§ 20-21, 165, 231; 12 March Resolution, *supra* note 208, at §§ 76, 79.

Standard 9: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance.

This standard more or less mirrors the previous one. From the requirement that all interference with the right to privacy should be 'in accordance with the law,' which includes the foreseeability condition, it follows that statute law should indicate the procedures for the use, dissemination, and destruction of intercepted data, as well as existing oversight mechanisms for secret surveillance and data collection. Clear legislation provides a framework for oversight and supports public scrutiny of the surveillance powers.[225] In fact, experience in some countries in Europe and the United States has demonstrated it is possible to disclose information about the collection, analysis, and dissemination of personal data without damage to national security.[226] Oversight bodies should have a right to access all (classified) information relevant for their task.[227] In support of this, intelligence services – and others involved in the value chain, i.e. including ministers/governmental bodies – should be obliged to keep detailed records and to disclose to oversight bodies any material requested.[228] Where an oversight body is competent to assess the effectiveness of intelligence services in executing government policy, access to operational details is necessary.[229] An oversight body of which the functions include reviewing questions of legality, effectiveness and respect for human rights will require access to even more specific information.[230] Furthermore, the publication of aggregate interception warrant numbers provides insight into the working methods of the intelligence services and supports public confidence in the judicial oversight mechanisms.[231] Publication of aggregated notification and non-notification figures also supports oversight by civil society.[232] Individual notification should be carried out as soon as possible without jeopardizing the purpose of the surveillance. This enables the individual to challenge any measure directed against him. Where an individual requests access to his intelligence file, an independent authority should finally decide whether access has to be granted.

Standard 10: Companies and other private legal entities involved in national surveillance should be able to impart information about their involvement.

Sharing information on the functioning of the intelligence services while not jeopardizing operations is necessary to support robust oversight by civil society. This means that organizations should be able to disclose publicly general information about orders they receive directing them to provide information to

225. Venice Commission 2015, *supra* note 3, at § 98.
226. PCLOB 215 report, *supra* note 220, at 196.
227. EUR. PARL. ASS. RES. 2045 (2015), *Mass surveillance*, § 19.2 (Apr. 21, 2015).
228. 12 March Resolution, *supra* note 208, at § 79.
229. Venice Commission 2007, *supra* note 3, at § 160.
230. Venice Commission 2007, *supra* note 3, at § 163.
231. EUR. PARL. ASS. RES. 2045 (2015), § 7; PCLOB 215 report, *supra* note 220, at 199-200.
232. Venice Commission 2015, *supra* note 3, at § 137.

the government. Such information might disclose the number of orders that providers have received, the broad categories of information produced, and the number of users whose information has been produced.[233] It also allows for the verification of information made available by the intelligence agencies. Organizations should further be able to make more detailed and possibly confidential information available to oversight bodies.

233. *See also* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECH., LIBERTY AND SECURITY IN A CHANGING WORLD (Dec. 12, 2013); PCLOB 215 report, *supra* note 220, at 204.