FREEDOMS

Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Mapping Member States' legal frameworks

FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

This report addresses matters related to the respect for private and family life (Article 7), the protection of personal data (Article 8) and the right to an effective remedy and a fair trial (Article 47) falling under Titles II 'Freedoms' and VI 'Justice' of the Charter of Fundamental Rights of the European Union.

Photo (cover & inside): © Shutterstock

More information on the European Union is available on the Internet (http://europa.eu).

FRA – European Union Agency for Fundamental Rights
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu – info@fra.europa.eu

Luxembourg: Publications Office of the European Union, 2015

Paper:	978-92-9491-225-1	10.2811/85028	TK-04-16-020-EN-C
PDF:	978-92-9491-224-4	10.2811/009038	TK-04-16-020-EN-N

Printed in Belgium

Printed on process chlorine-free recycled paper (PCF)

Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU

Mapping Member States' legal frameworks

Foreword

Protecting the public from genuine threats to security and safeguarding fundamental rights involves a delicate balance, and has become a particularly complex challenge in recent years. Terror attacks worldwide have triggered broad measures allowing intelligence services to cast ever-wider nets in the hope of preventing further violence. At the same time, the digital age has produced technological innovations facilitating large-scale communications data monitoring – which could easily be abused.

These developments affect a variety of fundamental rights protected by European Union (EU) law, particularly the rights to privacy and data protection – enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the EU treaties and EU directives.

The Snowden revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, highlight that violations of these rights are not merely a theoretical concern. The sheer magnitude of the uncovered intelligence activity has prompted disquiet and underscored the importance of maintaining effective mechanisms to help prevent fundamental rights encroachments. The European Parliament responded with a resolution which, among others, calls on the European Union Agency for Fundamental Rights to research thoroughly fundamental rights protection in the context of surveillance, in particular in terms of available remedies.

This report – which constitutes the first part of FRA's response to this request – aims to support the adoption and meaningful implementation of oversight mechanisms in the EU and its Member States. It does so by analysing the legal frameworks on surveillance in place in EU Member States, focusing on so-called 'mass surveillance', which carries a particularly high potential for abuse. The report does not assess the implementation of the respective laws; instead, it maps the relevant legal frameworks in the Member States. It also details oversight mechanisms introduced across the EU, outlines the work of entities tasked with overseeing surveillance measures, and presents the various remedies available to individuals seeking to challenge such intelligence activities.

The research findings presented in this report demonstrate the complex considerations involved in safeguarding fundamental rights in the context of surveillance. Finding a balance between national security protection and respect for fundamental rights is a challenge that requires thorough and candid discussion. This report contributes to that discussion.

Constantinos Manolopoulos
Director a. i.

Country codes

Code	EU Member State
AT	Austria
BE	Belgium
BG	Bulgaria
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
EL	Greece
ES	Spain
FI	Finland
FR	France
HR	Croatia
HU	Hungary
IE	Ireland
IT	Italy
LT	Lithuania
LU	Luxembourg
LV	Latvia
MT	Malta
NL	Netherlands
PL	Poland
PT	Portugal
RO	Romania
SE	Sweden
SK	Slovakia
SI	Slovenia
UK	United Kingdom

Contents

List of figures and tables

Introduction

Recent revelations of mass surveillance underscore the importance of mechanisms that help prevent fundamental rights violations in the context of intelligence activities. This FRA report aims to evaluate such mechanisms in place across the European Union (EU) by describing the current legal framework related to surveillance in the 28 EU Member States. The report first outlines how intelligence services are organised, describes the various forms surveillance measures can take and presents Member States' laws on surveillance. It then details oversight mechanisms introduced across the EU, outlines the work of entities set up thereunder, and presents various remedies available to individuals seeking to challenge surveillance efforts. The report does not assess the implementation of the respective laws, but maps current legal frameworks. In addition, it provides an overview of relevant fundamental rights standards, focusing on the rights to privacy and data protection.

Background

In June 2013, media worldwide began publishing the 'Snowden documents', describing in detail several surveillance programmes being carried out, including by the United States' National Security Agency (NSA) and by the United Kingdom's Government Communications Headquarters (GCHQ). These brought to light the existence of extensive global surveillance. Details of these programmes, which set up a global system of digital data interception and collection, have been widely publicised[1] and critically assessed.[2] Neither the US nor the British authorities questioned the authenticity of the revelations,[3] and in some cases confirmed them.[4] However, the media's interpretation of the programmes was sometimes contested – for example, by the UK Intelligence and Security Committee of Parliament [5] and academia.[6] Since most of the Snowden revelations have not been recognised by the British government, the Investigatory Powers Tribunal, in hearing challenges to the legality of the programmes, took the approach of hearing cases on the basis of hypothetical facts closely resembling those alleged by the media.[7] For the Austrian Federal Agency for State Protection and Counter Terrorism (BVT), the Snowden revelations represented a "paradigm shift": "Up until a few years ago, espionage was largely directed at state or business secrets, and not, for the most part, at people's privacy, which can now be interfered with extensively by intelligence services since they possess the necessary technical resources to do so". [8]

The Snowden revelations were not the first to hint at the existence of programmes of large-scale communication surveillance set up in the aftermath of the 11 September 2001 attacks.[9] But the magnitude of the revelations was unprecedented, potentially affecting the entire world. The revelations triggered an array of reactions.[10] In the intelligence community, and in particular among the specialised bodies in charge of overseeing the work of intelligence services, dedicated inquiries were conducted.[11] The European Union reacted strongly. The European Commission (EC), the Council of the European Union and the European Parliament (EP) reported on the revelations, expressing concern about mass surveillance programmes, seeking clarification from US authorities, and working on "rebuilding trust" in light of the damage created by the revelations.[12]

On 12 March 2014, the EP adopted a resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights, and transatlantic cooperation in Justice and Home Affairs (the Resolution).[13] The resolution drew on the in-depth inquiry that the EP tasked the Civil Liberties, Justice and Home Affairs Committee (LIBE) to conduct during the second half of 2013, shortly

1 See European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013a); European Union Agency for Fundamental Rights (FRA) (2014a); PACE, Committee on Legal Affairs and Human Rights (2015a); Vermeulen, M. (2014).
2 See, for example, France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014), p. 129 and following.
3 See Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (2014), p. 135. The Belgian oversight body has not yet found any indication that the slides revealed were not authentic, and would tend to conclude that they are truthful. See also Standing Committee I (2015), p. 11.
4 The Guardian (2013).
5 See United Kingdom, Intelligence and Security Committee of Parliament (2013).
6 Cayford, M. *et al.*, P. H. A. J. M. (2015), p. 646.
7 United Kingdom, Investigatory Powers Tribunal (2014/2015). The UK government adopted, for security reasons, a general policy of neither confirming nor denying allegations made in respect of surveillance activities in other cases. See also ECtHR, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008, para. 47.
8 Austria, Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*) (2014), p .57.
9 See, for example, European Parliament (2001); Chesterman, S. (2011); Lowenthal, M. (2015), p. 124.
10 Wright, D. and Kreissl, R. (2015).
11 See, for example, Germany, Federal Parliament (2013), p. 10 and following; Italy, COPASIR (2014), p. 18 and following; Belgium, Standing Committee I (2014), p. 132 and following; Belgium, Standing Committee I (2015), p. 8 and following, pp.67–68, and its recommendations, p. 115 and following; The Netherlands, CTIVD (2014a), p. 8 and following.
12 FRA (2014a), p. 81 and following; FRA (2015).
13 European Parliament (2014).

after the revelations on mass surveillance were published in the press.[14]

The wide-reaching resolution launched a "*European Digital Habeas Corpus*", aimed at protecting fundamental rights in a digital age while focusing on eight key actions. In this context, the EP called on the EU Agency for Fundamental Rights (FRA) "to undertake in-depth research on the protection of fundamental rights in the context of surveillance, and in particular on the current legal situation of EU citizens with regard to the judicial remedies available to them in relation to those practices".[15]

Scope of the analysis

This report constitutes the first step of FRA's response to the EP request. It provides an overview of the EU Member States' legal frameworks regarding surveillance. FRA will further consolidate its legal findings with fieldwork research providing data on the day-to-day implementation of the legal frameworks. A socio-legal report based on an empirical study, to be published at a later stage, will expand on the findings presented here.

While the EP requested the FRA to study the impact of 'surveillance' on fundamental rights, given the context in which the resolution was drafted, it is clear that 'mass surveillance' is the main focus of the Parliament's current work. During the data collection phase, FRA used the Parliament's definition to delineate the scope of Franet's research. The EP resolution refers to

> *"far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner" (Paragaph 1).*

This definition encompasses two essential aspects: first, a reference to a collection technique, and second, the distinction between targeted and untargeted collection.

The report does not analyse the surveillance techniques themselves, but rather the legal frameworks that enable these techniques. For Member States that carry out signals intelligence, the focus of the analysis is on this capacity, and not on other intrusive capabilities the services may have (such as wiretapping).

This report covers the work of intelligence services. It does not address the obligations of commercial entities which, willingly or not, provide intelligence services with the raw data that constitute Signals Intelligence (SIGINT), and are otherwise involved in the implementation of the surveillance programmes.[16] The private sector's role in surveillance requires a separate study.

While the premise of this report is the existence of an interference, since the "secret monitoring of communications" interferes with privacy rights from a fundamental rights point of view,[17] the report focuses on analysing the legal safeguards in place in the EU Member States' legal frameworks, and therefore on their approaches to upholding fundamental rights.

> *"Assuming therefore that there remains a legal right to respect for the privacy of digital communications (and this cannot be disputed (see General Assembly Resolution 68/167)), the adoption of mass surveillance technology undoubtedly impinges on the very essence of that right."*
>
> *UN, Human Rights Council, Emmerson, B. (2014), para. 18*

The report's analysis of EU Member States' legal frameworks tries to keep law enforcement and intelligence services separate. By doing so, the report excludes the work of law enforcement from its scope, while recognising that making this division is not always easy. As stated by Chesterman, "Governments remain conflicted as to the appropriate manner of dealing with alleged terrorists, the imperative to detect and prevent terrorism will lead to ever greater cooperation between different parts of government".[18] The EP resolution recognises this and called on the Europol Joint Supervisory Body (JSB) to inspect whether information and personal data shared with Europol have been lawfully acquired by national authorities, particularly if the data were initially acquired by intelligence services in the EU or a third country.[19]

The Snowden revelations have also shed light on cooperation between intelligence services. This issue, important for the oversight of intelligence services' activities, has been addressed by the EP resolution (Paragraph 22),

14 See FRA (2014a).
15 European Parliament (2014), paras. 132 and 35.
16 See Bigo, D. *et al.* (2013), p. 41.
17 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 78.
18 See Chesterman, S. (2011), p. 237.
19 European Parliament (2014), para. 84; Europol Joint Supervisory Body (2014).

by oversight bodies,[20] by the Venice Commission,[21] and by academia.[22] This aspect, however, proved impossible to analyse in a comparative study, since, in the great majority of cases, cooperation agreements or modalities for transferring data are neither regulated by law nor public. This in itself creates a fundamental rights issue linked to the rule of law and, more particularly, regarding the importance of the existence of a law that is accessible to the public, as well as regarding the rules governing the transfer of personal data to third countries. Though this report could not deal with this aspect beyond referencing the lack of proper control by oversight bodies, it does raise important questions under relevant legal standards.

Fundamental rights and safeguards

Given the scope of the EP request, the FRA decided to focus its research on privacy and data protection, because surveillance measures acutely encroach on these fundamental rights. According to the Council of Europe Commissioner for Human Rights, "[i]t is not only the actual use of these measures against given individuals that infringes the right to privacy but also their potential use and/or the mere existence of legislation permitting their use".[23] This in no way means that other fundamental rights are not equally affected. The EP resolution highlighted this when referring to other affected fundamental rights, in particular "freedom of expression, of the press, of thought, of conscience, of religion and of association, [...] the presumption of innocence and the right to a fair trial and non-discrimination".[24]

A fundamental right must be properly safeguarded to be effectively exercised. This report analyses, as per the EP request, the remedies at an individual's disposal to uphold his or her rights to privacy and data protection. Past FRA research provides important findings on how data protection remedies work in practice. While recognising the specificity of surveillance measures, this report draws on key conclusions elaborated on in the 2014 FRA report on access to data protection remedies, which carefully assessed the practical role of national data protection authorities.[25] This report also examines the crucial role specialised bodies play in overseeing the work of security and intelligence services.

International and European standards applicable to surveillance have been exhaustively developed and commented on by multiple organisations, so this report will merely refer to them to avoid duplicating already existing work. The United Nations (UN) has set standards in this area for decades. Its various expert bodies and human rights procedures were forthright in their condemnations of mass surveillance practices following the Snowden revelations.[26] In March 2015, the Human Rights Council of the UN decided to create the post of Special Rapporteur on the Right to Privacy, who will be in charge of monitoring privacy rights in the UN context.[27]

The European Court of Human Rights (ECtHR) has over the years also developed standards, based on Article 8 of the ECHR (right to respect for private and family life) – including its procedural aspects[28] – and Article 13 of the ECHR (right to an effective remedy).[29] Its case law has reviewed various forms of surveillance, but issues related to the Snowden revelations have not yet been adjudicated.[30] ECtHR standards have triggered legislative reforms at national level;[31] narrowed the scope of the term 'national security' and required that the threat to national security have some reasonable basis in facts;[32]

20 The Belgian Standing Committee I, for example, refers to Germany and the Netherlands, whose laws organise data transfer; see Belgium, Standing Committee I (2014), pp. 4–5. The Dutch Review Committee has conducted a number of investigations on cooperation between Dutch and foreign services. Its latest investigation addresses this issue, as well, and additional investigations are expected to be published; see The Netherlands, CTIVD (2014b), pp. 13 and 148 and following; The Netherlands, CTIVD (2014a), p. 29 and following. See also The Netherlands, CTIVD (2010), p. 47 and following. However, CTIVD recognises the limits of its power in this context; see The Netherlands, CTIVD (2015), p. 35.

21 See Venice Commission (2015).

22 See Born, H. *et al.* (eds.) (2011); Born, H. *et al.* (2015); Bigo, D. *et al.* (2013), pp. 24 and 39; Cousseran, J,-C. and Hayez, P. (2015), p. 133 and following.

23 Council of Europe Commissioner for Human Rights (2015), p. 21.

24 European Parliament (2014), para. T. See also United Nations (UN) General Assembly (GA) (2014b); UN, Human Rights Council, Kaye, D. (2015); UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) (2015); ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, para. 88, in which the ECtHR acknowledges that the surveillance methods interfered with the applicant's freedom of expression; Council of Europe Commissioner for Human Rights (2015); Raab, C. *et al.* (2015).

25 FRA (2014c).

26 See UN, GA (2014a); UN, GA (2014b); UN, Human Rights Council, Scheinin, M. (2009); UN, Office of the High Commissioner for Human Rights (OHCHR) (2014); UN, Human Rights Council, Emmerson, B. (2014); UN, Human Rights Committee (2014) and UN, Human Rights Committee (2015a).

27 UN, Human Rights Council (2015).

28 ECtHR, *M.N. and Others v. San Marino*, No. 28005/12, 7 July 2015, para. 83.

29 For a discussion of the ECtHR case law, see European Commission for Democracy through Law (Venice Commission) (2007); Venice Commission (2015).

30 See the pending case: ECtHR, *Big Brother Watch and Others v. the United Kingdom*, No. 58170/03, communicated on 9 January 2014.

31 ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 August 1984; ECtHR, *Kruslin v. France*, No. 11801/85, 24 April 1990.

32 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, paras. 45–46; ECtHR, *Janowiec and Others v. Russia* [GC], Nos. 55508/07 and 29520/09, 21 October 2013, paras. 213–214; ECtHR, *C.G. and others v. Bulgaria*, No. 1365/07, 24 April 2008, para. 40.

and clarified procedural rules such as legal standing in the area of surveillance,[33] the extent to which an individual can have an "expectation of privacy",[34] and the minimum safeguards that should be in place during surveillance.[35] Moreover, the ECtHR has cited 1981 Council of Europe data protection Convention (Convention 108) principles when examining personal data processing within the scope of the ECHR and the concept of private life.[36] According to the Venice Commission, the ECHR standards should be considered as minimum human rights standards.[37] They are often used as a benchmark when assessing legislation or a surveillance practice.[38]

European Union Law

At the EU level, the rights to privacy and data protection are enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter). The right to data protection is also laid down in Article 16 of the Treaty on the Functioning of the European Union (TFEU), and in Article 39 of the Treaty on the European Union (TEU). In addition, secondary legislation adopted earlier than the Charter and the TFEU protect this right. Relevant legal instruments include the Data Protection Directive 95/46/EC, the e-Privacy Directive 2002/58/EC and the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. These instruments ensure, amongst others, that in their respective scope of application, the processing of personal data is carried out lawfully and only to the extent necessary for the fulfilment of the legitimate aim pursued. These rights extend to all persons, whether they are EU citizens or third-country nationals. According to Article 52 (1) of the Charter, any limitation to this right must be necessary and proportionate, genuinely meet objectives of general interest recognised by the Union, be provided by law, and respect the essence of such rights.

Applicability of these instruments in the field of security is, however, subject to the specific legal and policy framework in the area and particularly to the national security exemption. Article 4 (2) of the TEU provides that "national security remains the sole responsibility of each EU Member State". This exemption is reiterated both in Article 3 (2) of the Data Protection Directive and in Article 1 (4) of Framework Decision 2008/977/JHA, which excludes "essential national security interests and specific intelligence activities in the field of national security" from the rules applicable to 'regular' law enforcement action.

The limits of the national security exemption are subject to debate, including in relation to the activities of intelligence services.[39] Although international guidelines[40] exist, there is no uniform understanding of 'national security' across the EU. The concept is not further defined in EU legislation or in CJEU case law, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified.[41] The CJEU has also stated that the mere fact that a decision concerns state security does not render EU law inapplicable.[42]

The lack of clarity on the precise scope of the national security exemption goes hand in hand with the varied and seldom clearly drawn line between the areas of law enforcement and national security in individual Member States. This is particularly true with counter-terrorism, since terrorism is generally considered a threat to both national security and to law and order. As a result, the division of competences amongst intelligence and law enforcement authorities varies throughout the EU Member States, as do the modalities of their information exchanges.

It falls outside the scope of this report to analyse in great detail the extent of EU competence in this field. However, the current situation is relevant not only to surveillance and the rights of privacy and personal data protection, but also to efforts at the EU level in the area of internal security, in accordance with Article 4 (2) (j) of the TFEU, which defines the area of freedom, security and justice as an area of shared competences between

33 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, para. 34. See also ECtHR, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008, para. 56.
34 ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007, para. 42.
35 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 95.
36 ECtHR, *Z. v. Finland*, No. 22009/93, 25 February 1997, paras. 95–97; ECtHR, *Amann v. Switzerland*, No. 27798/95, 16 February 2000, para. 65; ECtHR, *Rotaru v. Romania*, No. 28341/95, 4 May 2000, para. 43; ECtHR, *S. and Marper v. The United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008, paras. 41, 66–69, 76, 103–104, 107; ECtHR, *Uzun v. Germany*, No. 35623/05, 2 September 2010, paras. 43–48; ECtHR, *Bernh Larsen Holding AS and Others v. Norway*, No. 24117/08, 8 July 2013, paras. 76–78; ECtHR, *Khelili v. Switzerland*, No. 16188/07, 8 March 2012, paras. 20–21; ECtHR, *M.M. v. the United Kingdom*, No. 24029/07, 29 April 2013, paras. 122–124.
37 Venice Commission (2015), p. 24.
38 See, for example, the work of the Dutch Review Committee for the Intelligence and Security Services (CTIVD).
39 See, for example, Peers, S. (2013), pp. 2–3, on the distinction between national security and law enforcement functions of intelligence services.
40 See especially Article 19 (1996), Johannesburg Principles on national security, freedom of expression and access to information; UN, Human Rights Council, Scheinin, M. (2010).
41 See CJEU, C-387/05, *European Commission v. Italian Republic*, 15 December 2009, para. 45, and Article 29 Working Party (2014b), p. 24.
42 See CJEU, C-300/11, *ZZ v. Secretary of the State of Home Department*, 4 June 2013, para. 38.

the EU and the Member States. At present, the lack of a clear delimitation between 'public order' and 'national security' – the protection of the latter being left to the Member States without interference from the EU, in accordance with Article 4 (2) of the TFEU – influences the ongoing debate on the renewal of the EU Internal Security Strategy regarding the exchange and use of existing intelligence for countering terrorist threats.[43]

Although a dedicated mechanism within EU structures (the EU Intelligence Analysis Centre, INTCEN, and to some extent also the EU Satellite Centre) exists, information exchanges between national intelligence authorities take place on a voluntary and *ad hoc* basis, and largely outside the EU legal framework.[44] What is known about information exchanges in this field is necessarily limited, as much of it is shielded from public scrutiny. Coordinated action at the EU level is therefore limited to enhancing law enforcement information exchanges, with emphasis on better utilising the potential of the European Police Office (Europol) and, to some extent, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex).

The national security exemption provides a methodological challenge because of a lack of a clear delineation between surveillance activities conducted for law enforcement and for national security purposes, and the resulting variety in the involvement and competence of actors.

This unclear delineation of 'national security' also has repercussions for the applicability of EU law, which depends both on the interpretation of the national security exemption's scope and on the specific characteristics of the various surveillance programmes carried out by intelligence services. Although the existence of such programmes remains largely unknown, even in light of the Snowden revelations, some contain elements that can justify the full applicability of EU law. For instance, when EU companies transfer data to intelligence services, including those of third countries,[45] they are considered under the Data Protection Directive as data controllers who collect and process data for their own commercial purposes. Any subsequent data processing activities, such as the transfer of personal data to intelligence services for the purpose of the protection of national security, will therefore fall within the scope of EU law.[46] Any limitations of the rights to privacy and personal data protection should be examined according to Article 13 of the Data Protection Directive and Article 15 of the e-Privacy Directive, as well as Article 52 (1) of the Charter. Such limitations are to be treated as exceptions to the protection of personal data, and thus subject to narrow interpretation and requiring proper justification.[47] The essence of the right to privacy and protection of personal data shall at any rate be respected. The 'national security' exception thus cannot be seen as entirely excluding the applicability of EU law. As the UK Independent Reviewer of Terrorism Legislation recently put it,

> *"National security remains the sole responsibility of each Member State: but subject to that, any UK legislation governing interception or communications data is likely to have to comply with the EU Charter because it would constitute a derogation from the EU directives in the field."*[48]

Finally, even when EU law does not apply, other international instruments do, notably the ECHR and Convention 108[49] and its 2001 Additional Protocol.[50] The CJEU refers to Member States' international obligations under the ECHR when a subject matter falls outside EU law.[51]

Methodology

This report draws on data provided by the agency's multidisciplinary research network Franet, which were collected through desk research in all 28 EU Member States, based on a questionnaire submitted to the network.[52]

Additional information was gathered through desk research and exchanges with key partners, including a number of FRA's national liaison officers in the Member States and individual experts. These include Ian Cameron, Professor of International law, Uppsala University, and Member of the Venice Commission; Douwe Korff, Emeritus Professor of International Law, London Metropolitan University and Oxford Martin

43 This relates particularly to the debate on whether more effective exchanges of intelligence within and between Member States could prevent terrorist attacks by persons already known to national authorities, as was allegedly the case with perpetrators of the 2014 Brussels and 2015 Paris attacks.

44 For instance through the *Club de Berne* and the derived Counter Terrorist Group, an intelligence-sharing forum that specifically focuses on counterterrorism intelligence and encompasses all EU Member States, as well as Norway and Switzerland.

45 See Article 29 Working Party (2014c), Section 5 on data transfers to non-EU countries.

46 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015.

47 CJEU, C-387/05, *European Commission v. Italian Republic*, 15 December 2009, para. 45.

48 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 71.

49 Council of Europe, Convention 108; CJEU, C-387/05, *European Commission v. Italian Republic*, 15 December 2009, para. 45.

50 Council of Europe, Convention 108, Additional Protocol.

51 CJEU, C-127/08, *Metock v. Minister of Justice, Equality and Law Reform*, 25 July 2008, paras. 74–79.

52 See FRA (2014b).

Associate, Oxford Martin School, University of Oxford; Andreas Krisch, managing partner, mksult GmbH, Vienna, Austria; Ian Leigh, Professor of Law, Durham University; Carly Nyst, Legal Director, Privacy International, London; Peter Schaar, Chair of the European Academy for Freedom of Information and Data Protection and former German Federal Commissioner for Data Protection and Freedom of Information (2003-2013); and Martin Scheinin, Professor at the European University Institute, coordinator of the FP7 project SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency), and former United Nations Special Rapporteur on human rights and counter-terrorism.

FRA expresses its gratitude for these valuable contributions. The opinions and conclusions in this report do not necessarily represent the views of the organisations or individuals who helped develop the report.

While this report maps the EU-28 legal frameworks, the FRA findings also draw on existing reports and publications aimed at supporting national legislators in setting up legal frameworks for the intelligence services and their democratic oversight.[53] The findings refer in particular to the compilation of good practices issued by Scheinin as Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[54]

The mapping of legal frameworks in the EU in this report follows the structure the ECtHR suggests for surveillance cases. So far, most of the cases brought before the Strasbourg judges have focused on the legality of interferences with the right to privacy – in other words, whether the secret surveillance was "in accordance with the law". Contrary to its other jurisprudence, the ECtHR has added to the legality test *stricto sensus* requirements for other specific safeguards that surveillance laws should have. As stated by Cameron, "[A] law, or legal mechanism, which is regarded as deficient in formulation (e.g. because it is imprecise) may nonetheless be corrected by a safeguard (e.g. because it compensates for the risk of abuse caused by the imprecision)".[55] This relates to the approval mechanism of the measure and the oversight mechanism controlling its implementation, as well as to available remedies.

Following this approach, after providing overviews of the intelligence services and surveillance laws in the EU Member States (Chapter 1), this report presents the safeguards in place (Chapter 2), and the available remedies (Chapter 3).

53 See, for example, Venice Commission (2007); Venice Commission (2015); or Born, H. and Wills, A. (eds.) (2012).

54 UN, Human Rights Council, Scheinin, M. (2010).

55 See Cameron, I. (2013), p. 164.

1 Intelligence services and surveillance laws

1.1. Intelligence services

UN good practices on mandate

Practice 1. Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights.

Practice 5. Intelligence services are explicitly prohibited from undertaking any action that contravenes the Constitution or international human rights law. These prohibitions extend not only to the conduct of intelligence services on their national territory but also to their activities abroad.

UN, Human Rights Council, Scheinin, M. (2010)

The organisation of the intelligence community in each EU Member State is closely linked to historical developments, wars and external threats. The intelligence community is therefore greatly diverse. Intelligence scholars have drawn up models based on existing intelligence community structure.[56] This is an area of state sovereignty not affected by ECtHR case law; the institutional organisation and services' mandates belong to the state prerogatives and are guided by identified threats and needs. This chapter provides a description of the main actors.

To analyse the work of the security and intelligence services in the EU, a short description of these services and their core functions is necessary. First, a conceptual clarification: 'intelligence services' are agencies focusing on external threats (they have a foreign mandate), while 'security services' are agencies focusing on domestic threats, with a domestic mandate.[57] This report uses generic terminology and refers to 'intelligence services' for both. Born and Wills suggest the following definition of an intelligence service: "A state organisation that collects, analyses, and disseminates information related to threats to national security".[58] The line between "foreign" and "domestic" threats is often blurred. Such is the case with terrorist activities, which are often of transnational character. As a result, close cooperation between services with a domestic mandate and services with a foreign mandate is usually necessary. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism adopted the same approach, so the UN good practices could apply to internal, external, civil and military services.[59]

The Annex shows that intelligence services are organised in different agencies based on their mandate. The table focuses only on the services, and not the coordination bodies that might exist in Member States, such as the Department for Security Information (DIS) in Italy or the National Intelligence Coordinator in France, which is part of the French intelligence community.[60] Moreover, the differences between internal and external mandates should not be overemphasised since the surveillance of digital communication does not necessarily recognise geographical borders.

Almost all EU Member States have established at least two different bodies for conducting civil and military intelligence activities. In practice, the line separating the mandates between civil and military security

56 See Cousseran, J.-C. and Hayez, P. (2015), p. 35 and following.

57 Born, H. and Leigh, I. (2005), p. 31.
58 Born, H. and Wills, A. (eds.) (2012), p. 6. See also Cousseran, J.-C. and Hayez, P. (2015), p. 41.
59 UN, Human Rights Council, Scheinin, M. (2010), p. 4.
60 France, Defence Code (*Code de la Défense*), Art. D 1122-8-1.

services is becoming increasingly blurred.[61] A distinction can sometime be established, though, in the referred authorities: civil intelligence services are generally subordinate to interior ministries, sometimes also to the prime ministers, whereas military bodies refer to the Ministry of Defence. This report focuses on civil intelligence services.

In some Member States, such as France, Germany, Italy, Romania and Poland, civil intelligence services are further divided into two separate services, mandated with a domestic or foreign scope. Moreover, some Member States grant intelligence-like means to units specialised in a defined threat, such as organised crime in Spain, corruption in Poland or the fight against terrorism in Hungary.

Another key element to consider is the extent of the relationship between security services and law enforcement. Indeed, an organisational separation between intelligence services and law enforcement authorities is commonly considered a safeguard against the concentration of powers into one service and the risk of arbitrary use of information obtained in secrecy. As noted in 1999 by the Parliamentary Assembly of the Council of Europe (PACE), "[I]nternal security services should not be authorised to carry out law enforcement tasks such as criminal investigations, arrests, or detention. Due to the high risk of abuse of these powers, and to avoid duplication of traditional police activities, such powers should be exclusive to other law enforcement agencies".[62] The majority of intelligence services have their own structure and organisation, independent of the police and other law enforcement authorities.

In Germany, for example, the Act on the Federal Intelligence Service (BND) specifically states that the BND "must not be attached to a police authority".[63] The separation of police and intelligence services is not explicitly laid down in the Basic Law (*Grundgesetz*), i.e. the constitution. Its constitutional protection has been a subject of discussion in academia, while the Federal Constitutional Court has not directly addressed the issue.[64] In Estonia, the Security Police became the Internal Security Service (*Kaitsepolitseiamet, KAPO*) in 2001. More recently, in Sweden (as of 1 January 2015), the Security Service (*Säkerhetspolisen*, SÄPO) was reorganised into a separate authority, independent of the rest of the new police authority.[65] Few Member States make exceptions to this rule; they include Austria, Denmark, Finland, Ireland, and Latvia, where the body responsible for conducting intelligence activities belongs directly to the police and/or law enforcement authorities. In Hungary, a specific body of the police, specialised in counter-terrorism, is allowed to conduct non-criminal investigations and use secret surveillance methods for this purpose.

However, such organisational separation in law does not necessarily mean that the exchange of information and personal data between law enforcement and intelligence services is prohibited by law, given increasingly common fields of competence, such as the fight against terrorism. Indeed, national legislation may provide for data transfers between these authorities, in accordance with the rights to privacy and personal data protection.[66] As stated by the Council of Europe Commissioner of Human Rights, this cooperation should take place within a clear legal framework.

> *"Co-operation between law enforcement agencies and national security agencies can only happen under the rule of law if both agencies act in accordance with rule of law principles [e.g. clear legal frameworks]."*
>
> *Council of Europe Commissioner for Human Rights (2014), p. 110*

The more intelligence services shift their activities from state to non-state entities and individuals or groups of individuals, as in the case with terrorist organisations, the more important respect of the rule of law becomes. The enactment of laws is indeed a relatively recent process.[67] The turn to law might have been challenged following the attacks of 11 September 2001 on the United States.[68] Recent revelations regarding the intelligence services' surveillance capabilities, however, have underscored the need to respect the fundamental principle of the rule of law in democratic societies.

In short, the organisation of intelligence services in the EU is extremely diverse and dependent on Member State specificities. The intelligence community in each Member State is increasingly established by law.

Cousseran and Hayez note that there is a growing tendency to establish the intelligence community by law.

> *« Le renseignement demeure une information et une activité secrètes mais n'est désormais plus une organisation secrète. »* (Intelligence remains a secret information and a secret activity but is no longer carried out by a secret organisation – FRA translation).
>
> *Cousseran, J.-C. and Hayez, P. (2015), p. 55*

61 See Venice Commission (2015), p. 8; Cousseran, J.-C. and Hayez, P. (2015), p. 30.
62 PACE (1999), p. 2.
63 Germany, Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst*), 20 December 1990, as amended, Section 1. See also Section 2 (3) of the same act.
64 Sule, S. (2006), pp. 121–123.
65 Sweden, Ministry of Justice (*Justitiedepartementet*) (2012).
66 Sule, S. (2006), pp. 128 and 236.
67 See Laurent, S.-Y. (2014), p. 160.
68 Chesterman, S. (2011), p. 9.

1.2. Surveillance measures

UN good practices on intelligence collection and management and use of personal data

Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorising, overseeing and reviewing the use of intelligence-collection measures.

Practice 23. Publicly available law outlines the types of personal data that intelligence services may hold, and which criteria apply to the use, retention, deletion and disclosure of these data. Intelligence services are permitted to retain personal data that are strictly necessary for the purposes of fulfilling their mandate.

Practice 24. Intelligence services conduct regular assessments of the relevance and accuracy of the personal data that they hold. They are legally required to delete or update any information that is assessed to be inaccurate or no longer relevant to their mandate, the work of oversight institutions or possible legal proceedings.

UN, Human Rights Council, Scheinin, M. (2010)

The following paragraphs clarify the terms that will be used in the report. First, the section outlines surveillance measures related to technical collection, then distinguishes between targeted and untargeted collection.

1.2.1. Technical collection

'Technical collection' is traditionally distinguished from 'human collection', which takes place on the ground. Technical collection refers to the automated gathering of information through the interception and collection of digital data related to the subject of intelligence activity.[69] It is based on four key pillars: 1) cryptography, i.e. encryption (or decryption) of communications; 2) signals intelligence (SIGINT); 3) imagery or photo intelligence (IMINT); and 4) digital intelligence.[70]

In the digital age, these four pillars tend to disappear. They are merged into one single concept of 'digital network intelligence' (DNI), a term used by the NSA.[71] In fact, the National Research Council of the National Academies concludes that "signals intelligence has come to embrace almost any data stored on an electronic device".[72] Omand, a former GCHQ director, refers to this type of collection as 'digital intelligence'.[73] According to the Venice Commission, "SIGINT is a collective term referring to means and methods for the interception and analysis of radio (including satellite and cellular phone) and cable-borne communications".[74] Lowenthal's definition clearly shows that SIGINT derived from military intelligence. Indeed, SIGINT was traditionally used by military and foreign intelligence services to prevent military actions endangering national security.[75]

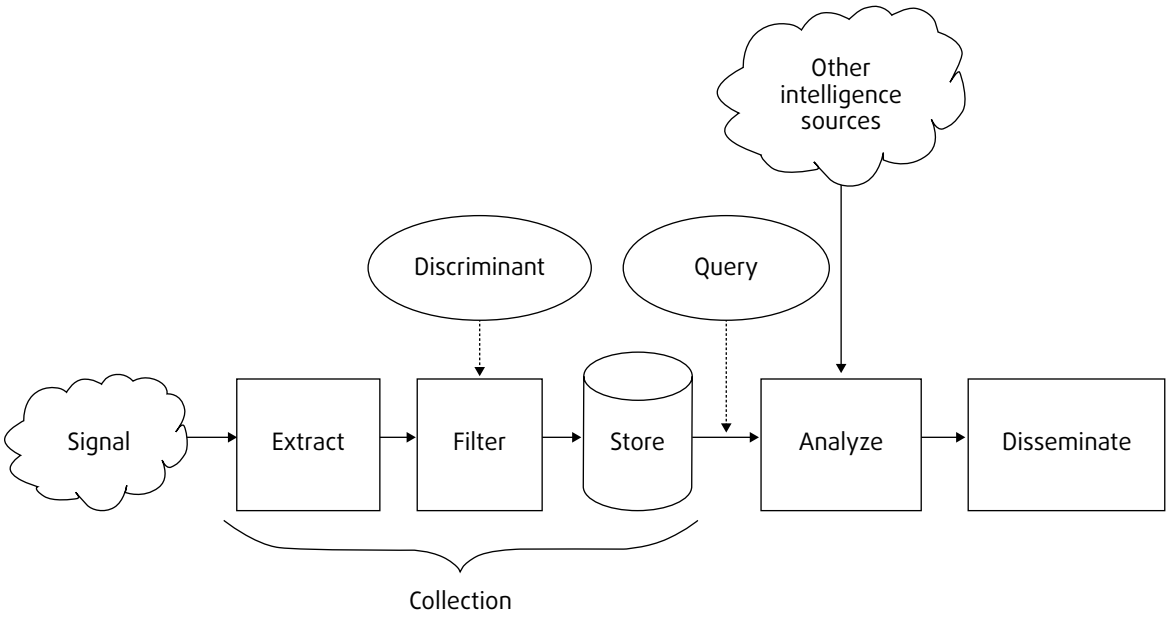
> *"SIGINT consists of several different types of intercepts. The term is often used to refer to the interception of communications between two parties, or COMINT. SIGINT can also refer to the pickup of data relayed by weapons during tests, which are sometimes called telemetry intelligence (TELINT). Finally, SIGINT can refer to the pickup of electronic emissions from modern weapons and tracking systems (military and civil), which are useful means of gauging their capabilities, such as range and frequencies on which systems operate. This is sometimes referred to as ELINT (electronic intelligence) but is more customarily referred to as FISINT (foreign instrumentation signals intelligence). The ability to intercept communications is highly important, because it gives insight into what is being said, planned, and considered."*
>
> *Lowenthal, M. (2015), pp. 118–119.*

With the development of digital communications, national borders (i.e. the indications of what is foreign and what is national) are more difficult to identify. Furthermore, national security threats are not only posed by states, but also by terrorist groups and organised crime networks. Since the fight against terrorism led to (internal) security services using SIGINT, this report focuses only on such interception, strictly speaking, for non-military purposes. In doing so, FRA aligns its analysis with the scope of the EP resolution, which does not cover military threats. FRA uses 'signals intelligence' (SIGINT) as a generic term that covers the elements used in the EP resolution,[76] even though most of it could fall into the communications intelligence (COMINT) category. However, since detailed surveillance methods by intelligence services rarely appear in the text of the law, FRA uses 'signals intelligence' as an encompassing term.[77]

For intelligence services, one of the key challenges of collection is the quantity of data available. As Lowenthal puts it, "[A]s of 2013, there are some 7 billion telephones worldwide [...] generating some 12.4 billion calls every

69 European Parliamentary Research Service (EPRS), Science and Technology Options Assessment (STOA) (2014a); EPRS, STOA (2014b).
70 See Cousseran, J.-C. and Hayez, P. (2015), p. 91 and following.
71 *Ibid.*, p. 92.
72 United States, National Research Council (2015), p. ix.
73 Omand, D. (2015).
74 Venice Commission (2015), p. 8.
75 See Venice Commission (2015), p. 8. See also Lowenthal, M. (2015), pp. 118–119; Brown, I. *et al.* (2015), p. 5; Cousseran, J.-C. and Hayez, P. (2015), pp. 65 and 90.
76 European Parliament (2014), para. 1.
77 For detailed explanations of how SIGINT are used by the NSA, see United States, National Research Council (2015).

Figure 1: A conceptual model of signals intelligence



Source: United States, National Research Council (2015), p. 28

day. Newer communications channels add to the total. In the United States alone, 2.2 trillion text messages were sent in 2012, as well as 400 million tweets (Twitter messages) daily in 2013."[78] This requires important budgetary investments that not all countries can afford. Cousseran and Hayez identify the following EU countries as having services with important capacities that can afford SIGINT collection: the UK (5,500 staff working at GCHQ), France (2,100 staff working at the Directorate General of External Security (*Direction de la sécurité extérieure*, DGSE) and 700 staff working at the Directorate of Military Intelligence (*Direction du renseignement militaire*, DRM), Germany (1,000 staff working at the BND) and Sweden (*Försvarets Radioanstalt*).[79] Brown *et al.* add the Netherlands, Italy and Spain to the list of Member States performing SIGINT.[80] The US National Research Council's analysis shows that SIGINT requires discriminants (or selectors) to make it possible to filter the data before its storage, and further analysis by the intelligence services (example: "all email addresses used in communications with Yemen").[81] Figure 1 illustrates this process.

When 'signals intelligence' is not used, institutions and commentators use various terms to refer to these surveillance techniques. The UN refers to "bulk access to communications and content data without prior suspicion",[82] "high levels of Internet penetration",[83] "intercept digital communications",[84] or "governmental mass surveillance".[85] The Committee of Ministers of the Council of Europe refers to "broad surveillance of citizens",[86] the specialised ministers of the Council of Europe refer to "the question of gathering vast amounts of electronic communications data on individuals by security agencies",[87] and the Parliamentary Assembly of the Council of Europe entitled its report "mass surveillance".[88] The European Parliament refers to "mass surveillance" (see the Resolution), and Bigo *et al.* in their commissioned report for the European Parliament refer to large-scale surveillance and "cyber-mass surveillance".[89]

Finally, the Venice Commission uses the concept of 'strategic surveillance' to emphasise that "signals intelligence can now involve monitoring of 'ordinary communications'".[90] In doing so, it builds on the concept used in German law (strategic restriction, *strategische Beschränkung*), adding that 'strategic surveillance' also includes "signals intelligence to collect information

78 Lowenthal, M. (2015), p. 120.
79 Cousseran, J.-C. and Hayez, P. (2015), p. 92 (number of staff working at the Swedish SIGINT agency not specified). See also Bigo, D. *et al* (2013), p. 21.
80 Brown, I. *et al.* (2015), p. 9.
81 See United States, National Research Council (2015), p. 36. A discriminant is defined as "detailed instructions for searching a database of collected data". See also Belgium, Standing Committee I (2015), p. 12.
82 UN, Human Rights Council, Emmerson, B. (2014), p. 4.
83 *Ibid.*
84 UN, Human Rights Council (2015), p. 2.
85 UN, OHCHR (2014), p. 3.
86 Council of Europe, Committee of Ministers (2013).
87 Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), para. 13 (v).
88 PACE (2015b).
89 Bigo, D. *et al.* (2013), p. 14.
90 Venice Commission (2015), p. 9.

on identified individuals and groups",[91] therefore covering initially untargeted surveillance that becomes more targeted. The word 'strategic' denotes a process involving a selection by way of automated tools. The data goes through selectors or discriminants applied by algorithms. This touches on the second key aspect of the EP resolution definition, which requires an explanation of the distinction between targeted and untargeted collection.

In short, when 'signals intelligence' – which FRA applies generically – is not used, Member State terminology will guide this report's legal analysis.

1.2.2. Targeted and untargeted collection

This report looks at the impact of surveillance on fundamental rights and at available remedies, so covers targeted surveillance as well as untargeted surveillance by intelligence services.

The Dutch Review Committee for the Intelligence and Security Services (CTIVD) defines targeted and untargeted surveillance as follows:

- targeted interception: "Interception where the person, organisation or technical characteristic at whom/which the data collection is targeted can be specified in advance";
- untargeted interception: "Interception where the person, organisation or technical characteristic at whom/which the data collection is targeted cannot be specified in advance".

The Netherlands, CTIVD (2014a), p. 45 and following

The wide-reaching reactions to the Snowden revelations were triggered by the scale of data collected through the revealed programmes. The concept of 'mass surveillance' illustrates the difference between the amount of data collected through these programmes and the data collected through traditional secret (targeted) surveillance methods, such as telephone tapping. The latter presupposes the existence of prior suspicion of a targeted individual or organisation. This type of surveillance is widely known in EU Member States' laws. Since the overwhelming majority of EU Member States' legal frameworks do not regulate or indeed speak of 'mass surveillance' as such – mass surveillance is not a legal term"[92] – it is important to analyse how targeted surveillance is prescribed in EU Member States' legal frameworks to assess how fundamental rights are upheld.

The concept of 'untargeted surveillance' is more problematic to delineate because a surveillance measure can start without prior suspicion or a specific target, which is defined after collection and filtration of certain data. In the US context, the distinction is made between 'bulk' and 'targeted' collection in the context of SIGINT. The National Research Council of the National Academies acknowledged in its report on signals intelligence, however, that this distinction "is quite unclear".[93] It suggested the following distinction: "If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted."[94] This is what the Venice Commission's definition highlights when it defines strategic surveillance: its difference with law enforcement surveillance and its impact on fundamental rights.[95]

> *"Strategic surveillance thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lay both the value it can have for security operations, and the risk it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights."*
>
> *European Commission for Democracy through Law (Venice Commission) (2015), p. 12.*

Distinguishing between mass surveillance and targeted surveillance requires a close analysis of the various surveillance programmes. Cayford *et al.*'s analysis of several surveillance programmes revealed by Snowden illustrates this. While the authors consider, for example, PRISM[96] to be "a targeted technology used to access court ordered foreign internet accounts",[97] they consider wiretapping of fiber-optic cables programmes as revealed in the UPSTREAM or TEMPORA[98] programmes to be mass surveillance.

The Snowden revelations have demonstrated that current legal frameworks and oversight structures have been unable to keep up with technological developments that allow for the collection of vast amounts of data. In some cases, outdated laws not intended to regulate these new forms of surveillance are being used to justify them. Moreover, the Council of Europe Commissioner for Human Rights stated that "in many Council of Europe member states, bulk, untargeted surveillance by security services is either not regulated by any publicly

91 *Ibid.*, p. 9, fn. 3.
92 *Ibid.*, p. 14.
93 United States, National Research Council (2015), p. 33.
94 *Ibid.*, p. 2, footnote omitted.
95 See also Bigo, D. *et al.* (2013), p. 15.
96 For a definition, see European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013a).
97 Cayford, M. *et al.* (2015), p. 646.
98 For a definition, see European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013a).

available law or regulated in such a nebulous way that the law provides few restraints and little clarity on these measures".[99] Consequently, in some Member States, discussion about the adequacy of the legal frameworks triggered calls for legal reforms.[100]

Brouwer summarised one of the key conclusions of the Dutch Review Committee's investigation as follows: "Technological developments – and consequently the digitalisation of society – have not only largely facilitated digital communication and the digital storage of large volumes of data by individuals, they have by that consequently also increased the possibilities of the services to acquire, process and exchange this data. This means that there is much more personal data available for processing than ever before."[101] In the United States, President Obama requested the Director of National Intelligence (DNI) to "assess the feasibility of creating software that would allow the IC [Intelligence Community] to more easily conduct targeted information acquisition [of signals intelligence] rather than bulk collection".[102] The DNI tasked the National Research Council with conducting this assessment. In its report, the National Research Council concluded that no software technique could fully substitute bulk collection, but suggested enhancing automatic controls of the usage of data collected.[103]

Delmas-Marty nicely summarises the difference in approaches to targeted and untargeted surveillance: "Instead of starting from the target to find the data, one starts with the data to find the target. [*Au lieu de partir de la cible pour trouver les données, on part des données pour trouver la cible*]."[104]

99 Council of Europe Commissioner for Human Rights (2015), p. 23. For an example of proposed legal changes, see: The Netherlands, Draft law on the Intelligence and Security Services 20XX (*Concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX*), 02 July 2015.

100 See in Germany, Löning, M. (2015); The Netherlands, Draft law on the Intelligence and Security Services 20XX; United Kingdom, Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 8; Austria, State Security Bill (*Entwurf Polizeiliches Staatsschutzgesetz – PStSG*), 1 July 2015, Explanatory note (*Erläuterungen*), 31 March 2015.

101 Brouwer, H. (2014), p. 4. See also, Cayford, M. *et al.* (2015), p. 643.

102 See United States, The White House (2014).

103 See United States, National Research Council (2015).

104 Delmas-Marty, M. (2015).

1.3. Member States' laws on surveillance

> *"Security services have a number of characteristics that create the potential for human rights abuses if these services are not subject to effective oversight and underpinned by effective laws. These characteristics include recourse to very invasive powers that can be used in a highly discretionary manner, undertaken largely in secret and, in some countries, viewed as an instrument of the incumbent government that can be used for political purposes."*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 19*

This chapter presents the legal frameworks on surveillance in the EU-28. It focuses first on the quality of the surveillance laws by referring to the ECtHR standards. It then looks at the aims of the surveillance laws, and in particular at how they address national security. The following analysis does not assess the implementation of the legislation; FRA will provide such an assessment following future fieldwork research entailing data collection on implementation.

1.3.1. Surveillance 'in accordance with the law'

UN good practices on mandate and legal basis

Practice 2. The mandates of intelligence services are narrowly and precisely defined in a publicly available law. Mandates are strictly limited to protecting legitimate national security interests as outlined in publicly available legislation or national security policies, and identify the threats to national security that intelligence services are tasked to address. If terrorism is included among these threats, it is defined in narrow and precise terms.

Practice 3. The powers and competences of intelligence services are clearly and exhaustively defined in national law. They are required to use these powers exclusively for the purposes for which they were given. In particular, any powers given to intelligence services for the purposes of counter-terrorism must be used exclusively for these purposes.

Practice 4. All intelligence services are constituted through, and operate under, publicly available laws that comply with the Constitution and international human rights law. Intelligence services can only undertake or be instructed to undertake activities that are prescribed by and in accordance with national law. The use of subsidiary regulations that are not publicly available is strictly limited, and such regulations are both authorized by and remain within the parameters of publicly available laws. Regulations that are not made public do not serve as the basis for any activities that restrict human rights.

UN, Human Rights Council, Scheinin, M. (2010)

That it is important to define the role and tasks of intelligence services in legislation is an accepted human rights

standard. Yet, as Born and Leigh state, "[T]he rule of law requires more than a simple veneer of legality."[105] The well-established standards that stem from the ECtHR's case law support the UN good practices. Any interference with Article 8 of the ECHR needs to be established in law. This means that surveillance measures must be established in a statute.[106] This does not mean, however, that the full surveillance measures have to be established by a law; administrative regulations or well-established case law can specify the law on the books.[107] This flexible approach is particularly important in an area where the details of surveillance techniques cannot all be prescribed by law (see UN good practice No. 4).

Furthermore, the law has to be of a certain quality. In other words, the law must be accessible and foreseeable. In its case law on surveillance, the ECtHR often concludes that the cited domestic legal basis is insufficient or not 'in accordance with the law'. Both national rules governing the interception of individual communications and more general programmes of surveillance should therefore comply with the rule of law and be accessible to the individual, who needs to be able to assess how a specific piece of legislation can impact his or her actions.[108] Moreover, it is important to note that interference with a right deemed permissible under national law is not necessarily lawful under international law. It may in fact conflict with a range of international standards.[109]

Given the seriousness of the interference, the ECtHR has developed a set of minimum safeguards for laws to pass the 'quality' test.[110] These criteria have been established in the context of targeted surveillance and, as highlighted in two ECtHR judgments addressing quality of the law, are applicable to SIGINT, as well.

FRA data show that for some Member States the legal basis that frames the intelligence services' mandates and powers is constituted by one unique legal act governing their organisation and means (such as Estonia or Luxembourg). In others, complex frameworks made up of several laws and ordinances regulate specific aspects of the services' mandate, organisation, competences or means. Most Member States, though, organise the work of the intelligence services in two laws: one on the mandate and organisation of the service, the other on means of action and the conditions for using them. This is the case in Denmark, where the act regulating the mandate of the Danish Security and Intelligence Service (PET) was enacted in 2009, and an act codifying the activities of the Danish intelligence services entered into force in 2014. While the latter does not alter the basic tasks of the intelligence service, it establishes new rules on how to collect, process and disclose personal data.

105 Born, H. and Leigh, I. (2005), p. 19.
106 ECtHR, *Heglas v. Czech Republic*, No. 5935/02, 1 March 2007, para. 74.
107 See Cameron, I. (2013), p. 172.
108 ECtHR, *Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008, para. 59.
109 UN, OHCHR (2014), para. 21.
110 See Cameron, I. (2013).

ECtHR case law: quality of the law

"[F]oreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly [...]. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident [...]. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated [...]. The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures [...]. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference."

ECtHR, Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, paras. 93–94*

"In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

ECtHR, Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 95*

"The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other."

ECtHR, Liberty and Others v. the United Kingdom*, No. 58243/00, 1 July 2008, para. 63*

To assess the quality of law requirement, it is important to look at how targets are defined in EU Member States in both cases of targeted surveillance and of signals intelligence. This includes clearly defining the categories of persons and activities that may be subject to intelligence collection.

1.3.1.1. Targeted surveillance

A review of the legal frameworks that regulate surveillance methods used by intelligence services shows that almost all Member States (26/28, with the exceptions of Cyprus and Portugal) have codified their use into law. In Cyprus, a bill regulating the intelligence service's functioning is under discussion.[111] In Portugal, intelligence services are not entitled to conduct surveillance activities. Article 34 (4) of the constitution limits their mandate by not allowing any sort of intrusion into mail, telephone or communications other than in the course of a criminal investigation. Since the intelligence services cannot perform criminal investigations, they do not have, by law, surveillance powers. Their mandate is limited to promoting research and analysis, processing intelligence and archiving and disseminating the information gathered.

Targeted surveillance as regulated in the Member States' laws refers to concrete targets upon suspicion that an act falling within the remit of the intelligence services' tasks could be committed before a surveillance measure can be initiated. In several Member States, such targets may either be a group of people (defined through their relation to an organisation or a legal person) or an individual. This is the case in Austria, Belgium, Denmark, Finland, France, Italy, Lithuania and Slovakia. In some other Member States, such as Greece, the law does not explicitly mention the requirement of suspicion-based surveillance and prior identification of an individual or a group thereof.[112]

In Denmark, for example, the Security and Intelligence Service (*Politiets Efterretningstjeneste*, PET) can carry out 'coercive and investigative measures' in accordance with the Administration on Justice Act[113] where:

- there are specific grounds for suspicion that information is being transferred from/to the subject of the coercive measure;
- the coercive measure is strictly required for the investigation;
- the investigation is conducted in relation to a crime punishable with a minimum of six years of imprisonment, or for the prevention and investigation of the crimes enumerated in chapters 12 and 13 of the Danish Penal Code, e.g. terrorism.

PET collects information that "could be of importance" to its activities and conducts investigations that "can be assumed to be of importance" to its efforts in relation to counter-terrorism or that are "strictly required" for its other activities.[114]

In short, targeted collection takes place when the target is known before the surveillance measure is initiated.

1.3.1.2. Signals intelligence

FRA's analysis of the legal frameworks that regulate surveillance methods used by intelligence services shows that five Member States (France, Germany, the Netherlands, Sweden and the United Kingdom) detail the conditions that permit the use of both targeted surveillance and signals intelligence. This report focuses on these five Member States due to the existence of detailed legislation on SIGINT. This does not mean that this list is in any way exhaustive. FRA's selection is based on the fact that this type of collection is prescribed, in detail, in the law.

Three examples illustrate where the accessible law of a Member State provides insufficient details to allow for a legal analysis of the exact procedure in place on how signals intelligence is collected.[115] First, in Italy, the relevant articles establishing the intelligence service (AISE) do refer in very general terms to the need for AISE to collect relevant information for the protec-

111 Cyprus, Draft Law of 2014 (*Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών (ΚΥΠ) Νόμος του 2014*), submitted to the House of Representatives on 23 September 2014.

112 Greece, Act 2225/1994 on the protection of freedom of correspondence and communications and other provisions (*Νόμος 2225/1994 για την προστασία της ελευθερίας της ανταπόκρισης και άλλες διατάξεις*), 18 July 1994, as amended, Art. 5 (1) in combination with Art. 3 (2).

113 Denmark, Administration of Justice Act, Consolidated Act No. 1139, (*Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013*), 24 September 2013, Section 754 (a).

114 Denmark, Act No. 604 on the Danish Security and Intelligence Service as amended by Act. No. 1624 of 26 December 2013 (*Lov nr. 604 af 12. Juni 2013 om Politiets Efterretningstjeneste (PET), som ændret ved lov nr. 1624 af 26. december 2013*), 12 June 2013, Sections 1, 3 and 4.

115 Laws in Spain and Slovenia serve as further examples. For Spain, see Spain, National Intelligence Centre Act (*Ley 11/2002 reguladora del Centro Nacional de Inteligencia*), 6 May 2002, Art. 4 (d), read in conjunction with Spain, Organic Law Regulating *a priori* judicial control of the National Intelligence Centre (*Ley Orgánica 2/2002 reguladora del control judicial previo del Centro Nacional de Inteligencia*), 6 May 2002, Art. 1, which tasks the Spanish intelligence service with obtaining, evaluating and interpreting the traffic of strategic signals in fulfilment of the intelligence objectives assigned to the Service. For Slovenia, see Slovenia, Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji,* ZSOVA), 7 April 1999, Art. 21, which allows for the surveillance of international communication systems, but does not define these. The Information Commissioner challenged this provision before the Slovene Constitutional Court, which rejected the claim on procedural grounds, stating that the Information Commissioner may only lodge a claim for constitutional review if a question of constitutionality arises in relation to the inspection procedure. See Slovenia, Constitutional Court (*Ustavno sodišče*), No. U-I-45/08-21, 8 January 2009.

tion of national interest, but no reference to specific methods are made.[116] However, the director of AISE described AISE's communications intelligence (COMINT) activities to the Italian parliamentary oversight committee (COPASIR), specifying their legality within the current legal framework, and describing the methods and techniques used. During the same hearing, AISE's SIGINT activities were also mentioned.[117]

Similarly, in Germany, some of the SIGINT activities that the Federal Intelligence Service (BND) may undertake is not regulated in detail by law, unlike other SIGINT activities in Germany. The Federal Intelligence Act states that the BND "shall collect and analyse information required for obtaining foreign intelligence, which is of importance for the foreign and security policy of the Federal Republic of Germany" and that it "may collect, process and use the required information, including personal data [...]".[118] This definition of the BND's competences provides the legal basis for the German intelligence service to perform SIGINT activities abroad between two foreign countries or within one single foreign country, provided that the intercepted signals have no connection - besides the actual data processing - with Germany. This SIGINT activity is referred to as "open sky" (*offener Himmel*), and, according to various commentators, takes place outside of any legal framework.[119] So far however, no judicial decision, either in Germany or by the ECtHR, has confirmed this assessment. This surveillance method does not fall within the scope of the Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (G 10 Act),[120] which was adopted in application of Article 10 (2) of the Basic Law to lay down the specific conditions to restricting privacy of communications. Consequently, this surveillance method is outside the G 10 Commission's remit (the expert body in charge of overseeing the intelligence services). The Parliamentary Control Panel is the sole body that oversees this surveillance method. The absence of tight control has triggered calls for reform, and the matter is being discussed before the NSA Committee of Inquiry (*NSA - Untersuchungsauschuss*).[121]

Finally, the French Bill on intelligence[122] organised the surveillance of communications made or received abroad (international surveillance), referring to a non-public decree prescribing the modalities of its implementation.[123] The Constitutional Court, however, found that the legislator did not determine the fundamental rights guarantees that need to be provided to the individuals, and so declared draft Article L. 854-1 of the Code on Interior Security contrary to the constitution and annulled the specific provision.[124] Following this court decision and in order to provide a legal basis for international surveillance, a bill on the surveillance of electronic international communications was prepared and is under discussion in the French parliament.[125]

The following paragraphs present the legal frameworks of the five Member States that are authorised to carry out not only targeted surveillance but also signals intelligence. References to systematic access via telecommunication data retention laws are excluded since these laws are primarily used for law enforcement purposes in their criminal investigation work, which falls outside the scope of this report.

In Germany, Article 10 (2) of the Basic Law (*Grundgesetz*) permits restrictions of the inviolability of the privacy of correspondence, post and telecommunications. It states, "Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a *Land*, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

The 'strategic restrictions' prescribed by the G 10 Act enable the Federal Intelligence Service (*Bundesnachrichtendienst,* BND) to wiretap international communications to and from Germany. They are called 'strategic' because of their original military purpose. In 1994, the

116 Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on State secrets (*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*), 3 August 2007, Art. 6.
117 See Italy, COPASIR (2014), p. 26.
118 Germany, Act on the Federal Intelligence Service, Sections 1 (1) and 2 (1).
119 See Huber, B. (2013), p. 2575 f.; Heumann, S. and Wetzling, T. (2014), p. 13.
120 Germany, Act on Restricting the Privacy of Correspondence, Posts and Telecommunications (Article 10, G 10 Act) *(Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10, Gesetz G 10))*, 26 June 2001, as amended.
121 See Bäcker, M. (2014); Hoffmann-Riem, W. (2014).
122 France, National Assembly (*Assemblée nationale*), Bill on intelligence (*Projet de loi relatif au renseignement*), as adopted 25 June 2015.
123 These international surveillance measures should be distinguished from those prescribed in Art. L 811–5 (former Art. L 241–3) of the Interior Security Code (*Code de la sécurité intérieure*), as amended, which are not controlled by the French oversight body. See also France, National Commission for the Control of Security Interceptions (CNCIS) (2015a), p. 125 and following calling for the abrogation on this article.
124 France, Constitutional Court (Conseil constitutionnel), Decision No. 2015-713 DC, 23 July 2015. For an example of concerns expressed shortly after adoption of the bill, see French Data Network (*Réseau de données français*) *et al.* (2015), p. 69 and following.
125 France, National Assembly (*Assemblée nationale*), Bill on the surveillance of international electronic communications (*proposition de loi relative aux mesures de surveillance des communications électroniques internationales*), 1 October 2015.

BND's mandate was expanded to include the fight against crime. The 1994 Combating Crime Act (*Verbrechensbekämpfungsgesetz*)[126] amended the G 10 Act, in particular the grounds on which strategic surveillance could be carried out.[127] The BND is authorised to proceed only with the aid of selectors (*Suchbegriffe*), which serve and are suitable for the investigation of one of the threats listed in the law. The BND sets a list of either format-related selectors (e.g. telephone number or email) or content-related selectors (e.g. holy war).[128] The BND needs to specify the region and the percentage of the communication channel it wants to monitor. This percentage cannot exceed 20 % of the full telecommunication channel capacity.[129] In 2013, for example, the BND established a list of 1,643 selectors in the context of internal terrorism to be applied on 906 telecommunication channels, of which only 73 turned out to be useful from an intelligence point of view.[130] The selectors should not contain any distinguishing features leading to a targeted telecommunication connection nor affect the core area of the private sphere. These restrictions do not apply to communications outside Germany, unless they involve German citizens.[131] The list of selectors and the overall request for surveillance is controlled *a priori* by the G 10 Commission, the German oversight body, which decides whether the measures are permissible and necessary.[132] The surveillance order is valid for a renewable three-month period.

In the Netherlands, Article13 (2) of the constitution states that "the privacy of the telephone and telegraph shall not be violated except in the cases laid down by an Act of Parliament, by or with the authorisation of those designated for the purpose by an Act of Parliament".[133] The Intelligence and Security Services Act 2002 (2002 Act) sets the conditions under which the right to privacy of communications may be restricted.[134] The 2002 Act establishes a clear difference between cable-bound telecommunications, for which only targeted surveillance can be used, and non-cable bound (e.g. via satellite and radio waves) telecommunications, for which both targeted and untargeted interception is allowed (Article 27 of the Act).[135] While the act applies to both the civil and military services, this report focuses exclusively on the civil intelligence service, the General Intelligence and Security Service (*Algemene Inlichtingen - en Veiligheidsdienst*, AIVD). AIVD focuses its SIGINT collection on communications intelligence (COMINT), which is the focus of this report because it includes analogue (telephone and telefax) and digital streams, which are transmitted via the Internet. AIVD therefore intercepts communication content and metadata (telephone number, IP addresses, time and duration of the call, as well as location).[136] The Joint Sigint Cyber Unit (JSCU) performs the SIGINT collection for AIVD. It filters the digital streams based on selectors approved by the Minister of the Interior and Kingdom Relations. Analogue communication is not filtered before it is transmitted to AIVD, because the amount of data is quite small nowadays due to the ever increasing development of digital communications.[137] According to Article 27 (2) of the 2002 Act, no permission is required at the stage of untargeted collection and recording. The AIVD seeks the ministers' approval before searching the content of the data provided by JSCU. According to AIVD, a search in the metadata from SIGINT does not require ministerial approval either. This approach, while sound according to Dutch law, has been criticised by the Review Committee, which called for legal reform.[138] The search terms can either be targeted based on a name or number[139] – rules on targeted surveillance then apply – or on a topic.[140] The minister's permission is granted for three months renewable for targeted surveillance. The permission is for a maximum of one year for selections based on topics, since this is less privacy invasive. Figures on the number of untargeted operations performed are not published, despite calls for enhanced transparency by the CTIVD.[141]

126 Germany, Combating Crime Act (*Verbrechensbekämpfungsgesetz*), 28 October 1994.
127 See ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006 for detailed background information and the reasoning underlying the German Constitutional Court's decision to declare parts of the 1994 Act incompatible with the German Basic Law in its judgement of 14 July 1999; Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999.
128 See Huber, B. (2013), p. 2573.
129 Germany, G 10 Act, Section 10 (4).
130 See Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 8.
131 Germany, G 10 Act, Section 5 (2). Academia has questioned whether this nationality-based legislation is compatible with the German constitution and with EU Law. See Schenke, W.-R. *et al.* (2014), p. 1402.
132 Germany, G 10 Act, Section 15 (5).
133 The Dutch government has proposed amending the Constitution and adapting Article 13 to all forms of communications: The Netherlands, Ministry of the Interior and Kingdom Relations (2014). See also: https://zoek.officielebekendmakingen.nl/dossier/33989.
134 The Netherlands, Intelligence and Security Services Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*), 7 February 2002.
135 For a detailed explanation, including an analysis of parliamentary efforts, see The Netherlands, CTIVD (2014), p. 139 and following.
136 See The Netherlands, CTIVD (2014), p. 68 and following.
137 See *Ibid.*,p. 69 and following.
138 See *Ibid.*,p. 96 and following.
139 The Netherlands, Intelligence and Security Services Act 2002, Art. 27 (3) a) and b). In these cases, Art. 25 on targeted surveillance applies.
140 *Ibid.*, Art. 27 (3) (c).
141 See The Netherlands, CTIVD (2015), p. 32.

In Sweden, Articles 1, 2 and 2 (a) of the Signals Defence Intelligence Act[142] mandate a signals intelligence agency (which in practice is the National Defence Radio Establishment (*Försvarets Radio Anstalt*)) to monitor and collect signals intelligence over the airways and by way of fibre optic cables. The Defence Radio Establishment may only intercept wires that cross Sweden's borders.[143] Also, interception may not relate to signals between a sender and recipient who are both located in Sweden. If such signals cannot be separated at the time of interception, the recording or register must be destroyed as soon as it becomes apparent that such signals have been intercepted.[144] The Defence Radio Establishment may not intercept signals intelligence on its own initiative; the government, its offices, the armed forces or its security service must task it to do so, and the Foreign Intelligence Court must approve such requests. The permits are issued for up to six months and can be renewed for further six-month periods.[145] The National Defence Radio Establishment then collects the signals that are transferred to the 'interaction points' by the Communication Service Providers (CSPs), and filters them with the use of certain selectors (or search terms) in an automated manner.[146]

In the United Kingdom, signals intelligence is referred to under the terminology of "interception of external communications in the course of their transmission by means of a telecommunication system" in Section 8.5 of the 2000 Regulation of Investigatory Powers Act (RIPA). This includes the associated communications data. 'Telecommunication system' is defined by RIPA as "any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy".[147] The British Intelligence and Security Committee of Parliament (ISC) refers to this as 'bulk interception'. Warranting of the interception of such external communications is done in the terms set out in Section 8.4 of RIPA, which must be read in conjunction with Sections 5, 15 and 16 of RIPA. Section 5 states that the Secretary of State may only issue a warrant if it is necessary and proportionate, and that, for the interception to be considered necessary, it must be carried out for one of the legitimate reasons in Section 5.3.

The warrant must also include whether the information thought necessary to be obtained could "reasonably be obtained by other means". Such warrants are valid for six months and may be renewed by the Secretary of State. Though a legal distinction is made between external and internal communications (external being those where at least one end is overseas, and internal being UK-to-UK communications), the incidental interception of internal communications is allowed for by Section 5 (6) of RIPA, since making a distinction between the two is practically impossible. Sections 15 and 16 of RIPA set out the applicable safeguards. GCHQ uses this bulk interception capability to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, such as to find terrorist plots, cyber-attacks or other threats to national security.[148] According to the ISC, however, GCHQ only covers a fraction of internet communications since it does not have the capacity to intercept all communications.[149]

Finally, the French parliament adopted in June 2015 a Law on intelligence (*Loi relative au renseignement*).[150] The Constitutional Court reviewed the constitutionality of the bill and confirmed that most of the provisions were in line with the Constitution.[151] The law, which amends the Interior Security Code (*Code de la sécurité intérieure*) and other relevant codes, entered into force on 3 October 2015, with the nomination of the President of the National Commission of Control of the Intelligence Techniques (CNCTR).[152] Among the various intelligence techniques prescribed by law, one is relevant in the context of signals intelligence.

Article L. 851–3 of the Interior Security Code provides for the possibility to oblige telecommunications providers and Internet Service Providers (ISP) to set up automatic processing, based on predefined parameters (generally referred to as algorithms) that could detect a terrorist threat. The algorithms do not enable the identification of the users but only collect 'information or documents' (*informations ou documents*). The French government referred to these as 'digital

142 Sweden, Act on Signals Defence Intelligence (2008:717) (*Lag om signalspaning i försvarsunderrättelseverksamhet (2008:717)*), 10 July 2008. For the government's preparatory efforts on the law, see Sweden, Government Bill 2006/07:46 Processing of Personal Data by the Armed Force and the National Defence Radio Establishment (*Regeringens proposition 2006/07:46, Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt*).
143 Sweden, Act on Signals Defence Intelligence, Section 2.
144 *Ibid.*, Section 2 (a).
145 *Ibid.*, Section 5 (a) second indent.
146 Klamberg, M. (2009); see also, Klamberg, M. (2010).
147 United Kingdom, Regulation of Investigatory Powers Act 2000, 1 August 2000, Section 2 (1).
148 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), p. 25.
149 *Ibid.*, p. 27.
150 France, National Assembly (*Assemblée nationale*), Law No. 2015–912 on intelligence (*Loi n°2015–912 relative au relative au renseignement*), 24 July 2015.
151 France, Constitutional Court (*Conseil constitutionnel*), No. 2015-713 DC, 23 July 2015.
152 France, Law No. 2015–912 on intelligence, Art. 26; France, Decree on the composition of the National Commission of Control of the Intelligence Techniques (*Décret relative à la composition de la Commission national de contrôle des techniques de renseignement*), 1 October 2015.

data' (*données informatiques*) and connexion data[153] but in fact it seems that these notions are not exactly the same.[154] For purposes of this research, it should be understood as 'metadata'.

Taking into account the principle of proportionality, the required authorisation by the prime minister defines the technical scope of this intelligence method. The National Commission of Control of the Intelligence Techniques (CNCTR) provides the prime minister with a non-binding opinion on the algorithms and the parameters chosen. The CNCTR has continuous access to the gathered intelligence and is informed about any modifications. It can also make recommendations. The first authorisation is provided for two months. The renewal request should state the numbers of hits and their relevance for the intelligence services. As soon as the automatic processing provides data that can suggest the existence of a terrorist threat, the prime minister, after having received the opinion of the CNCTR, can authorise the identification of the users. Their data can be analysed within 60 days and should then be destroyed.[155]

In sum, despite legislative efforts to regulate the work of intelligence services, the Council of Europe Commissioner for Human Rights recently concluded that "in many countries, there are few clear, published laws regulating the work of these agencies".[156] The lack of clarity and hence necessary quality of the legal rules governing the work of intelligence services raises fundamental rights issues. It has furthermore triggered lawsuits in a number of Member States.[157] The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, stated that bulk access to communications and content data without prior suspicion "amounts to a systematic interference with the right to respect for privacy of communications, and requires a corresponding compelling justification".[158]

Though it is too early to assess the full impact of the Snowden revelations on legal reforms, post-Snowden inquiries in some Member States indeed led to the conclusion that their current national legal frameworks need to be reformed. The annual report of the French Parliamentary Delegation on Intelligence, the parliamentary oversight body, linked its assessment of the revelations to the need for overarching intelligence reform in France.[159] In the United Kingdom, the post-Snowden inquiry by the Intelligence and Security Committee (ISC) also resulted in the conclusion that the British legal framework is deserving of reform.[160] This was supported by a report issued by the Independent Reviewer of Terrorism Legislation, who stated that the Regulation of Investigatory Powers Act, "obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable."[161]

1.3.2. Surveillance following a legitimate aim

In this report, the notion of national security is examined in light of the mandate of the intelligence services and the surveillance measures they may carry out.

Article 8 (2) of the ECHR states that all interferences with the right to privacy should pursue a legitimate aim. It refers in particular to "national security, public safety or the economic wellbeing of the country". Article 52 (1) of the EU Charter of Fundamental Rights does not refer to specific aims, but states that "any limitation of the exercise of the rights and freedoms recognised by this Charter must [...] respect the essence of those rights and freedoms [...] and genuinely meet objectives of general interest recognised by the Union or protect the rights and freedom of others."

The well-established ECtHR case law acknowledges that secret surveillance measures pursue the legitimate aims mentioned in Article 8 (2) of the ECHR, in particular 'national security'. As illustrated in *Weber and Saravia v. Germany*, the legitimate aim test does not create any major issue in the court's case law.

153 France, Law No. 2015-912 on intelligence, Explanatory note (*exposé des motifs*), 19 March 2015.
154 See French Data Network (*Réseau de données français*) *et al.* (2015), p. 31 and following.
155 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 851-3.
156 Council of Europe Commissioner of Human Rights (2014), p. 109.
157 See for example: France, Constitutional Court (*Conseil constitutionnel*), Association French Data Network and Others, Decision 2015-478 QPC, 24 July 2015, confirming the constitutionality of Arts. L. 246-1 to L. 246-5 of the Interior Security Code; United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014 and 6 February 2015; Poland, Constitutional Court (*Trybunał Konstytucyjny*), K 23/11, 30 July 2014.
158 UN, Human Rights Council, Emmerson, B. (2014), para. 9.
159 France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014).
160 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015).
161 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 8. See also UN, Human Rights Committee (2015b), pp. 10–11.

ECtHR case law: a legitimate aim

"The Government argued that the impugned interferences with the secrecy of telecommunications for the various purposes listed [in the G 10 Act], pursued a legitimate aim. They were necessary, in particular, in the interests of national security, public safety, the economic well-being of the country, and of the prevention of crime. The applicants did not comment on this issue.

The Court shares the Government's view that the aim of the impugned provisions of the amended G 10 Act was indeed to safeguard national security and/or to prevent crime, which are legitimate aims within the meaning of Article 8 § 2. It does not, therefore, deem it necessary to decide whether the further purposes cited by the Government were also relevant."

ECtHR, Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, paras. 103–104.*

Legitimate aim as such is rarely questioned by the ECtHR. The scope of the various legitimate aims could, however, be debated, since the lack of a precise definition may create situations where concepts such as 'national security' acquire a scope that is too broad, and therefore justify undue restrictions of the right to privacy.

According to the ECtHR, notions like national security, the protection of which is a primary aim of the intelligence services, must therefore comply with the 'quality of law' requirements, in particular with the requirement of foreseeability/clarity of the law. The need for a definition in the law is stressed by different actors as a means to preserve the commitment to the rule of law and accountability of the executive and the national intelligence services.[162]

In 1996, experts in the fields of international law, national security, and human rights described national security in the so-called Johannesburg principles as "protect[ing] a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government".[163]

The UN has also made clear that measures that interfere with the right to privacy need a legitimate aim, with statements such as:

> *"That mass surveillance technology can contribute to the suppression and prosecution of acts of terrorism does not provide an adequate human rights law justification for its use. The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not provide an adequate human rights law justification for its use."*[164]

The ECtHR has held that it is difficult to precisely define the concept of national security. Yet, even broadly defined, and leaving a large margin of appreciation to the member states of the Council of Europe, the court assigns to the notion of national security the existence or security of a state; the protection of the democratic constitutional order from terrorism, separatism, or espionage; and the security of the armed forces. On the other hand, the court has clarified that the concept of national security cannot be based on an interpretation that is unlawful, contrary to common sense or arbitrary. The offence of drug trafficking, for instance, is not considered, in any reasonable definition of the term, as falling within the scope of 'national security' in the concrete case of an alien subject to a deportation order. Moreover, the Court requires the threat to national security to have some reasonable basis in facts.[165]

In some EU secondary legislation, 'national security' is explained as state security, for instance in Article 15 (1) of the e-Privacy Directive 2002/58/EC. Moreover, the CJEU in *ZZ v Secretary for the Home Department* implicitly held that the notion of state security as used in EU secondary legislation is equivalent to the notion of 'national security' as used in the national law.[166]

FRA research shows that the concept of national security is not used harmoniously across the EU. In some Member States, the term is not used at all. Instead, the terms 'internal and/or external security', or 'security of the state' are used. In Member States where the term 'national security' is used, it may or may not be defined. Where 'national security' is not defined, however, the additional tasks assigned to the intelligence services resemble those mentioned in other national legal frameworks under the notions of national security, state security, or external/internal security.

162 Born, H. and Leigh, I. (2005), p. 17; Bigo, D. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2014), pp. 35–38, 67 and 82–83; Sule, S. (2006), p. 236.

163 Article 19 (1996), Principle 2 (a).

164 UN, Human Rights Council, Emmerson, B. (2014), p. 6

165 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, paras. 45–46; ECtHR, *Janowiec and Others v. Russia* [GC], Nos. 55508/07 and 29520/09, 21 October 2013, paras. 213–214; ECtHR, *C.G. and Others v. Bulgaria*, No. 1365/07, 24 April 2008, para. 40; ECtHR, *Iordachi and Others v. Moldova*, No. 25198/02, 10 February 2009, para. 46. See also ECtHR: Research Division (2013).

166 CJEU, C-300/11, *ZZ v. Secretary of the State of Home Department*, 4 June 2013, paras. 5, 11, 35, 38 and 54.

In some cases, the notion of national security was inserted into national law under the influence of the European Convention of Human Rights. This is the case in France, for example.[167] The French Law on Intelligence refers to the overarching notion of "fundamental interests of the Nation" (*intérêts fondamentaux de la Nation*), which is defined in Article 410–1 of the Penal Code. This overarching notion, which clearly includes national security, justifies the implementation of surveillance measures in other areas, as well.[168] The French constitutional court considered this aim precise enough and declared it in conformity with the constitution.[169]

In addition, the scope of the various tasks of the intelligence services, i.e. their mandate, are also not identical across the EU Member States. Aside from more traditional fields, i.e. protection of national integrity, sovereignty, or constitutional order, the mandates of some intelligence services include organised crime and cybercrime. These terms are not harmoniously defined, either. There are Member States that narrow down the forms of organised crime to those very few cases that can clearly be identified as a threat to national or state security; others use a much broader catalogue, which is sometimes non-exhaustive. The broader the terms, the lower the requirement of legal clarity and foreseeability. In the latter case, the wide spectrum of organised crimes may allow for the involvement of the intelligence services.

The objective of the protection of economic interests is also part of intelligence services' mandates in several Member States' legislation. This objective is not always defined, either; sometimes it is qualified as either "vital interest" or "crucial interest". The Venice Commission highlights that conducting intelligence activities for the purpose of the economic well-being of a state "may result in economic espionage".[170] The Venice Commission identifies three trade areas where intelligence may be legitimate (proliferation of weapons of mass destruction, circumvention of UN/EU sanctions, and major money laundering), and stresses the need for establishing rules prohibiting economic espionage and rules establishing stronger oversight in this area. Some Member States include further objectives, such as national wealth, the corruption of high state officials, or migration.

Of the five Member States that have detailed legislation on signals intelligence, Germany**,** the Netherlands, and the United Kingdom use the term 'national security' as a reason for gathering such intelligence. The United Kingdom includes in its mandate the prevention or detection of serious crime, the economic well-being of the UK, and the purpose of giving effect to an international agreement.[171] The Netherlands adds the protection of the rule of law and other important state interests.[172] Germany lists situations in which its intelligence service may gather signals intelligence: armed attack, international terrorism, arms proliferation, smuggling of narcotics of substantial important in the EU, counterfeiting of money undermining the stability of the Euro, money laundering, and human trafficking of substantial importance.[173]

Sweden, on the other hand, does not use the term 'national security', but rather lists a series of circumstances permitting it to gather signals intelligence, some of which the law individually identifies as threats to the security of national interests: external military threats, international peacekeeping and humanitarian initiatives, international terrorism or other serious transnational crime, proliferation of weapons of mass destruction, serious external threats to the infrastructure of society, conflicts abroad, foreign intelligence activites against Swedish interests, or a foreign power's actions or intentions of vital importance to Swedish foreign security or defence policy.[174] France adopted a similar approach, specifying what the notion of 'fundamental interests of the Nation' encompasses. It includes national independence, integrity of the territory and national defence; major interests of foreign policy, which include the execution of international and European agreements; economic, industrial and scientific major interests for France; terrorism prevention; prevention of acts affecting: the republican form of government, the reconstitution of dissolved groups and collective violence gravely affecting public peace; prevention of organised crime; and prevention of the proliferation of weapons of mass destruction.[175]

167 France, Law No. 2015-912 on intelligence, Explanatory note. See also France, National Commission for the Control of Security Interceptions (CNCIS) (2015b), p. 120 and following.
168 France, Interior Security Code, Art. L. 811–3.
169 France, Constitutional Court (*Conseil constitutionnel*), No. 2015-713 DC, 23 July 2015.
170 Venice Commission (2015), p. 20.
171 United Kingdom, Intelligence Services Act 1994, 26 May 1994, Section 3 (2).
172 The Netherlands, Intelligence and Security Services Act 2002, Art. 6 (2).
173 Germany, Act on the Federal Intelligence Service, Sections 1 (1) and 2(1); Germany, G 10 Act, Section 5 (1). Section 8 of the G 10 Act also prescribes strategic surveillance in cases of kidnapping.
174 Sweden, Act on Signals Defence Intelligence.
175 France, Interior Security Code, Art. L. 811–3.

FRA key findings

Objective and structure of intelligence services

The main goal of intelligence services in democratic societies is to protect national security and the fundamental values of an open society by using secret intelligence tools. The organisation of the intelligence community in individual EU Member States is closely linked to country-specific historical developments, and does not necessarily abide by fundamental rights standards. As a result, intelligence services are set up in extremely diverse manners across the EU. In some Member States, two intelligence services carry out the work, while in others, five or six bodies are in charge.

- Almost all EU Member States have established at least two different intelligence services bodies, one for civil and one for military matters; the latter are not covered in this report. Civil intelligence services are generally subordinate to interior ministries, and sometimes also to the prime minister or president.

- In some Member States, the civil services are further sub-divided into one service with a domestic mandate and one with a foreign mandate. Moreover, some Member States have entrusted intelligence measures to units specialised in a particular threat, such as organised crime, corruption or the fight against terrorism.

Protecting national security

FRA's research examines the notion of 'national security' in light of the intelligence services' mandate and the surveillance measures they may carry out. Again the findings reveal great diversity among EU Member States.

- The primary aim of the intelligence services is to protect national security, but the concept is not harmonised across EU Member States. The scope of national security is rarely defined, and sometimes similar terms are used. Other Member States do not use the term 'national security' at all and refer instead to 'internal security' and/or 'external security', or to the 'security of the state'.

- The scope of the various tasks of intelligence services (i.e. their mandate) is not identical across EU Member States. In addition to the more traditional fields, the mandates of some intelligence services include organised crime and cybercrime. These terms are not harmoniously defined.

Legal regulation of surveillance

The line between tasks of law enforcement and those of intelligence services is sometimes blurred. Every expansion of tasks must be properly justified as necessary for safeguarding the state, which is the underlying reason for establishing intelligence services.

- Most Member States' legal frameworks only regulate targeted surveillance, either of individuals or defined groups/organisations. In addition to addressing targeted surveillance, five Member States have enacted detailed laws on the conditions for using signals intelligence.

- Looking at applicable human rights standards, national legal frameworks lack clear definitions indicating the categories of persons and scope of activities that may be subject to intelligence collection.

- Intelligence services are regulated by law in the vast majority of Member States (26 out of 28). Legal provisions regulate the organisation and functioning of the countries' intelligence services. One Member State's constitution prohibits its intelligence service from undertaking surveillance. Another Member State is in the process of enacting legislation that will regulate its intelligence services' surveillance practices.

- FRA analysis shows that the legal basis which frames the mandates and powers of the national intelligence services in EU Member States range from one unique legal act governing the organisation and means of the national services, to complex frameworks consisting of several laws and ordinances regulating specific aspects of their mandate, organisation, competences or means.

- Most Member States organise the work of the intelligence services in two laws: one on the mandate and organisation of the service, and another on means of action and the conditions for using them.

- Most EU Member States (23 out of 28) have separated intelligence services from law enforcement authorities. Two Member States have recently moved away from systems in which the intelligence services belonged to the police or similar law enforcement authorities.

2 Oversight of intelligence services

This chapter outlines how oversight mechanisms are established in the EU Member States. It looks at the accountability mechanisms imposed by law on the intelligence services. Future FRA fieldwork research will provide data on how the legal framework is implemented in practice.

The main goal of intelligence services is to protect the fundamental values of an (open) society using secret tools, and, as Born and Leigh put it, "It is because of this paradox (defence of an open society by secretive means), that the security and intelligence services should be the object of democratic accountability and civilian control".[176]

Oversight has thus been defined as "a means of ensuring public accountability for the decisions and actions of security and intelligence agencies."[177] Oversight is aimed at 1) avoiding abuse of power, 2) legitimising the exercise of intrusive powers, and 3) achieving better outcomes after an evaluation of specific actions.[178]

The diversity among EU Member States in terms of politics, history, and legal systems has resulted in a variety of bodies that oversee the intelligence services. Additionally, a great assortment of powers is granted to these various oversight bodies, including the extent to which they may exercise these powers. Though recognising that Council of Europe member states (which include the EU-28) have made great strides in establishing external oversight of their intelligence services, the Council of Europe Commissioner for Human Rights pointed out that few countries have reviewed their effectiveness. He recommended this be done periodically to ensure they remain efficient over time.[179]

> *"There is no Council of Europe member state whose system of oversight comports with all the internationally or regionally recognised principles and good practices [...] and [...] there is no one best approach to organising a system of security service oversight."*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 7*

The general consensus, taken from the Venice Commission report[180] and academic studies,[181] is that oversight should be a combination of:

- executive control;
- parliamentary oversight;
- judicial review; and
- expert bodies.

Judicial review, which mainly occurs as a result of a lawsuit, is covered under Chapter 3 of this report. Judicial involvement in oversight of intelligence services occurs via warranting and monitoring of surveillance measures. However, since these bodies are not exclusively judicial, the broader category of *approval and review of surveillance measures* has been used in this report. The role of the ombudspersons in the oversight of intelligence services is covered in Chapter 3, since it is mainly a complaints-handling body.

By giving diverse powers to an array of bodies that should complement each other, the maximum level of

176 Born, H. and Leigh, I. (2005), p. 16.
177 Born, H. *et al.* (eds.) (2005), p. 7.
178 See Chesterman, S. (2011), pp. 208 and 222.

179 Council of Europe Commissioner for Human Rights (2015), p. 10.
180 Venice Commission (2007).
181 See Born, H. and Leigh, I. (2005), p. 15; Chesterman, S. (2011); Born, H. and Wills, A. (eds.) (2012); Institute for Information Law (2015); Dewost, J.-L.*et al.* (2015), pp. 12 and following.

oversight is guaranteed. Their oversight, however, is only effective if they are independent and granted sufficient powers and resources, both human and financial, to fulfil their mandate. As stated by the CoE Commissioner for Human Rights, "The adequacy of such resources should be kept under review and consideration should be given as to whether increases in security service budgets necessitate parallel increases in overseers' budgets".[182] As outlined in the UN good practices, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism also supports this approach.

UN good practices on oversight institutions

Practice 6. Intelligence services are overseen by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions whose mandates and powers are based on publicly available law. An effective system of intelligence oversight includes at least one civilian institution independent of both the intelligence services and the executive. The combined remit of oversight institutions covers all aspects of the work of intelligence services, including their compliance with the law; the effectiveness and efficiency of their activities; their finances; and their administrative practices.

Practice 7. Oversight institutions have the power, resources and expertise to initiate and conduct their own investigations and have full and unhindered access to the information, officials and installations necessary to fulfil their mandates. Oversight institutions receive the full cooperation of intelligence services and law enforcement authorities in hearing witnesses and obtaining documentation and other evidence.

UN, Human Rights Council, Scheinin, M. (2010)

To achieve the maximum level of protection, in addition to the four layers of legally-based oversight mentioned above, the media and civil society organisations also play an important role. Their impact will be assessed through additional fieldwork research, but the media unquestionably played a crucial role in the Snowden revelations by presenting to the broader public the existence and functioning of large-scale surveillance programmes. Furthermore, NGOs have launched lawsuits in various EU Member States, promoted reforms,[183] developed international principles applicable to oversight of intelligence services,[184] and act as watchdogs of legislative processes.[185] Consequently, it is important that their roles be supported so that they can contribute to the oversight of intelligence matters.

Figure 2 illustrates the points made in this introduction.

Control of the services, however, cannot be limited to external authorities. Intelligence services have a clear responsibility to act within the law, and the law itself can state such a responsibility. Though not strictly 'oversight', since that implies a certain measure of independence, internal control can be achieved by establishing a clear set of internal administrative policies that can guide staff. These are usually not legally established.

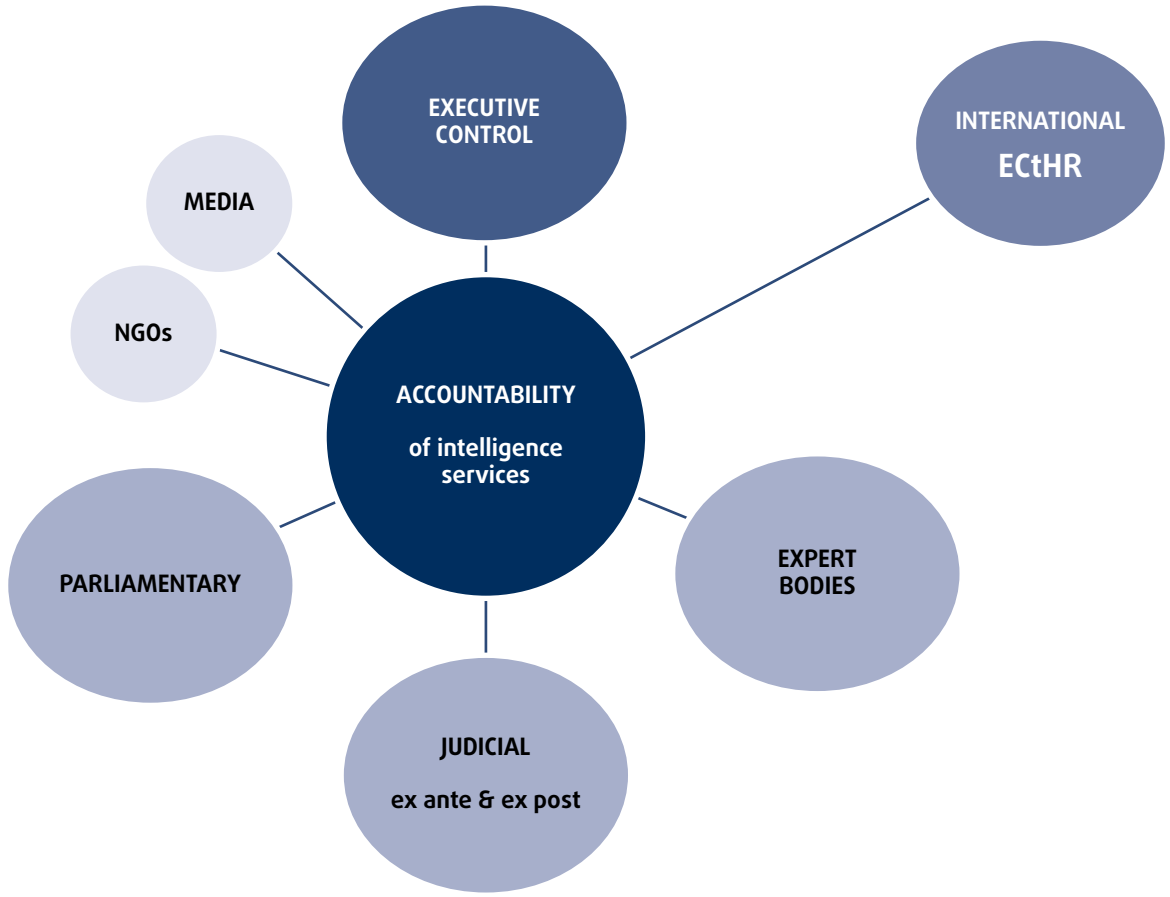
The CoE Commissioner for Human Rights has highlighted the importance of internal control.

> *"It is individual members of security services that play the most significant role in ensuring that security service activity is human rights compliant and accountable. External oversight can achieve little if the security services do not have an internal culture and members of staff that respect human rights."*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 8*

A number of Member States include such internal controls. Sweden, for example, has established data representatives in charge of ensuring that personal data is processed lawfully within the signals intelligence agency (the Defence Radio Establishment). They are appointed by the service itself and report to the Data Inspection Board.[186] The Defence Radio Establishment also has a National Integrity Protection Council, composed of three members, all appointed by the government.[187] The Integrity Protection Council monitors the internal activities of the service. The Council reports its findings to the Defence Radio Establishment and, if necessary, to the State Defence Intelligence Commission (*Statens Inspektion för Försvarsunderrättelseverksamhet,* SIUN),[188] which is one of the oversight bodies.

182 Council of Europe Commissioner for Human Rights (2015), p. 14.
183 See, for example, Löning, M. (2015); Brown, I. *et al.* (2015).
184 See Forcese, C. and LaViolette, N. (2006), Ottawa Principles on Anti-terrorism and Human Rights; Open Society Justice Initiative (2013), Global Principles on National Security and the Right to Information (Tshwane Principles); and Access *et al.* (2014), International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles).
185 See, for example, ECtHR, *Youth initiative for human rights v. Serbia*, No. 48135/06, 25 June 2013. The Serbian intelligence agency denied the applicant NGO information on the number of people subjected to electronic surveillance by the agency, despite an Information Commissioner order supporting the NGO's request. The ECtHR found a violation of freedom of expression, acknowledging the NGO's role in a debate of public interest (para. 24).
186 Sweden, Act on Processing of Personal Data in the National Defence Radio Establishment (2007:259) *(Lag om behandling av personuppgifter i Försvaretsradioanstalts försvarsunderrättelse-och utvecklingsverksamhet (2007:259))*, 10 May 2007, Chapter 4.
187 Sweden, Government Regulation SFS 2007:937, 15 November 2007, Art. 8a and 8b.
188 Sweden, Signal Intelligence Act, 2008:717, 10 July 2008, Art. 11.

Figure 2: Intelligence services' accountability mechanisms



Poland, Germany and the United Kingdom have similar internal controls. Poland employs an "agent for the control of personal data processing" within the Central Anti-Corruption Bureau.[189] In Germany, a staff member within the Federal Intelligence Service, qualified to hold judicial office, supervises the deletion of irrelevant data and assesses regularly whether personal data kept are indeed necessary. For the purposes of oversight and control, this data is stored for one year as log-files. Similar requirements apply to targeted and to strategic surveillance.[190] The Internal Compliance Team within the United Kingdom's GCHQ carries out *ex-post*, internal and random audit checks. Its IT Security Team also conducts technical audits.[191] The results of both are provided to the Interception of Communications Commissioner when s/he carries out inspections. Breaches in security are also reported to the Commissioner after they occur, such as the case of an analyst suspended from duty on discovery of illegitimate searches.[192]

As the Snowden revelations have shown, staff may want to raise concerns about the legality of activities witnessed within the agency. This can be achieved by means of internal controls and through whistleblower provisions, which allow staff to feel secure when doing so. The Dutch bill and French law on intelligence, for example, establish whistleblower protection.[193] In France, members of the intelligence services who come across facts that are in violation of the intelligence law can address the National Commission for Monitoring of Intelligence Techniques (CNCTR), which can then bring the case before the Council of State and inform the prime minister.[194] In Lithuania, intelligence officials may address the Parliamentary Committee on National Security and Defence.[195]

Intelligence services have begun to publish reports related to their activities. These, as expected, do not

189 Poland, Act on Central Anti-Corruption Bureau (*Ustawa o Centralnym Biurze Antykorupcyjnym*), 9 June 2006, Art. 22 (b).
190 Germany, G 10 Act, Sections 4, 6 (1) and Section 8 (4).
191 United Kingdom, IOCCO (2015), p. 26.
192 *Ibid.*, p. 40.
193 The Netherlands, Draft law on the Intelligence and Security Services 20XX, Arts. 114–120.
194 France, Interior Security Code, Art. L. 861–3. See also Foegle, J.-P. (2015).
195 Lithuania, Law of the Republic of Lithuania on Intelligence (*Lietuvos Respublikos žvalgybos įstatymas*), No. XI-2289, 17 October 2012, as amended, Art. 21 (5).

include sensitive information, but constitute a step towards making their role more transparent and accountable to citizens. In Croatia, for instance, the Security and Intelligence Agency (SOA) (*Sigurnosno-obavještajna agencija)* published a report on its activities for the first time in 2014, and invited civil society organisations to give feedback.[196]

2.1. Executive control

> *L'autorité politique « [...] entretient des relations complexes avec 'ses' services, dont elle est, tour à tour, le responsable, le contrôleur, le gardien et le protecteur. »*
>
> The political authority "[...] has complex relations with 'its' services, it is, in turn, the manager, the controller, the guardian and the protector." – FRA translation
>
> *Cousseran, J.-C. and Hayez, P. (2015), p. 27*

The executive branch can control intelligence services in a variety of ways: by establishing their policies, priorities or guidelines; by nominating and/or appointing the service's senior management; by formulating the budget that parliament will ultimately vote on; or by approving cooperation with other services. The executive also plays a crucial role in authorising surveillance measures in some Member States. This power will be addressed in Section 3.3. Examples from Member States illustrate the variety of functions played by the executive.

Figure 3 illustrates the main ways the executive exercises control over the intelligence services across the EU-28. Slovenia[197] and Cyprus are two Member States whose heads of intelligence services are nominated and/or appointed by the executive. The Cypriot CIS is directly accountable to the president of the republic to the extent that when it comes to CIS-related issues, the parliament deals with the presidency itself.

In France, a National Intelligence Council, chaired by the president of the republic, is in charge of ensuring the strategic guidance of the intelligence services and establishing the planning of their human and technical resources. The council comprises the prime minister, relevant ministers, the heads of the specialised intelligence services and the National Intelligence coordinator, who is the president of the republic's advisor and is responsible for coordinating the activities of the intelligence services and ensuring their cooperation.[198]

Bulgaria,[199] Croatia,[200] Italy,[201] and Portugal[202] have similar bodies. In France, the prime minister may also hold the services accountable via the Inspectorate of Intelligence Services, whose members s/he may appoint from among the personnel of existing inspectorates. This body is in charge of monitoring, auditing, researching, consulting, and assessing the services that make up the French intelligence community, which also reports back to the prime minister.[203]

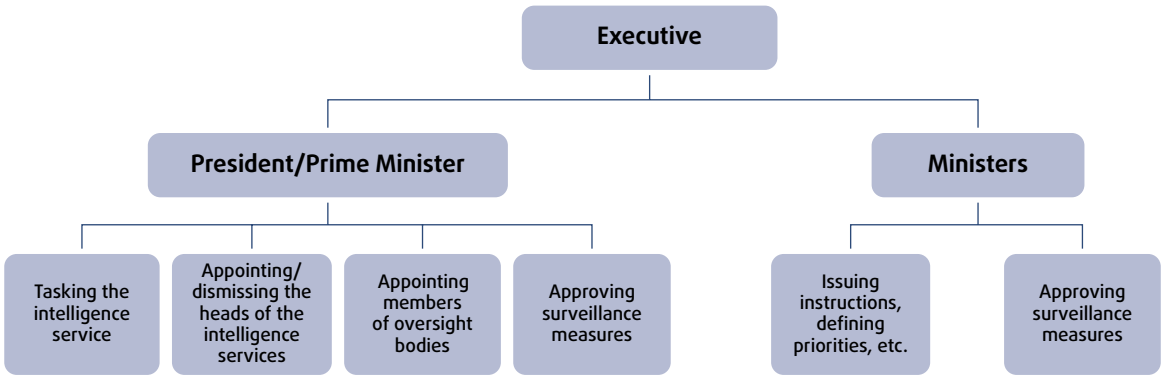
In Poland, the prime minister appoints and dismisses the heads of the Polish intelligence services. S/he is in charge of approving their intelligence objectives and has the most far-reaching competences in terms of oversight of the intelligence services within the country. However, the Supreme Audit Office found that his/her oversight lacks efficacy, since s/he does not have access to the internal procedures of the intelligence services. The information given by the services both as to the content and the means by which intelligence is collected cannot therefore be verified.[204]

Members of the executive other than the president or prime minister may also exercise control over the intelligence services. This is the case in Greece, where the National Intelligence Service is "under the authority of the Minister of Citizen Protection".[205]

The executive plays vastly different roles in the five Member States that have detailed legislation on signals intelligence. In Sweden, the Defence Radio Establishment may not initiate surveillance on its own but must rather act on assignment from the government (or from other authorities, such as the armed forces, Security Service or National Operations Department of the Police Authority).[206] The government is also responsible for appointing the members of most of the supervisory authorities: the board of the Swedish

196 Croatia, Security and Intelligence Agency (*Sigurnosno-obavještajna agencija)* (2014).
197 Slovenia, Intelligence and Security Agency Act, Art. 4.
198 France, Defence Code, Art. R 1122–6, R 1122–7 and R 1122–8.
199 Bozhilov, N. (2007), p. 89.
200 Croatia, Act on the Security Intelligence System of the Republic of Croatia (*Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske*), Official Gazette (*Narodne novine*) Nos. 79/06 and 105/06, 30 June 2006, Art. 1 (2).
201 Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on State secrets, Art. 5.
202 Portugal, Framework Law 30/84 on the Intelligence System of the Portuguese Republic (*Lei Quadro do Sistema de Informações da República Portuguesa),* 5 September 1984, as amended, Art. 18.
203 France, Decree No. 2014–833 on the Inspectorate of intelligence services (*Décret n°2014–833 relatif à l'inspection des services de renseignement*), 24 July 2014.
204 The full content of the report is confidential. See Poland, Supreme Audit Office (*Naczelna Izba Kontroli*) (2014).
205 Greece, Presidential Decree 189/2009 on determination and redistribution of competences of the Ministries *(Προεδρικό Διάταγμα 189/2009 Καθορισμός και Ανακατανομή αρμοδιοτήτων των Υπουργείων), 5 November 2009* (O.G. A 221/5.11.2009), Art. 2, 3rd indent.
206 Sweden, Act on Signals Defence Intelligence, Section 4.

Figure 3: Forms of control exercised over the intelligence services by the executive across the EU-28



Source: FRA (2015)

Defence Intelligence Commission,[207] privacy protection officers (who monitor the individual's interest in cases brought before the Foreign Intelligence Court),[208] members of the Foreign Intelligence Court,[209] the Privacy Protection Council,[210] and the Chancellor of Justice.[211] In its assessment of the Swedish law on Signals Intelligence, the UN's Human Rights Committee remarked that the law provides the executive with wide powers of surveillance in respect of electronic communications, stating that "the State party should take all appropriate measures to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant, and be consistent with obligations under article 17 of the Covenant. To that effect, the State party should guarantee that the processing and gathering of information be subject to review and supervision by an independent body with the necessary guarantees of impartiality and effectiveness".[212]

In the United Kingdom, secretaries of state generally authorise surveillance measures,[213] while the prime minister plays an important role by appointing the two Commissioners in charge of overseeing the intelligence services,[214] as well as nominating the members of the Intelligence and Security Committee of Parliament.[215]

In France, the prime minister approves all surveillance measures after receiving an opinion of the oversight body, the CNCTR. The relevant ministers seek the prime minister's authorisation by providing a detailed justification for the surveillance measure.[216] The emergency procedure enabling the prime minister to authorise a surveillance measure before receiving the CNCTR opinion is not permitted in the context of signals intelligence.[217]

In Germany, the federal chancellery is in charge of supervising and coordinating the work of the intelligence services. It defines the work and intelligence priorities of the intelligence service (BND).[218] The Ministry of the Interior also plays a role in accepting both targeted and strategic surveillance requests. Upon a request by the head of the intelligence service, the ministry studies the merit of the interception order, puts any favourable decision in writing, and forwards it to the G 10 Commission, which is in charge of its final approval. The Ministry of the Interior may also authorise surveillance in urgent cases, but the authorisation is subject to review by the G 10 Commission.[219] There are, therefore, a series of checks and balances in place.

In the Netherlands, on the other hand, executive control manifests in the Minister of Interior, who, together with the Minister of Defence and the minister of general affairs (the Prime Minister), is in charge of nominating the coordinator for the intelligence service (AIVD). The prime minister and the Minister of General Affairs, in accordance with other relevant ministers, instruct the coordinator.[220] The Minister of Interior then reports to parliament biannually regarding the work of AIVD. Though the work of the executive in implementing the

207 *Ibid.*, Section 10.
208 *Ibid.*, Section 6.
209 *Ibid.*, Section 2.
210 *Ibid.*, Section 11.
211 Sweden, The Chancellor of Justice (*Justitiskanslern*, JK), www.jk.se/.
212 UN, Human Rights Committee (2015c).
213 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 7 (1) (a).
214 *Ibid.*, Sections 57 (1) and 59 (1).
215 United Kingdom, Justice and Security Act 2013, 25 April 2013, Section 1 (5).
216 France, Interior Security Code, Art. L. 821–1 and Art. L. 821–2.
217 *Ibid.*, Art. L. 821-5 and Art. L. 851–3.
218 Germany, Act on the Federal Intelligence Service, Sections 1 and 12.
219 Germany, G 10 Act, Section 15 (6).
220 The Netherlands, Intelligence and Security Services Act 2002, Arts. 1 and 4.

Intelligence and Security Services Act is subject to oversight by the Dutch expert body, this is not done to the same extent as in Germany. The Review Committee on the Intelligence and Security Services may request information and the minister's cooperation, and can give the minister unsolicited advice.[221]

Care should be taken, however, to ensure that executive control does not displace that exercised by other, equally necessary oversight bodies. There should also be a clear separation of powers between those involved, since the aim "is that security and intelligence agencies should be insulated from political abuse without being isolated from executive governance".[222] The following sections will show that a number of EU Member States do not provide their external oversight bodies with broad powers, backed by effective independence and means. They therefore rely heavily on executive control. As Born and Wills have noted, the executive plays an intrinsic role and should always be informed about the work of the services. They further argue that it may not have a strong interest in revealing failures within the intelligence services when they occur due to the potential political cost,[223] which is why oversight must include, but not be restricted to, the executive.

2.2. Parliamentary oversight

Parliamentary oversight is very important because of parliament's "supreme responsibility to hold the government accountable"[224] and may be done in a variety of ways. Parliament, as the lawmaker, is responsible for enacting clear, accessible legislation and establishing the intelligence services and their organisation, special powers and limitations, or, in its stead, to review the drafts submitted by the executive. It also approves the intelligence service's budget and should play a strong role in scrutinising whether their operations are in line with the laws they set out. However, as stated by the Council of Europe Commissioner for Human Rights, "[T]he nature of these bodies means that most are not in a position to undertake regular, detailed oversight of operational activities including the collection, exchange and use of personal data".[225] The politicisation of oversight committees,[226] and the potential lack of lawmakers' technical competence regarding highly complex information and communications technology matters and the use of new technologies as applied to surveillance activities[227] have been raised as further hurdles.

Expert collaboration is indispensable. Parliamentarians cannot make correct legal assessments if these are based on wrong assumptions of how technology works. This would prevent effective oversight, hence the need of special arrangements in law to ensure proper support or interaction between experts and members of parliament.

Except for Ireland, Malta, Finland and Portugal, Member States have parliamentary committees that deal with the intelligence services. The powers granted to them, however, vary.[228] Cyprus, Greece and Sweden have not set up specific parliamentary committees, but rather rely on standing committees with broader remits.

2.2.1. Mandate

> *"In order to enjoy legitimacy and command trust it is vital that parliamentary oversight bodies in this area have a broad mandate, are appointed by parliament itself and represent a cross-section of political parties".*
>
> *Born, H. and Leigh, I. (2005), p. 85*

The different parliamentary committees across the Member States have varying mandates. Their powers can include overseeing the policies, administration, budget and expenditure of the intelligence services; receiving periodical reports from the services themselves or from the members of the executive that oversee them; and inspecting sensitive documents and records and the premises of the intelligence services. Some may also receive complaints from individuals. Some Member States have set up one parliamentary committee to deal with the various security and intelligence services, whereas others have created various committees to deal with the services individually. The former is recommended by the Venice Commission, since it allows the committee to carry out more far-reaching oversight and to "cross agency boundaries".[229]

Table 1 categorises the various parliamentary committees in the EU Member States according to their powers. For Member States that have more than one committee in charge of overseeing the intelligence services, the committee with the broadest powers is represented. The table differentiates between essential and enhanced powers. This categorisation is intended to facilitate the comparative analysis, and is not an assessment of the efficiency of the oversight carried out. These powers are categorised according to establishment in law, not in practice. The latter will be evaluated during the fieldwork phase.

221 *Ibid*., Art. 64.
222 Born, H. and Leigh, I. (2005), p. 13.
223 Born, H. and Wills, A. (eds.) (2012), p. 10.
224 Born, H. (2003), p. 36.
225 Council of Europe Commissioner for Human Rights (2015), p. 42.
226 *Ibid*., p. 46.
227 Chesterman, S. (2011), p. 80, Urvoas, J.-J. (2015), p 40.
228 See Wills, A., *et al*., Policy Department C: Citizens' Rights and Constitutional Affairs (2011).
229 Venice Commission (2007), p. 33.

- **Essential powers**
  - has competence overseeing the services' budget and expenditure;
  - may receive reports from the intelligence services and/or the executive and report to parliament;
  - may usually ask the intelligence services and/or the executive to provide the committee with information.

- **Enhanced powers** has essential powers that have been enhanced by:
  - the power to receive complaints/initiate investigations on its own initiative, and the power to subsequently investigate (power to inspect premises and/or access classified information), and issue recommendations or binding decisions; or
  - to be involved in the authorisation process of surveillance measures.

A select few parliamentary committees have been granted extensive powers that go beyond the more traditional role of parliament as an overseer. Among its other powers, for instance, Hungary's parliamentary committee may receive complaints on illegal activity of the intelligence services. The committee has the power to carry out investigations, may inspect the registers and documents of the services, and hear their staff. It then forwards its position to the minister so s/he can initiate an examination of liability.[230] Romania has two committees for defence, public order, and national security (one of the Senate, the other of the Chamber of Deputies), and two Joint Permanent Commissions of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the activity of the Romanian Intelligence Service, and over the External Intelligence Service. The committees may request reports, information and documents from the security agencies; may conduct investigations and submit reports to the parliament,[231] whereas the Joint Commissions also monitor the activities of the intelligence services; have the power to issue binding decisions; and investigate any complaints made against the intelligence services.[232]

In Luxembourg, on the other hand, the Parliamentary Control Commission has the power to conduct checks on specific issues. At the end of each review, the commission then files a confidential report that includes findings, conclusions and recommendations to its members, the prime minister, and the Director of the Intelligence. This may also be requested by the prime minister. The committee is also informed every six months of surveillance measures of communications ordered by the prime minister.[233]

The Belgian Monitoring Committee of the Chamber of Representatives responsible for monitoring the Standing Committee P (Standing Police Monitoring Committee) and the Standing Committee I (Standing Intelligence Agencies Review Committee), is unique in that it does not deal with the intelligence services themselves but rather supervises the expert bodies that oversee the police and intelligence services. It can also instruct Standing Committee I to investigate the intelligence services, to issue advice on legislation and to analyse the reports the Standing Committee submits to it.[234]

Parliamentary committees with more traditional powers, such as receiving reports, giving opinions on draft laws, making recommendations, or evaluating candidates for heads of intelligence services, exist in

230 Hungary, Act CXXV of 1995 on the National Security Services (*A nemzetbiztonsági szolgálatokról szóló 1995. Évi CXXV. törvény*), 28 December 1995, as amended, Section 14 (4).

231 Romania, Decision No. 28/2005 of the Romanian Senate concerning the regulation for the functioning of the Romanian Senate (*Hotărârea nr. 28/2005 privind Regulamentul Senatului*), 24 October 2005, Art. 67 (b) and (c); Romania, Decision no. 8/1994 of the Romanian Chamber of Deputies concerning the regulation of the functioning of the Chamber of Deputies (*Hotărârea nr. 8/1994 privind Regulamentul Camerei Deputaților)*, 24 February 1994, Art. 61.

232 Romania, Decision No. 30/1993 of the Romanian Parliament concerning the organization and functioning of The Joint Permanent Commission of the Senate and the Chamber of Deputies for the Exercise of Parliamentary Control over the activity of the Romanian Intelligence Service (*Hotararea nr. 30/1993 a Parlamentului Romaniei privind organizarea și funcționarea Comisiei comune permanente a Camerei Deputaților și Senatului pentru exercitarea controlului parlamentar asupra activității Serviciului Roman de Informații*), 23 June 1993, Art. 5 (a), (b) and (c); Romania, Law No. 1/1998 concerning the organisation and functioning of the External Intelligence Service (*Legea nr. 1/1998 privind organizarea si functionarea Serviciului de Informatii Externe*), 6 January 1998, Art. 6 (a), (e) and (f).

233 Luxembourg, Act of 15 June 2004 on the organisation of the State Intelligence Service (*Loi du 15 juin 2004 portant organisation du Service de Renseignement de l'Etat*), 15 June 2004, as amended, Art. 15.

234 Belgium, Organic Law on the control of police and intelligence services and the Coordination Unit for Threat Assessment (*Loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace*), 18 July 1991, Art. 32, 33 and 35 (2). See also, Belgium, Standing Committee I (2014), p. XV.

Table 1: Categories of powers exercised by the parliamentary committees as established in law

Member State	Essential powers	Enhanced powers
AT	X	
BE	X	
BG	X	
CY	X	
CZ	X	
DE		X
DK	X	
EE	X	
EL	X	
ES	X	
FI		
FR	X	
HR	X	
HU		X
IE		
IT	X	
LT	X	
LU		X
LV	X	
MT		
NL	X	
PL	X	
PT		
RO		X
SE	X	
SI	X	
SK	X	
UK	X	

Note: *Finland, Ireland, Malta and Portugal do not have parliamentary committees that deal with intelligence services.*
Source: *FRA, 2015*

Latvia,[235] Poland,[236] Estonia[237] and Austria.[238] The Czech parliamentary committee for the Control of the Security Information Service, for instance, possesses no investigative powers. It receives reports from the service and can request information where it believes the activity of the service entails illegal limitations on the rights and freedoms of individuals (or classified information has been disclosed). It cannot, however, access the files itself. If it establishes that there has been a breach of law, it must inform the appropriate minister, head of the service, and a prosecutor.[239]

The powers granted to some parliamentary committees, are limited, which makes fulfilling their mandate difficult. The Lithuanian Parliamentary Committee on National Security and Defence, for instance, may receive complaints from the public, but does not have the power to carry out inspections or audits, and so

235 Latvia, Law on State Security Institutions (Valsts drošības iestāžu likums), 19 May 1994, Section 25.
236 Poland, Resolution of the Polish Sejm on Polish Sejm Rules of Procedure (*Uchwała Sejmu Rzeczypospolitej Polskiej Regulamin Sejmu Rzeczypospolitej Polskiej*), 30 July 1992, Art. 140.
237 Estonia, Security Authorities Act (*Julgeolekuasutuste seadus*), 1 March 2001, Section 36; Estonia, Riigikogu Rules of Procedure and Internal Rules Act (*Riigikogu kodu- ja töökorra seadus*), 17 March 2003, Section 22.
238 Austria, Rule of Procedure Act 1975 (*Geschäftsordnungsgesetz 1975*), 4 July 1975, as amended, Section 32 (b).
239 Czech Republic, Security Information Service Act (*Zákon o Bezpečnostní informační službě*), 7 July 1994, Art. 19.

cannot resolve the complaint with an adequate investigation.[240] Without access to classified documents, oversight bodies rely on the data provided to them by the executive or the services themselves. This does not allow for independence or effective oversight. In agreement with this, the Council of Europe Commissioner for Human Rights has recommended that oversight bodies have access to all the information necessary to fulfil their mandate, regardless of its level of classification.[241]

The parliamentary committees of other Member States focus more on the executive. This is the case, for example, in Denmark and Estonia, as they receive reports from the government on the work of the intelligence services. The Danish Folketing's Parliamentary Control Committee can issue statements to the government, but they are non-binding.[242] The Estonian Special Committee on Oversight of the Security Authorities can refer offenses to the investigative body or the Chancellor of Justice and has other powers, such as the right to summon persons and require documents for examination.[243] Cyprus' House of Representatives deals directly with the president. This is due to the country's unique situation: there is no law regulating CIS' functioning, meaning it is not clear whether CIS can be considered a public service, and therefore subject to scrutiny by any of the existing parliamentary committees. The House of Representatives has not established a special parliamentary committee to oversee the intelligence services, and itself carries out very limited oversight.

Even parliamentary committees that are granted essential powers vary considerably. The Italian parliamentary Committee for the Security of the Republic (COPASIR), for instance, has quite different responsibilities. The reporting obligations of the intelligence services are quite broad and cover aspects such as the requests for telephone-tapping made by the services, or cases in which the services claim it is necessary to classify certain information as a state secret.[244] It may also inspect the offices of the Information System, the complex set of bodies and authorities that make up the intelligence community. COPASIR also has the power to order the President of the Council of Ministers to conduct internal investigations in the presence of seeming illegality. The results of such investigations are submitted to the committee.

Other parliamentary committees may hold hearings with members of the executive or intelligence services, such as in France,[245] Greece,[246] Italy[247] or Croatia,[248] or carry out on-site oversight, such as in Slovenia[249] and Croatia.[250]

In general, intelligence services' budgets are controlled by parliament, giving parliamentarians substantial leverage. A great majority of oversight parliamentary committees have a say on the appropriation of funding. Germany, exceptionally, has a separate parliamentary committee in charge of the budget – the Trust Panel (*Vertrauensgremium*), which also decides on investment in surveillance technologies. One of its members can participate in the meetings of the Control Panel and one of the members of the Control Panel participates in the deliberations of the Trust Panel.[251]

Among the five Member States that have detailed legislation on signals intelligence (France, Germany, the Netherlands, Sweden and the United Kingdom), the German Parliamentary Control Panel, which is prescribed by Article 45 (d) of the German Basic Law (*Grundgesetz*), i.e. constitution, was granted the broadest powers of oversight over its intelligence services. It is tasked with supervising the three intelligence services and is responsible for approving important aspects of the strategic surveillance the services may carry out.[252] It receives biannual reports from the Federal Ministry of the Interior regarding the implementation of the G 10 Act, which provides the legal basis for the strategic surveillance. The control panel has the right to request information from the federal intelligence authorities, to inspect their premises and to commission reports by external experts. It reports twice during the legis-

240 Lithuania, Law of the Republic of Lithuania on Intelligence, Art. 21.
241 Council of Europe Commissioner for Human Rights (2015), p. 13.
242 Denmark, Bill No. 162 of 27 February 2013 on the Act amending the Act on the establishment of a Parliamentary Committee regarding FE and PET (*Lovforslag nr. 162 af 27, februar 2013 om lov om ændring af lov om etablering af et udvalg of Forsvarets og Politiets Efterretningstjenester*), 27 February 2013, Section 2.
243 Estonia, Security Authorities Act, Section 36.
244 Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on State secrets, Arts. 31–34.
245 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies (*Ordonnance n°58-1100 relative au fonctionnement des assemblées parlementaires*), 17 November 1958, as amended, Art. 6 nonies, III.
246 Greece, Standing Orders of the Hellenic Parliament (Κανονισμός της Βουλής), 22/24 June 1987, as amended, Art. 43A (2) (a).
247 Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on State secrets, Art. 31 (1).
248 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 105 (1).
249 Slovenia, Parliamentary Supervision of the Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in* varnostnih *služb*), 26 February 2003, Art. 24.
250 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 104 (4).
251 Germany, Federal Budget Order (*Bundeshaushaltsordnung*), 19 August 1969, as amended, Section 10 (a); and Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, Section 9. See also de With, H. and Kathmann, E., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 225.
252 Germany, G 10 Act, Sections 5 and 8. See also Germany, Parliamentary Control Panel Act.

lature to the parliament.[253] A whistleblower mechanism provides for the possibility of being approached directly by intelligence service staff. However, the fact that its access to files and information may be limited by the "direct executive responsibility" of the Federal government means that it has restricted powers.

Sweden, in contrast, does not have a specialised parliamentary committee to oversee its intelligence services. The work of the intelligence services does, however, fall within the remit of two standing committees within the parliament: the Committee on Justice and the Committee on Defence. The Committee on the Constitution is also significant as it is responsible for the areas of fundamental rights, data protection and privacy.[254] One of the main problems in the realm of parliamentary oversight is that parliamentarians might not dedicate enough time to SIGINT-related matters due to their busy schedules.[255] This is exacerbated if this supervision is only a small part of the agenda of a committee with a broader mandate. Non-specialised committees, moreover, will find it more difficult to develop expertise in the area, since intelligence-related matters have a steep learning curve.

The French parliamentary oversight body – the parliamentary intelligence delegation (*délégation parlementaire au renseignement,* DPR) – has had its powers widened relatively recently (created in 2007, strengthened in December 2013), though it still faces certain restrictions. It examines and assesses governmental policy in the area of intelligence. It does not oversee the services directly, and may conduct hearings and request reports, and can make recommendations to the president of the republic and the prime minister. It also oversees the expenses of the intelligence services through the Audit Commission on special funds (*Commission de verification des fonds spéciaux*), which is composed of four members of the DPR. It does not, however, have access to information on ongoing operations carried out by the services, regarding governmental instructions given to them, or surveillance methods or exchanges with foreign services.[256]

In the United Kingdom, the Intelligence and Security Committee (ISC) is in charge of examining or overseeing the expenditure, administration, policy and operations of the security and intelligence services. However, it may not consider particular operational matters that involve ongoing intelligence or security operations, unless tasked to do so by the prime minister, or unless the information is provided voluntarily to the committee by the security or intelligence services, or another government department. In practice, however, as evidenced by Leigh, the ISC looks at operational material on its own initiative.[257] Nevertheless, since the ISC does not have formal investigative capacities and cannot corroborate the evidence it receives from the services, it must operate upon trust.[258] The ISC may also examine or oversee any other activities of the government in intelligence and security matters that are set out in a memorandum of understanding. Though it may request the chiefs of any of the three main intelligence and security services to disclose certain information, this may be vetoed by the secretary of state.[259] Its reports, whether annual or *ad hoc*, must be sent to the prime minister, who may redact them before they are sent to parliament.[260] The services may also request the redaction of certain information from the committee's reports, but these must be justified, and the committee has the final say.[261] The ISC may only report to the prime minister on national security-sensitive matters.[262] Following the Snowden revelations, the ISC carried out an 18-month-long inquiry and published its findings in March 2015, providing an overview of the legislation that governs the services and their intrusive capacities.[263] The findings conclude that while their capabilities are necessary, the complex, disperse legislation in place should be replaced by a new, comprehensive, detailed act of parliament that covers the services' intrusive powers, safeguards and oversight, as well as the intelligence sharing regime.

The Dutch parliamentary committee is composed of 11 members. It exercises parliamentary oversight over the government intelligence policy and looks in particular at the efficiency, effectiveness, lawfulness and budget of the intelligence service.[264]

Remarkably, the majority of parliamentary committees do not have access to classified information received from foreign secret services. This is explicitly

253 See Germany, Federal Parliament (*Deutscher Bundestag*) (2013), the latest report covering November 2011 to October 2013. See also de With, H. and Kathmann, E., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 218; Heumann, S. and Wetzling, T., Stiftung neue Verantwortung (2014).

254 Sweden, Parliament, The 15 parliamentary committees, www.riksdagen.se/en/Committees/The-15-parliamentary-committees/.

255 Venice Commission (2015), p. 30.

256 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6 nonies, I 4°. See also France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014), p. 13 and following and Urvoas, J.–J (2015), p. 41 and following.

257 Leigh, I. (2013), p. 436.

258 *Ibid.*, p. 441.

259 United Kingdom, Justice and Security Act 2013, Section 4 (2) (b) of Schedule One.

260 *Ibid.*, Sections 2 (3) and 2 (4) of Part 1.

261 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), p. iv (foreword).

262 United Kingdom, House of Commons Library (2013), p. 3.

263 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015).

264 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*)(2014), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', www.tweedekamer.nl/kamerleden/commissies/IV/index.jsp.

stated in the cases of Spain,[265] France[266] and the United Kingdom,[267] among others. This stems from the fact that, as In't Veld and Ernst stated, "The growing cooperation between national intelligence agencies has not been adequately matched by international collaboration between national oversight bodies".[268] Therefore, in practice there is for the most part no oversight of intelligence sharing.

> *"[Member states of the Council of Europe must] ensure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies".*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 13*

2.2.2. Composition

The appointing authority of a parliamentary committee should be parliament itself. This is the case in the vast majority of countries, allowing them to enjoy more legitimacy. However, in some Member States, such as the United Kingdom, the prime minister nominates the members of the parliamentary committee (after consulting the leader of the opposition), who are later elected by parliament.[269]

Many Member States include mandatory proportional representation rules on membership. This is the case in Estonia, Greece, Finland, Hungary and Italy.[270] In Austria,[271] Belgium[272] and Denmark,[273] each political party or political group represented in parliament has at least one member on the committee, as is the case in the Netherlands,[274] where the chairperson of each parliamentary group is a member. This is also true for the presidents of the political groups in Luxembourg.[275]

In Croatia, the members of the Committee for Internal Affairs and National Security of the Croatian parliament are chosen according to the general rules for the selection of members of parliamentary committees from members of parliament with an interest in national security matters.

To reinforce the legitimacy of parliamentary committees, Born and Leigh recommend that the committees "be chaired by a member of the opposition, or that chairmanship rotate between the opposition and the government party".[276] This is the case in various Member States, including Croatia,[277] Hungary,[278] Germany[279] and Italy.[280]

In France, the chairpersons of the standing committees of the National Assembly and Senate respectively charged with internal security affairs and defence are *de facto* members of the Parliamentary Delegation on Intelligence, and alternately hold the position of chair for one year.[281] In Spain, its members are the president of congress and the congressmen who have access to official secrets,[282] which eradicates the need to again vet the committee's members when they join the parliamentary committee.

UN good practices on oversight institutions

Practice 8. Oversight institutions take all necessary measures to protect classified information and personal data to which they have access during the course of their work. Penalties [should be] provided for the breach of these requirements by members of oversight institutions.

UN, Human Rights Council, Scheinin, M. (2010)

265 Spain, National Intelligence Centre Act, Art. 11 (2).
266 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6.
267 United Kingdom, Justice and Security Act 2013, Section 5(c) of Schedule 1.
268 European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013b).
269 United Kingdom, Justice and Security Act 2013, Sections 1 (3) and 1 (5).
270 Wills, A. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2011).
271 Austria, Rule of Procedure Act 1975, Section 32 (b). See also Austria, Parliament (*Parlament),* Permanent sub committees to control intelligence services, http://www.parlament.gv.at/ENGL/PERK/KONTR/POL/6STAEND_UNTERAUSSCHUESSE/index.shtml
272 Belgium, Rules of Procedure of the Chamber of Representatives (*Règlement de la Chambre des représentants*), 2 October 2003, as amended, Art. 149.
273 Wills, A. *et al.* Policy Department C: Citizens' Rights and Constitutional Affairs (2011).
274 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*) (2014), Commissie voor de Inlichtingen- en Veiligheidsdiensten, Web page, www.tweedekamer.nl/kamerleden/commissies/IV/index.jsp.
275 Luxembourg, Act of 15 June 2004 on the organisation of the State Intelligence Service, Art. 14.
276 Born, H. and Leigh, I. (2005), p. 85.
277 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 105 (4).
278 Hungary, Act CXXV of 1995 on the National Security Services, Section 14 (1).
279 Germany, Federal Parliament (*Deutscher Bundestag*), https://www.bundestag.de/bundestag/gremien18/pkgr
280 Wills, A. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 140.
281 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6 nonies.
282 Spain, Act 11/1995 regulating the use and control of secret funds (*Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados*), 11 May 1995, Art. 7 (1).

UN good practice 8 calls for mechanisms that ensure preservation of secrecy. Vetting, that is to say, assessing parliamentarians' backgrounds to identify any risks involved in providing the MPs with security clearance, is one way of ensuring the protection of classified information. It is required in the parliamentary oversight committees of Estonia, Hungary, Latvia, Lithuania, and Poland.[283]

The MPs of most Member States are however not subject to such procedures, and do not require security clearance. This is because in many Member States, such control would be regarded as a violation of the separation of powers. In Slovenia, for instance, the Classified Information Act states that parliamentarians who sit on the Commission of the National Assembly for the Supervision of Intelligence and Security Services do not require authorisation to access classified information in the exercise of their functions.[284]

2.2.3. Access to information and documents

> *"[A]ll bodies responsible for overseeing security services [should] have access to all information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law and supported by recourse to investigative powers and tools which ensure such access. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate."*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 13*

Access to information and documents by oversight bodies is essential for adequate oversight. While information gathered by intelligence services is sensitive and safeguards are required to guarantee that it will be dealt with accordingly, oversight bodies cannot carry out their tasks without access to the information necessary to make an informed decision and carry out apt supervision. The opposite, however, seems to be the norm.

As shown by the table on *Security clearance for members and staff of specialised oversight committees* in Wills, Vermeulen *et al.*'s report for the European Parliament, members of parliamentary committees tend to have access to classified information.[285] However, the law always qualifies the right of access, and no parliamentary committee has *unrestricted* access. In Italy, for instance, COPASIR may request information from the judiciary, private and public bodies, and the intelligence services, who may not allege investigational, professional or state secrets in return. However, this power is limited when the disclosure of the information or the transmission of a copy of a document can affect the safety of the republic, relations with foreign countries, the performance of ongoing operations or the safety of sources of information, employees or members of the services' information security. Nevertheless, if the committee insists, its request will be evaluated by the President of the Council of Ministers. If the committee does not agree with the President of the Council of Ministers' decision, or receives no response within 30 days, COPASIR may forward the issue to each of the houses for their assessment.[286]

In Germany, the Parliamentary Control Panel has the right to request information, documents and other data files from the federal government and the three intelligence services. However, the obligation of the government and the intelligence services to provide information covers only documents the government has produced, and not, for example, those of foreign services or documents that would affect the personal rights of third parties.[287] Though the Control Panel's members are sworn to secrecy, they can comment publicly on certain issues, as long as the decision to do so is reached by two-thirds of its members.[288] It may also request expert witnesses to submit evaluations, which are forwarded to parliament as reports.[289]

In Austria, the Standing Sub-Committee of the Committee on Internal Affairs (*Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten*) controls the work of the Federal Agency for State Protection and Counter Terrorism (BVT). It is entitled to ask the relevant minister for information. However, these are not obliged to provide the information if they are not in a position to do so, or if it might jeopardise national interests or the safety of persons.[290] Likewise, the United Kingdom's Intelligence and Security Committee may also obtain information from agencies and government departments, except where the secretary of state blocks disclosure of "sensitive information".[291]

Luxembourg's Parliamentary Control Committee is also authorised to access any information and documents it considers relevant to the performance of its duties, with the exception of information or documents that could reveal the identity of a source or that would impair

283 Wills, A. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 138 f.
284 Slovenia, Classified Information Act (*Zakon o tajnih podatkih*), 25 October 2001, Art. 4.
285 Wills, A. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 142.
286 Italy, Law No. 124/2007 on the Information System for the security of the Republic and new rules on state secrets, Art. 31 (8 to 10).
287 Germany, Parliamentary Control Panel Act, Section 6.
288 *Ibid.*, Section 10 (2).
289 *Ibid.*, Section 7. See also Dietrich, J.-H. (2015), p. 14.
290 Austria, Rule of Procedure Act 1975, Section 32 (c) (2).
291 United Kingdom, Justice and Security Act 2013, Section 4 (4) of Schedule 1.

the rights of third parties.[292] It can also request assistance from external experts when it requires special knowledge.[293] This ensures that technical information is not overlooked by, in this case, parliamentarians who may not have the proper training or expertise. This is in line with the CoE Commissioner for Human Right's recommendation that "oversight bodies should have recourse to specialists in information and communications technology who can enable overseers to better comprehend and evaluate surveillance systems and thus to better understand the human rights implications of these activities".[294]

Therefore, when it comes to the extent of committees' power to initiate their own investigations, the laws of most countries grant parliamentary committees the authority to *request* information from the intelligence services or the executive, but not to *demand* it.

2.2.4. Reporting to parliament

Though most parliamentary committees submit reports at least annually, some reports are made public and others kept secret. As stated by Born, "Democratic oversight can only be effective, as a principle of good governance, if the public is aware of major issues open to debate at parliamentary level";[295] therefore, public reporting to parliament furthers transparency and public awareness. To achieve greater transparency and engagement with the public, the CoE Commissioner for Human Rights recommends that publishing public versions of periodic and investigation reports be required by law.[296]

In Austria for example, the reports are kept secret, since the work of the sub-committees is confidential.[297] Similarly in Luxembourg, although the Parliamentary Control Commission submits annual reports to parliament, its checks on the intelligence service are confidential and the results are only submitted on a confidential basis to the prime minister, the head of the intelligence service and deputy members of the parliamentary committee.[298] In Germany, short activity reports presented before parliament are made public.[299] Every other document is kept confidential. In Denmark, on the other hand, there is no obligation for the Parliamentary Control Committee to report annually to parliament. In fact, it has only submitted eight reports on its activities since 1988.

The Intelligence and Security Committee of the United Kingdom reports to parliament annually and may also produce thematic ad hoc reports. The prime minister has the power to exclude beforehand matters considered "prejudicial to the continued discharge of functions" of the agencies.[300] The French Parliamentary Delegation on Intelligence publishes the annual report it makes to parliament. In 2014, the annual report was longer and more detailed than in the past. It covered topics such as the hearings the committee carried out that year, economic surveillance, and recommendations on how to improve the legal framework and supervision of intelligence services to increase citizens' confidence, to name a few.[301]

The Venice Commission recommends that parliamentary committees in charge of overseeing intelligence services have the power to issue more than an annual report, to make sure that their reporting remains relevant and can draw attention to activities that demand urgent responses.[302] It is evident from the above examples that Member State practices are inadequate in this respect.

2.3. Expert oversight

2.3.1. Specialised expert bodies

Expert oversight is exceptionally valuable as it allows for the actions of the intelligence services to be scrutinised by those familiar with the subject, who have time to dedicate to the matter, and are independent of political allegiances. As stated by the CoE Commissioner for Human Rights, they "are often best placed to conduct detailed day-to-day oversight of the legality of security service activity".[303] For their potential to be maximised, however, they must be granted adequate independence, resources and powers.[304] The following table lists the various expert oversight bodies established in the Member States. To provide an overview of how these work across the EU-28, a sample has been explained in the text.

292 Luxembourg, Act of 15 June 2004 on the organisation of the State Intelligence Service, Art. 15 (3).
293 Born, H. and Leigh, I. (2005), p. 93.
294 Council of Europe Commissioner for Human Rights (2015), p. 14.
295 Born, H. *et al.* (eds.), Geneva Centre for the Democratic Control of Armed Forces (DCAF) (2003), p. 41.
296 Council of Europe Commissioner for Human Rights (2015), p. 14.
297 Austria, Rule of Procedure Act 1975, Section 32a (2).
298 Luxembourg, Act of 15 June 2004 on the organisation of the State Intelligence Service, Art. 15 (5) and 15 (8).
299 For the activities of the Parliamentary Control Panel, see German Federal Parliament (2013). Regarding the activities of the G 10 Commission, see the report presented by the Parliamentary Control Panel to Parliament: Germany, Federal Parliament (*Deutscher Bundestag*) (2015).
300 United Kingdom, Justice and Security Act 2013, Section 3 (4) of Part 1.
301 France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (2014).
302 Venice Commission (2007), p. 37.
303 Council of Europe Commissioner for Human Rights (2015), p. 8.
304 See Dewost, J.-L., Pelletier, H. and Delarue, J.-M. (2015), pp. 14 and following.

Table 2: Expert bodies in charge of overseeing surveillance, EU-28

EU Member State	Expert bodies
AT	Legal Protection Commissioner *(Rechtsschutzbeauftragter)*
BE	Standing Intelligence Agencies Review Committee *(Vast Comité van Toezicht op de inlichtingen - en veiligheidsdiensten / Comité permanent de Contrôle des services de renseignement et de sécurité)* Administrative Commission *(Bestuurlijke Commissie/Commission Administrative)*
BG	National Bureau for Control over Special Intelligence Means *(Национално бюро за контрол на специалните разузнавателни средства)*
CY	N.A.
CZ	N.A.
DE	G 10 Commission *(G 10-Kommission)*
DK	Oversight Committee of the Intelligence Services *(Tilsynet med Efterretningstjenesterne)*
EE	N.A.
EL	Hellenic Authority for Communication Security and Privacy *(Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών)*
ES	N.A.
FI	N.A.
FR	National Commission for Control of Intelligence Techniques *(Commission nationale de contrôle des techniques de renseignement)*
HR	Office of the Council for National Security *(Ured Vijeća za nacionalnu sigurnost)* Council for Civic Oversight of Security and Intelligence Services *(Vijeće za građanski nadzor sigurnosno-obavještajnih agencija)*
HU	N.A.
IE	Complaints Referee Designated Judge of the High Court
IT	N.A.
LT	N.A.
LU	Supervisory committee (autorité de contrôle) of Act of 2 August 2002 Commission *(commission)* of the Criminal Investigation Code *(Code d'Instruction Criminelle)*
LV	N.A.
MT	Commissioner of the Security Service *(Kummissarju tas-Servizz ta' Sigurtà)*
NL	Review Committee on the Intelligence and Security Services *(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)*
PL	N.A.
PT	Council for the Oversight of the Intelligence System of the Portuguese Republic *(Conselho de Fiscalização do Sistema de Informações da República Portuguesa)*
RO	N.A.
SE	State Defence Intelligence Commission *(Statens inspektion för försvarsunderrättelseverksamheten)* Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden)* Foreign Intelligence Court *(Försvarsunderrättelsedomstolen)*
SI	N.A.
SK	N.A.
UK	Intelligence Services Commissioner Interception of Communications Commissioner Investigatory Powers Tribunal

Source: FRA, 2015

Across the EU, 15 Member States have set up expert bodies exclusively dedicated to intelligence service oversight. Some of their competences include authorising surveillance measures, investigating complaints, requesting documents and information from the intelligence services, or giving advice to the executive and/or parliament.

> *"In contrast to parliamentary oversight committees, expert bodies conduct their work on a (near) full-time basis. This generally means that they can provide more comprehensive and in-depth scrutiny than their parliamentary counterparts".*
>
> *Council of Europe Commissioner for Human Rights (2015), p. 47*

Providing for parliamentary involvement in the establishment of the expert body and/or the election of its members grants the expert body more legitimacy and helps establish a good rapport between the two.[305] This occurs in Bulgaria, where the National Assembly appoints the five members of the National Bureau for Control over Special Intelligence Means. The bureau has the power to issue binding decisions to the intelligence services on the access, collection, storage and destruction of special intelligence means. It may also access all relevant information required to carry out its work.[306] In Croatia, the specialised parliamentary committee for Internal Affairs and National Security appoints the members of the Council for Civic Oversight of Security and Intelligence Agencies, and its seven members are chosen from among those who answer a public call on the basis of expertise. They are granted full security clearance once selected. The law states that some of its members must be law, political science or electrical engineering graduates.[307]

The Belgian Standing Intelligence Agencies Review Committee (Standing Committee I) is an example of an expert body with broad oversight powers.[308] Its three members are nominated by parliament. One member acts as president of the committee and must be a magistrate. The other two are counsellors and must hold law degrees. The committee members are supported by a five-staff investigation service headed by a magistrate, a member of an intelligence service, a member of a police service, or a public servant nominated by the committee; it also has 16 administrative staff. Among the Standing Committee's key assignments (eight in total) it may initiate investigations on its own initiative, on the request of the Chamber of Representatives or the competent minister or authority, or on the request of a citizen or a civil servant who lodges a complaint or files a denunciation. In a judicial capacity, the Standing Committee I is also responsible for the *ex post* control of 'specific and exceptional data collection methods' used by the intelligence and security services. The term 'specific and exceptional data collection methods' is relatively broad, covering all forms of collection of communications data relevant to this report, since they interfere with individual privacy.[309] Moreover, the Standing Committee I may, on request, advise on bills and regulatory acts or any other document expressing the political orientations of the competent ministers regarding the functioning of the intelligence services or the Coordination Unit for Threat Assessment.

Belgium has a second expert body referred to as the Administrative Commission. It is made up of three acting members and three substitute members, one of whom is a state prosecutor, while the other two are judges. The commission is responsible for monitoring specific and exceptional data collection methods used by the intelligence and security services. It controls the legality, subsidiarity and proportionality of these data collection methods. Furthermore, the implementation of an exceptional method requires the commission's approval.[310]

By contrast, the executive appoints the members of some expert bodies. This is the case, for instance, in Austria, Denmark (except the president of the expert body, who must be a High Court judge, and is nominated by the president of the High Court and the High Court),[311] Sweden and the United Kingdom. The Austrian Legal Protection Commissioner (*Rechtsschutzbeauftragter*, RSB) and his/her two deputies are appointed by the Federal president upon the proposal of the government, after consulting the president of parliament, and the presidents of the constitutional court and the administrative court. The RSB and his/her two substitutes are appointed to the Federal Ministry of the Interior for a five-year term and may be re-appointed. They are independent in the exercise of their functions and are not bound by instructions. RSBs are required to have experience in and knowledge of human rights, and at least five years' experience in a legal profession.[312] The police authorities provide the RSB with full access to documents and recordings necessary for performing his/her tasks. The RSB plays an important role in overseeing the implementation of data protection safe-

305 Venice Commission (2007), p. 50.
306 Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*), 21 October 1997, Art. 34 (b).
307 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 110.
308 Belgium, Organic Law on the control of police and intelligence services and the Coordination Unit for Threat Assessment, Arts. 28, 32, 33, 34 and 35.
309 Belgium, Standing Committee I (2012), p. 55 and following.
310 Belgium, Law on the Intelligence and Security Services (*Loi organique des services de renseignement et de sécurité*), 18 December 1998, Art. 43/1. For a description of the law; see Belgium, Standing Committee I (2011), *Rapport d'activités 2010*, pp. 49–61.
311 Denmark, Act No. 604 on the Danish Security and Intelligence Service as amended by Act. No. 1624, Sections 16 and 16 (2).
312 Austria, Police Powers Act, Section 91 (a).

guards, contributes to remedial actions, and reports annually to the Minister of Interior; this report has to be made available to the parliamentary oversight sub-committee.[313]

The Hellenic Authority for Communication Security and Privacy (ADAE) in Greece is an example of a well-staffed expert body. Its seven members, required to have the appropriate legal and technical expertise, are supported by a staff of 38 with competencies in the sciences to law. ADAE is fully independent and its members are appointed by the Conference of Parliamentary Chairmen.[314] It can carry out inspections, audits, and access the intelligence services' databases and documents. However, it has so far exclusively focused its oversight on telecommunications providers.[315] ADAE also issues statistical data regarding interception carried out by the services, receives complaints and carries out hearings. However, when reviewing interceptions, it must limit its review of their legality. It may not assess judicial holdings and its findings are not binding.[316]

One of the main issues regarding expert oversight is the lack of clarity about what constitutes the required expertise. In Portugal, for instance, the three candidates of the Council for the Oversight of the Intelligence System of the Portuguese Republic must be citizens of "recognised integrity and in full capability of their civil and political rights".[317] Though their selection follows procedure, it is not clear from the onset what is necessary to fulfil the expert requirements. In most countries, it is common practice for the members of expert bodies to be judges (active or retired). More is necessary to guarantee adequate oversight; for example, specialisation has been put forward as an option.[318] Only Ireland has established the position of a specialised judge, who is in charge of adjudicating matters of communications interception.

Oversight must cover both legal aspects of surveillance and its actual technical implementation, meaning a correct understanding of the technical aspect is essential. Judges are legal, not technology, specialists, and, as noted by the Venice Commission, do not necessarily have the expertise required to oversee intelligence services. To bridge this gap, oversight bodies should, to the greatest extent possible, be composed of individuals with diverse backgrounds, and, as recommended by the CoE Commissioner for Human Rights, be able to rely on information and communication technology specialists to provide them with a better understanding of surveillance systems and their human rights implications.[319] In France, for example, one member of the CNCTR has skills in electronic communications and is nominated by the Electronic Communications and Posts Regulatory Authority (*Autorité de régulation des communications électroniques et des postes,* ARCEP).[320]

All five Member States with detailed signals intelligence laws have established one or more expert bodies to oversee this capacity of the intelligence services (or part thereof, as with 'open sky' in Germany). However, their mandates are not always comparable.

In Germany, expert oversight is carried out by the G 10 Commission, which has four members and four substitutes. The chairperson must be qualified for judicial office,[321] and its members are elected by the Parliamentary Control Panel. Being a member of parliament is not mandatory.[322] At present, two substitute members are current MPs, and the other members are past MPs.[323] Its main task is to authorise surveillance measures of the intelligence services; to do so, it must meet at least once a month. The G 10 Commission draws up its own procedures, which must be approved by the Parliamentary Control Panel after consultation with the government.[324] It is supported by the same six-person secretariat that works for the Parliamentary Control Panel.

The Dutch three-member Review Committee on the Intelligence and Security Services (CTIVD) is an independent body, assisted in its work by seven staff members.[325] Through in-depth investigations and its "complaints advisory"[326] role, the committee ensures that the intelligence services perform their duties lawfully. To do so, it has unlimited and independent access to AIVD data. Interestingly, to tackle the issue of expertise, the CTIVD established a "knowledge network" composed of scientific experts advising the Review Committee on a regular basis on specific reports relating to technological, legislative and social developments.[327] Indeed, with

313 *Ibid.*, Section 91 (d). A case challenging the RSB's powers is pending before the ECtHR, see ECtHR, *Tretter and Others v. Austria*, No. 3599/10, communicated on 6 May 2013.
314 Greece, Law 3115/2003 on the Hellenic Authority for Communication Security and Privacy *(Ελληνική Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών)*, 27 February 2003, Art. 2 (2); Greece, Hellenic Constitution, (*Σύνταγμα*), 11 June 1975, as amended, Art. 101A; and Greece, Standing Orders of the Hellenic Parliament, Arts. 13 and 14.
315 Greece, Authority for Communication Security and Privacy, Annual reports for the years 2004–2014.
316 Greece, Law 3115/2003 on the Hellenic Authority for Communication Security and Privacy, Art. 6.
317 Portugal, Framework Law 30/84 on the Intelligence System of the Portuguese Republic, Art. 7 (2).
318 Venice Commission (2007), p. 46.
319 Council of Europe Commissioner for Human Rights (2015), p. 14.
320 France, Interior Security Code, Art. L. 831–1 (4).
321 European Network of National Intelligence Reviewers (ENNIR), Intelligence review in Germany, 12 June 2012.
322 Germany, G 10 Act, Section 15.
323 Germany, Federal Parliament (*Deutscher Bundestag*), Composition of the G 10 Commission.
324 ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, para. 21.
325 See The Netherlands, CTIVD (2015), p. 39.
326 The Netherlands, CTIVD (2014), p. 7.
327 See The Netherlands, CTIVD (2015), p. 10.

the increased sophistication of surveillance techniques, which often are automatised, the CTIVD recognised the need for ICT expertise, and invested additional financial resources in technology for carrying oversight.[328]

Following the Snowden revelations, the Dutch parliament asked the oversight body to conduct an in-depth investigation of how intelligence services acquire, use and exchange data with foreign services. The CTIVD concluded that the intelligence services' systematic acquisitions of personal data were done lawfully, but still deemed current privacy safeguards inadequate, and suggested enhancing them.[329] CTIVD also stated that "the potential of AIVD [...] to infringe privacy in the digital domain goes further than was foreseen when the ISS [Intelligence and Security Services] Act 2002 was drafted and enacted", and found some procedures that govern the intelligence services unlawful, calling for stricter oversight of the services' digital activities.[330] Based on past review reports, CTIVD concluded that "the services have not yet been able to establish a procedure that ensures their consistent compliance with the statutory safeguards when selecting from untargeted interception (SIGINT)."[331]

An ad-hoc committee in the Netherlands that presented an assessment of the Intelligence and Security Services Act to parliament suggested granting the intelligence services more extensive powers to intercept cable-bound communication in an untargeted manner. It balanced this call for more power by also recommending that the CTIVD be granted stronger oversight by making its decisions binding.[332] However, while the new draft law indeed grants the services more powers, the committee's opinions remain non-binding.[333]

In the United Kingdom, the Investigatory Powers Tribunal is charged with receiving complaints about surveillance.[334] Two Commissioners oversee the use of the powers established in the Regulation of Investigatory Powers Act: the Intelligence Services Commissioner[335] and the Interception of Communications Commissioner.[336] To be eligible for the position, the commissioners must hold or have held high judicial office. They are appointed by the prime minister and must report to him/her annually and bi-annually, respectively. The prime minister has the power to exclude from the commissioners' annual reports information that would contravene the public interest or be prejudicial to matters such as national security.[337] Specifically, the prime minister sends these commissioner reports to parliament, together with a statement as to whether any matter has been excluded therefrom.[338] No material was excluded from the Interception of Communications Commissioner Annual Report for 2014[339] or from the Intelligence Services Commissioner Annual Report for 2014.[340]

Both commissioners may obtain documents and information from officials and oversee that the warranting carried out by the Secretaries of State is done lawfully. They must also ensure that the safeguards relating to how the intercepted material is used are respected. However, while the Interception of Communications Commissioner has a chief inspector, nine inspectors and two office staff, the Intelligence Services Commissioner works part-time and has a part-time secretary. The efficacy of the commissioners' roles has also been called into question in light of their level of independence and resources. The Interception of Communications Commissioner, for instance, examined only 34 % of interception warrants issued in 2014, an increase of 14 % from the preceding year.[341] Furthermore, some of the intelligence services' powers are not subject to oversight by either commissioner. For example, the Intelligence and Security Committee discovered that GCHQ could access "bulk personal datasets" – large databases of information that are overtly and covertly obtained from private and bulk entities and used for intelligence purposes – and that this was not subject to oversight by any expert body. The prime minister therefore signed a direction putting the use of bulk personal datasets under the competence of the Intelligence Services Commissioner.[342] Though the role of the Interception of Communications Commissioner was found to be a "model" of review bodies by the Independent Reviewer of Terrorism Legislation,[343] the reviewer nevertheless recommended that they be replaced by an Independent Surveillance and Intelligence Commission (ISIC).[344]

328 See *Ibid.*, pp. 10 and 39.
329 The Netherlands, CTIVD (2014), p. 37 and following. See also The Netherlands, CTIVD (2015), p. 28.
330 The Netherlands, CTIVD (2014), p. 5.
331 *Ibid.*, p. 28.
332 The Netherlands, ISS Act 2002 Evaluation Committee (*Commissie evaluatie Wiv 2002*) (2013), Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002, pp. 78–80, 83, 87, 89 and 102. See also The Netherlands, CTIVD (2015), pp. 27–29.
333 The Netherlands, Draft law on the Intelligence and Security Services 20XX.
334 United Kingdom, Regulation of Investigatory Powers Act 2000, Sections 65–70.
335 *Ibid.*, Sections 59 and 60; United Kingdom, Justice and Security Act 2013, Section 5 of Part 1.
336 United Kingdom, Regulation of Investigatory Powers Act 2000, Sections 57 and 58.
337 *Ibid.*, Sections 58(7) and 60(5).
338 *Ibid.*, Sections 58(6) and 60(4).
339 United Kingdom, Interception of Communications Commissioner (IOCCO) (2015).
340 United Kingdom, Intelligence Services Commissioner (2015).
341 United Kingdom, IOCCO (2015), p. 30.
342 United Kingdom, Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015, http://www.intelligencecommissioner.com/docs/PM_Direction_12_March_15.pdf
343 Anderson, D., p. 123.
344 *Ibid.*, p. 280.

Sweden has three expert bodies.[345] The State Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) is tasked with ensuring that the state's defence intelligence is carried out lawfully.[346] SIUN monitors the conduct of the intelligence service and must be informed about the search terms the services apply. It exerts control over the signals that telecommunications carriers must provide to interaction points. SIUN is also in charge of reviewing the processing of personal data by the intelligence service, and ensuring that data collection complies with the permits issued by the Foreign Intelligence Court. It has the power to stop on-going signals intelligence and subsequently order its destruction. SIUN may appoint an expert to assist the committee. The government appoints its seven members, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliamentary party groups. The commission is supported by a secretariat.[347] It currently has six members. The four members nominated by the party groups are all former members of the national parliament. The second expert body, the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*, FUD), will be covered in Section 2.4, since it is in charge of authorising the gathering of signals intelligence. The third expert body, the Commission on Security and Integrity Protection (*Säkerhets- och integritetsskyddsnämnden*, SIN), is in charge of providing individuals with information regarding whether they have been subject to secret surveillance. This commission may access information held by any administrative authority. Its chair and vice chair must be judges or have a similar level of legal experience. Other members (a maximum of eight) are nominated by the party groups in parliament.[348] SIN is not involved in matters linked to signals intelligence.

In France, the law on intelligence set up the National Commission on the Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement,* CNCTR), which replaced the current National Commission on the Control of Security Interception (*Commission nationale de contrôle des interceptions de sécurité*).[349] The law strengthened the powers of the new commission, which comprises nine members: two members of the National Assembly, two senators, two members of the Council of State, two judges of the Court of Cassation and one member with technical skills in electronic communications.[350] They are nominated for six years, apart from the members of parliament, whose mandate is linked to their seat in parliament. The CNCTR is provided with the human, technical and budgetary means needed to accomplish its missions. A secretary general and staff members assist its work. Commission members and staff member have access to secret documents. The CNCTR's work is secret.

The CNCTR ensures that surveillance measures are carried out lawfully in France. It particularly assesses whether prescribed procedures are followed, and whether these respect the right to privacy and the principle of proportionality.[351] Should the CNCTR consider a surveillance measure to be carried out unlawfully, it can recommend to the prime minister, the relevant minister and the intelligence service that the surveillance be interrupted and the collected data destroyed. The prime minister must immediately inform the CNCTR about how the recommendation was followed up. If the recommendation is not followed appropriately, the CNCTR can bring the case before the Council of State. Interestingly, the commission can consult and answer the questions of the Electronic Communications and Posts Regulatory Authority.[352] The law does not mention any links to the French data protection authority (CNIL).

While expert bodies undoubtedly have recognised expertise in the area of intelligence, data protection authorities (DPAs) are specialised bodies that have been tasked with safeguarding privacy and data protection in EU Member States. In countries where both exist and DPAs are competent to oversee intelligence services, their interaction is sometimes organised by law, and sometimes takes place in practice without legal requirements. The next section addresses the roles of DPAs.

2.3.2. Data protection authorities

Data protection authorities also constitute expert bodies in the context of oversight. They play a fundamental role in safeguarding the right to the protection of personal data. This role is enshrined in EU primary and secondary law, notably in Article 8 (3) of the Charter and Article 16 (2) of the TFEU, as well as in Article 28 of the Data Protection Directive.[353] Similarly, the principle of compliance control by an independent body is endorsed in the Explanatory Report of Council of Europe Convention 108, and was eventually laid down in its Additional Protocol 181 of 2001. Moreover, in some Member States,

345 Cameron, I. (2011), pp. 280 and following.
346 Sweden, Act on the Foreign Intelligence Court (2009:966) (*Lagen om Försvarsunderrättelsedomstol* (2009:966)), 15 October 2009 and Sweden, Regulation 2009:968 with instructions for the Foreign Intelligence Court (*Förordning (2009:968) med instruktion för Försvarsunderrättelsedomstolen)*, 15 October 2009.
347 Sweden, Act on Signals Defence Intelligence, Section 10.
348 Sweden, The Swedish Commission on Security and Integrity Protection, http://www.sakint.se/InEnglish.htm
349 France, Interior Security Code, Art. L. 831-1 to Art. L. 833–11.
350 For a discussion of concerns expressed by former CNCIS presidents about the increase in number of members – which could affect the efficiency of the decision-making process – see Dewost, J.-L., Pelletier, H. and Delarue, J.-M. (2015), p. 19.
351 France, Interior Security Code, Art. L. 801–1 (5) and Art. L. 833–5.
352 *Ibid.*, Art. L. 833-11.
353 Data Protection Directive.

compliance control by an independent body is laid down in the Constitution (Greece and Portugal).[354]

The Court of Justice of the European Union (CJEU) held in a series of judgments that supervision by DPAs is an essential component of the right to personal data protection – more recently in judgments invalidating the Data Retention Directive and the Commission's Decision on Safe Harbour principles.[355] The cases show that, in accordance with Article 8 (3) of the Charter and Article 28 of the Data Protection Directive, DPAs shall act in full independence, in particular from the government.[356]

Article 28 of the Data Protection Directive endows DPAs with the powers deemed necessary to hear claims relating to the lawfulness of data processing and the protection of rights regarding the processing of personal data. For effective compliance control, Article 28 (2) and (3) of the Data Protection Directive give advisory powers to DPAs when Member States draw up legislative or administrative measures, as well as powers of investigation (access and collection of necessary information), intervention (ordering corrective measures, banning data processing, warning or admonishing the data controller, referring the matter to national parliaments and other political institutions), and engagement in legal proceedings. DPA decisions may be subject to judicial control. Additional Protocol 181 to Convention 108 also provides for these powers – except for advisory power, which is merely mentioned in the explanatory report to the protocol.[357]

FRA findings show that, compared to other fields of data processing activities and other data controllers of the public and private sector, DPAs in most Member States have no competences over national intelligence services, or their powers are limited. As highlighted earlier, both the Data Protection Directive and the e-Privacy Directive are subject to the national security exemption. Regulation of the competence of DPAs in respect of intelligence may, however, be provided in national law.

In seven Member States (Austria, Bulgaria, Croatia, Finland, Hungary, Slovenia, and Sweden) DPAs have the same powers over national intelligence services as they do over any other data controller. This does not necessarily mean that national legislators have endowed the DPAs with the full range of powers listed above. It means that the legislators have not distinguished between intelligence services and other categories of data controllers in the public sector.

DPAs have no powers over intelligence services in 12 Member States (the Czech Republic, Denmark, Estonia, Latvia, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovakia, Spain, and the United Kingdom). They are either expressly excluded by the general data protection law or by specific laws on the functioning of the national intelligence services. In Latvia, for instance, the general data protection law states that the DPA is not competent to supervise files classified as "official secrets". Personal data processed by the intelligence services fall entirely within this scope, as the Investigatory Operations Law stipulates.[358] In the United Kingdom, the Information Commissioner pointed out in his written submissions to the Intelligence and Security Committee of Parliament that, while surveillance entails significant privacy and data protection concerns, when national security is invoked, many exceptions to the data protection rules can apply.[359]

In Luxembourg, the DPA itself is not competent to supervise the intelligence service, but the supervisory authority competent to supervise data processing related to state security, defence and public safety comprises the Chief State Prosecutor and two members of the DPA.[360] This interesting solution ensures that the oversight body is knowledgeable on data protection requirements.

In nine Member States (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Poland, Lithuania), DPAs have limited powers over intelligence services. While these DPAs have the power to issue non-binding recommendations on general matters related to national intelligence services' surveillance, limitations vary considerably by Member State. Some are formal and do not really affect the DPAs' powers, while others are more substantive. The wider the limitations, the narrower the powers.

Formal requirements in Cyprus or Greece, for example, set forth that an on-site inspection can only take place if the DPA head is present.[361] Similarly, in France only

354 FRA (2010), Section 6.1, p. 47.

355 CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*, 8 April 2014, para. 68; CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 41 and 66.

356 CJEU, C-518/07, *European Commission v. Federal Republic of Germany* [GC], 9 March 2010, paras. 23 and 30, CJEU, C-614/10, *Commission v. Austria*, 16 October 2012, paras. 36–37; CJEU, C-288/12, *Commission v. Hungary*, 8 April 2014, paras. 47–48; CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, para. 68.

357 Council of Europe, Convention 108, Additional Protocol, para. 16.

358 Latvia, Investigatory Operations Law (*Operatīvās darbības likums*), 16 December 1993, Art. 24.

359 United Kingdom, Information Commissioner's Office (2014).

360 Luxembourg, Act of 2 August 2002 on the protection of persons with regard to the processing of personal data (*Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*), 2 August 2002, Art. 17 (2).

361 Cyprus, Law No. 138 [I] 2001 on the Processing of Personal Data (*Ο Περί της Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος*), as amended, Art. 23 (1) (h). Greece, Data Protection Law 2472/1997 (*Νόμος 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*), 10 April 1997, as amended, Art. 19 (1) (h).

a DPA commissioner who has been a member of the Council of State, the Court of Cassation or the Court of Auditors may carry out an investigation.[362] In Germany the law stipulates that, in place of the head, an officer duly authorised in writing may carry out this task.[363] Such formal limitations – especially those requiring the heads of the DPAs to be present during an on-site inspection – may indeed hamper the organisation of the DPA's work.

When vested with exercising individuals' right to access their own data, such as in Belgium, France or Italy, DPAs are merely permitted to inform an individual that the necessary checks have been made, but not which data have been processed, if such information affects the security of the state. In Italy, when investigating a complaint and accessing classified documents, the DPA shall not inform the individual of the investigation's outcome if such information may affect state security. The DPA may, however, request that appropriate measures be adopted, just as it may when handling complaints not related to intelligence services.

Other limitations are linked with core powers. Data processing activities by intelligence services may be wholly (Belgium) or partially (France) excluded from the notification requirement of controllers to DPAs.[364]

Investigatory powers, especially the powers to request and/or access data and premises, are also limited (France, Germany, Ireland and Poland).[365] In Ireland, for instance, the DPA cannot access premises and data, or request data that, in the opinion of the Minister or the Minister of Defence, are processed to safeguard state security. In Germany, such access may be denied if doing so would harm the security of the Federation or a *Land*.

Some DPAs lack the power to handle complaints of individuals related to data processing activities by intelligence services, or to issue binding decisions (Belgium, Poland).[366]

In Germany, the G 10 Commission can request the federal DPA to provide an opinion on issues related to data-protection safeguards when performing its tasks.[367] In principle, however, the G 10 Commission is exclusively competent to monitor the data processing of the services under its supervision.[368] For the so-called 'open-sky' data, which are not controlled by the G 10 Commission, the federal DPA should in principle be competent to supervise whether data protection safeguards are respected by the intelligence service (BND), which should facilitate its work.[369] That said, this matter is subject of on-going discussions, including before the NSA Committee of Inquiry of the German Federal Parliament.[370]

Finally, according to FRA data, the Lithuanian DPA's powers cannot be clearly defined because the wording of the data protection law in conjunction with the specific law on the national intelligence services is inconclusive.[371]

Table 3 presents a synopsis of the abovementioned findings.

The Article 29 Data Protection Working Party (WP29), which represents all EU DPAs, in 2014 twice stressed that effective and independent supervision of intelligence services is necessary. The WP29 recommended that this supervision be carried out by DPAs themselves, or with their genuine involvement.[372] Similarly, the 36th International Conference of Data Protection and Privacy Commissioners called for all electronic surveillance programmes to comply with the 2009 Madrid International Standards on the Protection of Personal Data and

362 France, Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties (*Loi n. 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), 6 January 1978, Art. 41 (2). See also France, CNIL (2015), p. 47.

363 Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), 14 January 2003, as amended, Section 24 (4).

364 Belgium, Data Protection Act (*Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*), 1 April 1993, as amended, Art. 3 (4) in conjunction with Art. 17; France, Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties, Art. 26 (3), in conjunction with France, Decree No. 2007-914 for application of Article 30 of Law No. 78–17 relating to information technology, files and freedoms (*Décret n°2007-914 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*), 15 May 2007.

365 France, Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties, Art. 44, in conjunction with France, Decree No. 2007-914 for application of Article 30 of Law No. 78-17 relating to information technology, files and freedoms; Germany, Federal Data Protection Act, Section 24 (4); Ireland, Data Protection Act, 13 July 1988, as amended, Section 12 (4) (b) and 24; Poland, Data Protection Act 1997 (*Ustawa o ochronie danych osobowych*), 30 April 1998, Art. 43 (2) in conjunction with Art. 14 (1) (3) (5).

366 In Belgium, the DPA generally does not have the power to handle complaints and issue binding decisions vis-a-vis NIS; see Belgium, Data Protection Act, Art. 3 (4) in conjunction with Art. 31 and Arts. 29 and 30. In Poland, the DPA generally does not have the power to handle complaints and issue binding decisions, see Poland, Data Protection Act 1997, Art. 43 (2) in conjunction with Arts. 12, 15–18.

367 Germany, G 10 Act, Section 15 (5).

368 Germany, Federal Data Protection Act, Section 24 (2).

369 See de With, H. and Kathmann, E. (2011) p. 227.

370 Krempl, S. (2015).

371 Lithuania, Law on Legal Protection of Personal Data (*Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas*), No. X-1444, 1 February 2008, as amended, Art. 1 (5); in conjunction with Lithuania, Law of the Republic of Lithuania on Intelligence, Art. 24.

372 Article 29 Working Party (2014b), p. 13; Article 29 Working Party (2014a), p. 3.

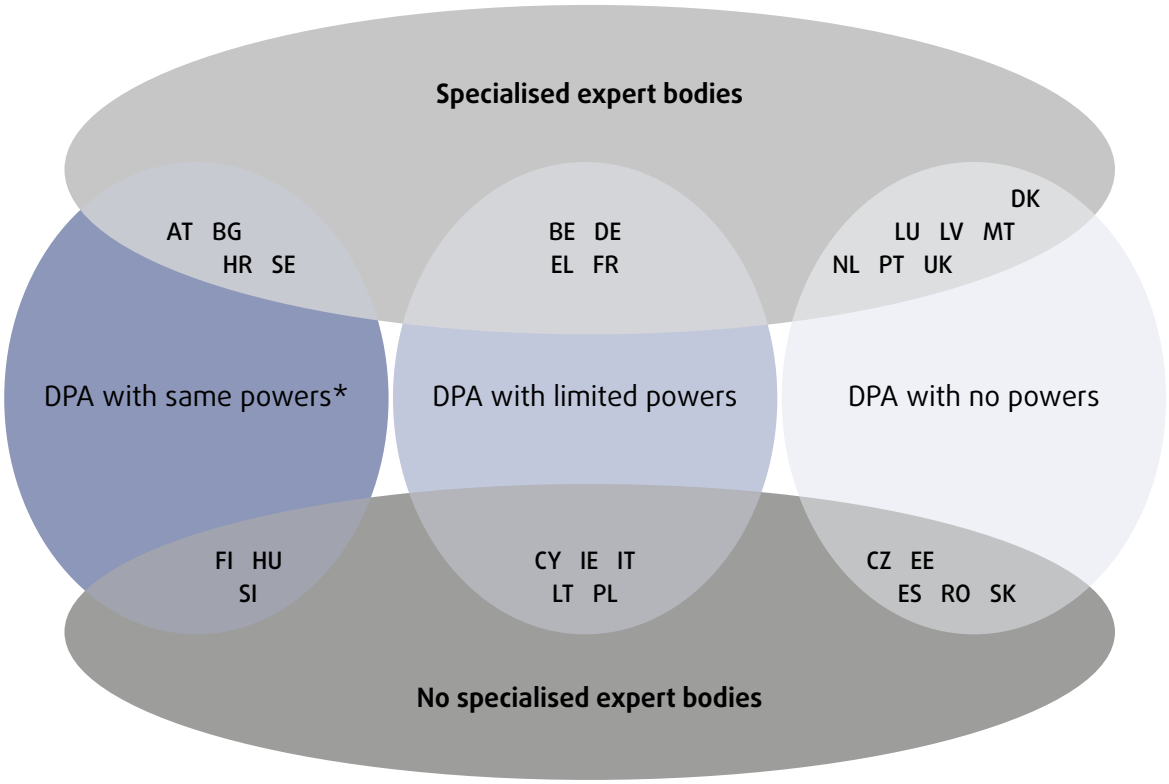
Table 3: DPAs' powers over national intelligence services, EU-28

EU Member State	No powers	Same powers (as over other data controllers)	Limited powers
AT		X	
BE			X
BG		X	
CY			X
CZ	X		
DE			X
DK	X		
EE	X		
EL			X
ES	X		
FI		X	
FR			X
HR		X	
HU		X	
IE			X
IT			X
LT			X
LU	X		
LV	X		
MT	X		
NL	X		
PL			X
PT	X		
RO	X		
SE		X	
SI		X	
SK	X		
UK	X		
TOTAL	12	7	9

Notes: *No powers: refers to DPAs that have no competence to supervise NIS.*
Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.
Limited powers: refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.

Source: FRA, 2015

Figure 4: Specialised expert bodies and DPAs across the EU-28



Note: * as over other data controllers*
Source: *FRA, 2015*

Privacy.[373] The Madrid Standards establish a proposal for a universal data protection instrument, including rules on independent supervisory authorities.[374]

In Germany, the federal and state (*Länder*) Data Protection Commissioners adopted two resolutions proposing measures for better protection of personal data and privacy. One asked parliament to remove the current oversight system's deficiencies.[375] Initiating an investigation, for instance, is a necessary power of any DPA and should be provided for by law. The resolution also asked to embed DPAs in the oversight system of intelligence services, thus taking advantage of their expertise. These calls build on a Federal Constitutional Court (*Bundesverfassungsgericht*) judgment on the anti-terrorism data file, which held that in a surveillance system that is not open to scrutiny by individuals, an effective oversight system must be in place. When various intelligence services exchange data, there must also be enhanced cooperation among the supervisory data protection authorities.[376] Moreover, the Federal Data Protection Commissioner highlighted gaps resulting from the fragmentation of the oversight system, and asked the legislator to amend the legal framework. The Federal DPA also emphasised that effective control requires adequate human resources and technical know-how.[377]

Where the law prevents DPAs from overseeing the work of intelligence services, this should not prevent oversight bodies from engaging with DPAs. For instance, the Dutch oversight body met the DPA in the context of its review report on the processing of communications data by the intelligence services.[378]

An example of a prompt, practical reaction after the Snowden revelations is the Memorandum of Understanding (MoU), signed in 2013 by the Italian DPA and the intelligence services. The MoU lists the files subject

373 International Conference of Data Protection and Privacy Commissioners, 36th (2014).
374 International Conference of Data Protection and Privacy Commissioners, 31st (2009).
375 Germany, Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 88th (2014).
376 Germany, Federal Constitutional Court, BvR 1215/07, 24 April 2013.
377 Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit*) (2013), Section 7. For the latest developments, see Germany, Federal Commissioner for Data Protection and Freedom of Information (2015), Section 2.
378 The Netherlands, CTIVD (2014a), pp. 12–13.

to inspection by the DPA, and provides rules on the DPA's access to the premises and files, the secure storage of intelligence information at the DPA's premises, and the implementation by the intelligence services of the DPA's findings. Finally, it provides for the possibility of the intelligence services consulting the DPA beyond what is currently laid down in the legal framework.[379] Regrettably, the MoU's content is classified and not publicly available.

In terms of how specialised expert bodies and DPAs complement each other, Figure 4 further illustrates the great diversity of oversight mechanisms across the EU. It also raises several questions, such as: How do expert bodies and DPAs that have the same powers over intelligence services that they have over other data controllers collaborate in practice in the four Member States where this situation exists? On the opposite end of the spectrum, how is oversight undertaken in the five Member States that have not established a specialised expert body or given their DPA competence to oversee the intelligence services? The current FRA legal comparative analysis cannot answer these questions. They will be addressed in forthcoming fieldwork.

2.4. Approval and review of surveillance measures

One way to ensure surveillance measures are carried out lawfully is to allow for *ex ante* control by a suitable authority through prior approval or warranting.

UN good practice on intelligence collection and oversight

Practice 22. Intelligence-collection measures that impose significant limitations on human rights are authorized and overseen by at least one institution that is external to and independent of the intelligence services. This institution has the power to order the revision, suspension or termination of such collection measures. Intelligence collection measures that impose significant limitations on human rights are subject to a multilevel process of authorization that includes approval within intelligence services, by the political executive and by an institution that is independent of the intelligence services and the executive.

UN, Human Rights Council, Scheinin, M. (2010)

As stated by Born and Wills, "*Oversight* is a catchall term that encompasses *ex ante* scrutiny".[380]

ECtHR case-law: Expert bodies as alternatives to judicial supervision

"The Court has indicated, when reviewing legislation governing secret surveillance in the light of Article 8, that 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 [...]. However, [...] the Court was prepared to accept as adequate the independent supervision available. In *Klass and Others*, this included a practice of seeking prior consent to surveillance measures of the G 10 Commission, an independent body chaired by a president who was qualified to hold judicial office and which moreover had the power to order the immediate termination of the measures in question [...]. In *Kennedy v. UK* [...] the Court was impressed by the interplay between the Investigatory Powers Tribunal ("IPT"), an independent body composed of persons who held or had held high judicial office and experienced lawyers which had the power, among other things, to quash interception orders, and the Interception of Communications Commissioner, likewise a functionary who held or had held high judicial office [...] and who had access to all interception warrants and applications for interception warrants [...]."

ECtHR, Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands, No. 39315/06, 22 November 2012, para. 98

Table 4 presents the various bodies responsible for *ex ante* approval in the EU Member States in the context of targeted surveillance. Table 5 presents similar data in the five Member States that have detailed laws on signals intelligence. Some states have also established an *ex post* independent review of the surveillance measures, judicial or otherwise.

In the case of targeted surveillance, a warrant may only be granted on the basis that the surveillance will target a specified individual or group. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism states, "With targeted surveillance, it is possible to make an objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation."[381] However, bulk access to digital communications does not allow for an individualised proportionality analysis, and "[e]x-ante security is therefore possible only at the highest level of generality".[382]

Though all Member States provide for this approval in some form or another, just over half charge the

379 Italy, Italian Government (2013). See also COPASIR (2014), p. 19.
380 Born, H. and Wills, A. (eds.), Geneva Centre for the Democratic Control of Armed Forces (DCAF) (2012), p. 6.
381 UN, Human Rights Council, Emmerson, B. (2014), para. 7.
382 *Ibid.*, para. 12

Table 4: Prior approval of targeted surveillance measures, EU-28

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
AT				X	
BE				X	
BG	X				
CY	X				
CZ	X				
DE				X	
DK	X				
EE	X				
EL	X				
ES	X				
FI	X				
FR			X		
HR	X				
HU	X		X		X
IE			X		
IT	X				
LT	X				
LU			X		
LV	X				
MT			X		
NL			X		
PL	X				
PT*					
RO	X				
SE**					
SI	X				X
SK	X				
UK			X		

Notes: * The Portuguese intelligence service is prohibited from undertaking surveillance; the Constitution only allows public authorities to interfere with correspondence, telecommunications or other means of communication in criminal proceedings, which the intelligence service is not allowed to conduct.

** Sweden's security and intelligence services do not carry out targeted surveillance. The security service processes and analyses data collected by law enforcement through secret wiretapping and intercepted traffic data, while the signals intelligence agency gathers signals intelligence (see Annex).

Source: FRA, 2015

judiciary (judges or prosecutors) with the approval process, while others charge ministers, prime ministers, and expert bodies. The Council of Europe's Commissioner for Human Rights stated that, given the difficulties that may arise when seeking to evaluate judicial decisions on the authorisation of intrusive measures, consideration may be given to quasi-judicial models.

In France and in Luxembourg, the prime minister authorises the surveillance of communications. In Luxembourg, the prime minister needs the assent of a commission

composed of the President of the Superior Court of Justice, the President of the Administrative Court, and the President of the District Court.[383] In France, the CNCTR gives a non-binding opinion (*avis*) to the Prime Minister either within 24 or 72 hours.[384] In the United Kingdom,[385] Malta,[386] Hungary[387], Ireland,[388] and the Netherlands,[389] approval comes from ministers.

Only three countries – Austria, Belgium and Germany – have tasked their expert bodies (the Legal Protection Commissioner, Administrative Commission and G 10 Commission, respectively) with approving targeted surveillance measures. In other Member States, expert bodies sometimes have an advisory role, such as in France or the Netherlands. While in France the CNCTR gives an *ex ante* opinion, in the Netherlands, the CTIVD does not have an *ex ante* advisory role, but does review surveillance measures after they are approved by the responsible minister. Its opinion, however, is non-binding.[390]

Hungary's approval process rests with different authorities, depending on the surveillance measure.[391] No authorisation is necessary to tap conversations in public spaces (or gather communications data from communications systems and data storage devices). The Minister of Justice must authorise, among others, the tapping of public lines, interception of post, and access to data stored on IT devices or systems. However, the above activity must be authorised by judges when it is carried out by the intelligence services to facilitate, amongst others: detecting – before an investigation is ordered – crimes enumerated in the Act on the National Security Services; revealing and preventing covert efforts to alter/disturb the legal order of Hungary by unlawful means; collecting information on illicit arms dealing representing a threat to national security, or on terrorist organisations threatening the security of the armed forces; or revealing and preventing efforts pertaining to terrorism by foreign powers. Hungary's authorisation legislation, specifically Act No. XXXIV of 1994 on the police and the "sweeping prerogatives" granted to the Minister of Justice when authorising surveillance, is currently under challenge before the ECtHR.[392]

Similarly, there are two ways of gathering intelligence in Slovenia, and one requires a court order, whereas the other does not. The latter, which comprises Slovenia's SIGINT activities, or surveillance of international communication systems, is authorised by the director of the Slovenian Intelligence and Security Agency (SOVA). [393] Court orders, on the other hand, are required for the interception and wiretapping of private correspondence, and are authorised by the President of the Supreme Court. For the court order to be issued, a danger to state security must exist. It must also be reasonable to expect that, in connection with the activity that is to be put under surveillance, telecommunications is being or will be used; and to conclude that information cannot be collected in any other way, or that doing so would endanger people's lives or health.[394]

In Austria, a Legal Protection Commissioner (RSB) was established to afford citizens another level of protection in the context of secret investigations carried out without their knowledge.[395] The RSB needs to approve covert investigations (*verdeckte Ermittlung*), or covert audio and video recording, in the context of the observation of groups thought to present a serious danger to public security through acts of religiously or ideologically motivated violence. The Federal Minister of the Interior seeks the RSB's opinion during operative and strategic analyses of personal data. This type of analysis is performed in the defence against criminal organisations or to prevent dangers emanating from the preparation or commission of criminal offences. The RSB has to provide an opinion on each surveillance measure. Once the opinion has been provided, the analysis can be conducted.[396]

In Spain, Article 18 (3) of the Constitution states that only the competent judicial authorities may authorise measures that affect the right to secrecy of communications. While the Spanish Code of Criminal Procedure refers to targeted surveillance carried out during a criminal investigation where an individual is already suspected of being involved in a crime and which is warranted by

383 Luxembourg, Ministry of Justice (*Ministère de la Justice*), Criminal Investigation Code (*Code d'Instruction Criminelle*), as amended on 15 April 2015, Art. 88-3.
384 France, Interior Security Code, Art. L. 821–1 and Art. L. 821–3. See also Dewost, J.-L., Pelletier, H. and Delarue, J.-M. (2015), p. 28 and following.
385 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 7 (1) (a).
386 Malta, Security Service Act, Chapter 391 of the Laws of Malta, 26 July 1996, as amended on 6 September 1996, Art. 8 (1) (a).
387 Hungary, Act CXXV of 1995 on the National Security Services, Section 58 (2).
388 Ireland, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 6 June 1993, Section 2 (2) (a).
389 The Netherlands, Intelligence and Security Services Act 2002, Art. 25, paras. 1-6.
390 For changes proposed to the law, see The Netherlands, Draft law on the Intelligence and Security Services 20XX. See also The Netherlands, CTIVD (2015), p. 29.
391 Hungary, Act CXXV of 1995 on the National Security Services, Sections 57 (1), 58 (1) and 58 (2).
392 ECtHR, *Szabo and Vissy v Hungary*, No. 37138/14, communicated on 12 June 2014.
393 Slovenia, Intelligence and Security Agency Act, Art. 21.
394 Slovenia, Intelligence and Security Agency Act, Art. 24.
395 Austria, Police Powers Act, Sections 91 (a)–91 (d).
396 In October 2015, the Austrian Parliament will discuss a bill amending the Police Powers Act (*Sicherheitspolizeigesetz*). This bill suggests important changes affecting the way surveillance measures will be authorised. See Austria, State Security Bill.

an ordinary judge,[397] the Spanish National Intelligence Centre must get permission from a Supreme Court judge when carrying out measures that target communications. When requesting such authorisation, the Spanish National Intelligence Centre has to provide information on the specific nature of the measures; articulate the facts, purposes and reasons underlying the adoption of such measures; identify the person/s who will be affected by the surveillance measure, if they are known; and specify the duration of the requested measures.[398] Worthy of mention is that the judicial decision must always state the grounds on which it is approved or dismissed. This is also the case for approvals of the use of special intelligence means in Bulgaria.[399] Requiring reasoned decisions helps avoid mere rubber-stamping, and ensures that judges take the time to study the merits of granting the measures.

However, most countries' laws include provisions permitting the primary authority to postpone approvals in exceptional cases. In Latvia, for instance, when there is a need to act without delay to prevent a threat to vital public interests, such as an act of terrorism or subversive activity, a murder or other serious crime, or if there is an actual threat to the life, health, or property of a person, surveillance can be initiated without the judge's approval. In its stead, a prosecutor must be notified within 24 hours and the judge's approval must be received within 72.[400]

Other countries, such as Poland and Romania, have a two-tiered system of judicial approval. In Romania, the intelligence services must first obtain approval from the Prosecutor General, who then applies for authorisation to the High Court of Cassation and Justice if the application is well grounded.[401] The Prosecutor General may also authorise surveillance measures in cases of emergency (for a maximum of 48 hours), as long as authorisation from the court is requested as soon as possible. This system allows for the legitimacy of the measures to be studied twice before being authorised.

Once the surveillance measures have been approved, they must be carried out lawfully. In Latvia, for instance, once the Chairman of the Supreme Court or a designated Supreme Court judge has approved a surveillance measure, the Prosecutor General and his or her designated prosecutors carry out continuous oversight. They have the right to examine documents, material and information at any stage of the investigatory operations.[402] Latvia, therefore, has double-tiered judicial involvement in the work of the intelligence services. This kind of review also occurs in Greece and Ireland. In Greece, a public prosecutor is specially appointed to the intelligence service and tasked with supervising the legality of the special operational activities.[403] In Ireland, it is a designated judge of the High Court who carries out ongoing oversight, supervising whether surveillance, which is carried out by a special police unit, is undertaken lawfully.[404]

By contrast, collection of signals intelligence – at least during its initial stages – targets not an individual but rather large flows of data. Search terms, also known as selectors, are later applied to the bundles of data to draw out information relevant to the work of the intelligence services. Table 5 presents the bodies in charge of approving signals intelligence collection in the five Member States that have detailed legislation on SIGINT.

In Sweden and Germany, an expert body is in charge of authorising the intelligence services to gather signals intelligence. In Sweden this is carried out by the Foreign Intelligence Court, which has eight members, two of whom are former judges (the chair and vice chair), and six of whom are lay members (there can be as few as two and as many as six lay members in total), mainly former politicians.[405] The court must be composed of at least the chair and two lay members, and no more than three members may decide its rulings.[406]

The government appoints all members. The chair and vice chair (presently only one vice chair, but there could be two) are appointed in the same manner as regular judges, after an open recruitment process led by the Judges' Board (*Domarnämnden*).[407] The other members are appointed after the parties represented in parliament consult with each other.[408] Lay judges should have special knowledge of court matters. The interests of individuals are represented by lawyers appointed for a four-year period. The court may declare that its

397 Spain, Code of Criminal Procedure *(Ley de Enjuiciamiento Criminal)*, Art. 579.
398 Spain, Organic Law Regulating *a priori* judicial control of the National Intelligence Centre, single article.
399 Bulgaria, Special Intelligence Means Act, Art. 15 (1).
400 Latvia, Investigatory Operations Law, Art. 7 (5).
401 Romania, Law No. 51/1991 concerning the national security of Romania (*Legea nr. 51/1991 privind securitatea nationala a Romaniei*), 29 July 1991, Arts. 15 (3) and (4).
402 Latvia, Investigatory Operations Law, Art. 19 (2) 1.
403 Greece, Law 3649/2008, National Intelligence Service (EYP) and other provisions *(Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις)*, 3 March 2008, Art. 5 (3).
404 Ireland, Interception of Postal Packets and Telecommunications Messages (Regulation) Act, Section 8.
405 The court currently includes one former Minister of Justice.
406 Sweden, Act on the Foreign Intelligence Court, Section 9.
407 This is a government agency with a board consisting of nine members. Five members should have been judges, two should practice law outside of the court system (and one of these should be *'advokat'* (member of the bar)), and the remaining two should represent 'society' (presently two members of the national parliament). See http://www.domstol.se/Om-Sveriges-Domstolar/Domarnamnden/Om-Domarnamnden/Domarnamndens-ledamoter/.
408 Venice Commission (2015), p. 36.

Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

EU Member State	Judicial	Parliamentary	Executive	Expert
DE		X (telco relations)		X (selectors)
FR			X	
NL			X (selectors)	
SE				X
UK			X	

Source: FRA, 2015

sessions are not public, and its decisions may not be appealed.[409]

In Germany, on the other hand, strategic surveillance – the interception of international telecommunications between foreign countries and Germany – is authorised by the Parliamentary Control Panel and the G 10 Commission. The intelligence service is required to channel its request with proper justification and specification of the selectors used through the Ministry of Interior. The request needs the approval of the Control Panel, specifically regarding the selection of "telecommunication relations", i.e. the geographical regions of interest.[410] A strategic surveillance request cannot concern more than 20 % of the overall transmission capacity of a given transmission channel (Section 10 (4) of the G 10 Act). The surveillance order is valid for three months and can be renewed for the same period once, if the conditions for the initial approval are maintained. The G 10 Commission then ensures the surveillance is "permissible and necessary" by approving the list of selectors to be used to filter the data.[411]

The Netherlands does not require authorisation when the services collect non-cable bound communications, which include satellite and radio transmissions. However, once the data has been narrowed down or keywords are applied, ministerial approval becomes necessary.[412] The CoE Commissioner for Human Rights, among others, recommends that "independent *ex ante* authorisation should be extended to untargeted bulk collection of information" and not merely to the access to such data.[413] The Dutch system also takes a different approach to that recommended by the Venice Commission: that the application of selectors to data, and therefore the authorisation of targeted surveillance, be done by a judicial body or a hybrid body composed of judges and experts.[414]

In contrast, warrants in the United Kingdom are authorised by the corresponding Secretary of State. Such warrants address communications collection. An accompanying certificate specifies which of the collected communications can be examined. However, the Intelligence and Security Committee of Parliament found that the categories identified in the certificates are very broad.[415] Warrants for the interception of communications are authorised by the Home Secretary if the warrant is applied for by the Security Service (or MI5), or by the Foreign Secretary if the warrant is applied for by the Security Intelligence Service (or MI6) or GCHQ. Under the Regulation of Investigatory Powers Act (RIPA), only 'external' communications (which are those that begin and/or end outside the British Isles, also referred to as "one-end foreign" warrants) can be collected in bulk.[416] The warrants issued by the Secretary of State must cover the sources that can be targeted and the types of material that can be accessed from the intercepted material. This distinction between internal and external is not always clear, however, since the British government interprets 'external communications' to include those which are routed via foreign companies, such as Facebook or Twitter, as well as accessing foreign websites. This lack of clarity was evidenced by the Intelligence and Security Committee's finding that these communication categories are

409 Sweden, Act on the Foreign Intelligence Court, Sections 3, 5, 6, 9, 14 and 16. Details are provided in Sweden, Regulation 2009:968 with instructions for the Foreign Intelligence Court. The website of the Court is available in Swedish only, http://www.undom.se/. The Court was established in 2009, replacing a previously exisiting Signals Intelligence Board.

410 Germany, G 10 Act, Sections 5 and 8. See also Germany, Parliamentary Control Panel Act.

411 Germany, G 10 Act, Section 15 (5).

412 The Netherlands, Intelligence and Security Services Act 2002, Art. 26.

413 Council of Europe Commissioner for Human Rights (2015), p. 9.

414 Venice Commission (2015), p. 6.

415 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), pp. 37–38.

416 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 8 (4).

confusing also for members of government.[417] Moreover, although the warrant must be targeted at external communications, the incidental interception of internal communications is permitted. Once communications are intercepted, no distinction is made as to subsequent use or analysis.[418] In't Veld and Ernst hypothesise that, as a result of this action, "as the world becomes more and more wired and interconnected, these [personal digital] data are increasingly stored and transmitted freely across borders and through transit countries, leading to an unclear situation regarding jurisdiction and diminishing the relevance of national legislation and of national oversight".[419]

A similar debate occurred in France in relation to international surveillance.[420] When it comes to SIGINT, as prescribed by Article L. 851–3 of the Interior Security Code, the prime minister authorises the automatic processing based on selected parameters. The CNCTR provides the prime minister with a non-binding opinion on both the automatic processing and the parameters. The oversight body is kept informed about every modification during the operation and has permanent, complete and direct access to this processing and the intelligence gathered. The first authorisation is valid for two months. It is renewable, but the prolongation request should include the number of relevant targets obtained by the automatic processing and an analysis of their relevance. Should this data reveal the existence of a terrorist threat, the CNCTR provides the prime minister with its opinion on his/her authorisation to identify the relevant targets. Pursuant to Article L. 851-3 V of the Interior Security Code, absolute emergency (Article L. 821-5) cannot be put forward to authorise this surveillance measure without the CNCTR opinion.

What constitutes best practice in this area is a highly debated issue. In the series of enquiries held in October 2014 by the Intelligence and Security Committee of the British parliament, representatives of civil liberties organisations questioned the Secretary of State as a higher authority than a judge, since judges are independent of political pressure. The Home Secretary, however, who, as stated above, is responsible for authorising warrants for the interception of communications by MI5, responded that intrusions on privacy should be authorised by someone who is accountable directly to the British people and who has a greater understanding of the wider context in which these actions are being taken.[421] Though the committee shared the Home Secretary's opinion, the Independent Reviewer of Terrorism Legislation did not. In his exhaustive report, he recommended that Judicial Commissioners be created. These would be in charge of warranting surveillance judicially, and would therefore replace the Secretaries of State in the warranting process.[422] Cameron and the Council of Europe Commissioner for Human Rights have suggested another alternative worth contemplating: separating the tests of whether surveillance is necessary and appropriate from the test of whether it is lawful by requiring both ministerial and judicial authorisation.[423] This would allow the executive to maintain some form of control while protecting against political abuse.

It is therefore clear that, as a general rule, when targeting communications' content data, prior approval is required in most Member States for both targeted surveillance and the use of selectors in the context of SIGINT. This changes, however, when intelligence services solely access metadata via data retention laws (Croatia,[424] Hungary,[425] United Kingdom[426]). In these cases, it is usually sufficient for the services' directors to authorise access. This is problematic, because communications data do in fact reveal an individual's pertinent personal information in a similar way to content data.[427] This situation may change, however, since these laws have been challenged in several Member States. The Dutch Review Committee found that analysis of communications using metadata should be further safeguarded by providing for internal (in the service) or external (ministerial) approval procedures. The services should have to substantiate that the processing fulfils the requirements of necessity, proportionality and subsidiarity for it to be lawful.[428]

417 United Kingdom, ISC (2015), p. 40.
418 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 5 (6). See also United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, para. 68 and following.
419 See European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013b).
420 See France, French Data Network (2015), p. 69 and following.
421 United Kingdom, ISC (2015), pp. 73–76.
422 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 280.
423 Cameron, I. (2000), p. 151; Council of Europe Commissioner for Human Rights (2015), p. 63.
424 Hungary, Act CXXV of 1995 on the National Security Services, Section 40.
425 Croatia, Electronic Communications Act (*Zakon o elektroničkim komunikacijama*), Official Gazette (*Narodne novine*) Nos. 73/08, 90/11, 133/12, 80/13 and 71/14, 1 July 2008, as amended, Art. 108.
426 United Kingdom, Regulation of Investigatory Powers Act 2000, Chapter II.
427 Article 29 Working Party (2010).
428 See The Netherlands, CTIVD (2014), p. 97.

FRA key findings

FRA's analysis looks at the accountability mechanisms related to surveillance by intelligence services. It describes in particular how EU Member States have established oversight mechanisms. Oversight is a means to ensure public accountability for the decisions and actions of intelligence services. According to experts, oversight aims to avoid the abuse of power, legitimise the exercise of intrusive powers and achieve a better outcome after an evaluation of specific actions. The general consensus, taken from a Venice Commission report and other academic studies, is that oversight should be a combination of:

- executive control;
- parliamentary oversight;
- expert bodies;
- judicial review.

Executive control and coordination between oversight bodies

The executive branch can control the intelligence services in a variety of ways: by specifying their strategic policies and priorities, or establishing guidelines; by nominating and/or appointing the service's senior management; by formulating the budget that parliament will ultimately vote on; or by approving cooperation with other services. The executive plays also a crucial role in authorising surveillance measures in some Member States.

Effective oversight calls for proper coordination between the various oversight bodies to ensure that every aspect of the work of intelligence services is covered. If oversight bodies do not have a clear, comprehensive understanding of the work of the entire national intelligence community, gaps in oversight will ensue, and the effectiveness of the oversight system as a whole will be hindered.

- The diversity among the EU Member States in terms of politics and legal systems has translated into a great variety of bodies that oversee the intelligence services. EU Member States have vastly different oversight systems. While good practices can be drawn from the systems in place, individual areas would benefit from legal reform enhancing the power of the oversight bodies.

- A great assortment of powers are granted to the various oversight bodies, and the extent to which they may exercise these powers also varies.

- Seven Member States have oversight systems that combine the executive, parliament, the judiciary (via *ex-ante* approval) and expert bodies. However, these do not include any of the countries that have legal frameworks allowing signals intelligence collection.

- Effective oversight does not necessarily require all four types of oversight mechanisms. Such oversight can be accomplished as long as the bodies in place complement each other and as a whole constitute a strong system capable of assessing whether the intelligence services' mandate is carried out properly. This will occur if the oversight powers cover all areas of an intelligence service's activity. Where the mandate itself is unclear or insufficiently developed, however, oversight bodies will not be able to exercise any influence.

- Access to information and documents by oversight bodies is essential. While information gathered by intelligence services is sensitive, and safeguards must guarantee that it will be dealt with accordingly, oversight bodies cannot carry out their tasks without first having access to all relevant information. The opposite, however, seems to be the norm.

Parliamentary oversight

Parliamentary oversight is important given the parliament's responsibility to hold the government accountable. Parliament, as the lawmaker, is responsible for enacting clear, accessible legislation establishing the intelligence services and specifying their organisation, special powers and limitations. It is also in charge of approving the intelligence services' budget, and in some Member States scrutinises whether their operations are in line with the legal framework.

- FRA findings show that 24 EU Member States involve parliamentary oversight; in 21 of these, special parliamentary committees oversee the intelligence services. Some Member States have set up one parliamentary committee to deal with the various security and intelligence services, whereas others have created various committees to deal with the services individually.

- No Member State's parliamentary committee is granted unrestricted access to intelligence information.

- The different parliamentary committees in the Member States have varying mandates: most have traditional oversight powers related to legislation, the budget and the reception of information on the services' function, while a select few can handle complaints, make binding decisions on the intelligence services or aid in approving surveillance measures.

- In terms of parliamentary committees' power to initiate investigations, the laws of most countries authorise these committees to request information from the intelligence services or the executive, but not to demand it.

Expert oversight

Expert oversight is exceptionally valuable because it allows individuals who are familiar with the subject, have time to dedicate to the matter, and are independent of political allegiances to scrutinise the actions of the intelligence services. According to the Commissioner for Human Rights of the Council of Europe, they are often best placed to conduct day-to-day oversight over security and intelligence service activity.

- Although parliamentary oversight is crucial, it must be complemented by other oversight bodies, particularly by strong expert bodies that can oversee operational activities, including the collection, exchange and use of personal data, as well as the protection of the right to private life.

- Across the EU, 15 Member States have set up one or more expert bodies exclusively dedicated to intelligence service oversight. Their competences include authorising surveillance measures, investigating complaints, requesting documents and information from the intelligence services, and giving advice to the executive and/or parliament. To maximise their potential, they must be granted adequate independence, resources and powers.

- In some Member States, the authorisation of surveillance measures does not involve any institutions that are independent of the intelligence services and the executive.

- In Member States that have an independent body to authorise surveillance measures, targeted surveillance tends to require judicial approval, while approval via expert bodies is the other preferred solution. There is no common approach to overseeing signals intelligence collection.

- While understanding the legal aspects of surveillance is indispensable, expert bodies must also be technically competent. Some Member States ensure this by including experts from a range of fields, including information and communications technology (ICT). Others rely heavily on a combination of current or former judges and parliamentarians.

In EU Member States, data protection authorities (DPAs) – specialised bodies called to safeguard privacy and data protection – have been given a fundamental role in safeguarding personal data. This role is enshrined in EU primary and secondary law. But expert bodies undoubtedly have recognised expertise in privacy and data protection in the area of intelligence.

- FRA findings show that, compared with other data processing activities and data controllers of the public and private sector, DPAs in seven Member States have the same powers over intelligence services as over all other data controllers. In 12 Member States, DPAs have no competence over intelligence services, and in nine their powers are limited.

- In Member States in which DPAs and other expert oversight bodies share competence, a lack of cooperation between these may leave gaps resulting from fragmented responsibilities. In Member States where DPAs lack competence over intelligence services, the oversight body is responsible for ensuring that privacy and data protection safeguards are properly applied.

- Past FRA research in the area of access to data protection remedies identifies the need to improve DPAs' capacity; this is important in view of the role DPAs could play in supervising intelligence services.

3 Remedies

The right to an effective remedy is an essential component of access to justice, and allows individuals to seek redress for the violation of their rights. A remedy must be 'effective' in practice and in law.

UN good practice on complaints and effective remedy

Practice 9. Any individual who believes that her or his rights have been infringed by an intelligence service can bring a complaint to a court or oversight institution, such as an ombudsman, human rights commissioner or national human rights institution. Individuals affected by the illegal actions of an intelligence service have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.

UN, Human Rights Council, Scheinin, M. (2010)

In addition, the existence of mechanisms that handle individual complaints against intelligence services can also be seen as bolstering "accountability by highlighting administrative failings and lessons to be learned, leading to improved performance".[429]

As presented by FRA reports on access to remedies for violations of data protection and on access to justice, a number of remedial avenues are available to victims of privacy and data protection violations.[430] These include judicial mechanisms and non-judicial bodies, such as DPAs. The complexity of the remedial landscape does not facilitate the implementation of effective remedies.

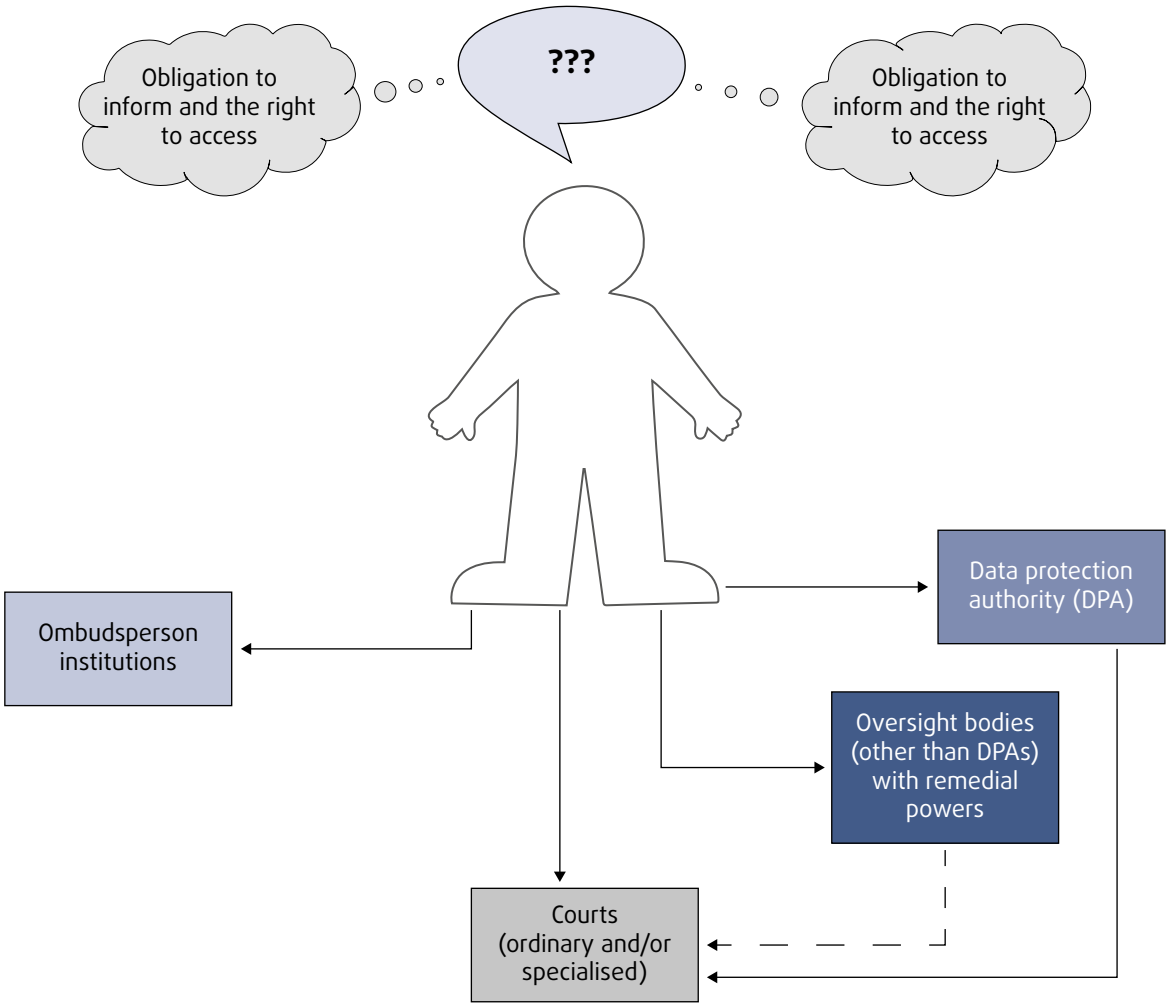
When an individual wishes to complain about interference with his or her right to privacy and data protection by intelligence services, the remedial landscape appears even more complex. The different remedial avenues are often fragmented and compartmentalised, and the powers of remedial bodies curtailed when safeguarding national security is involved. In fact, data collected for this research shows that only a very limited number of cases challenging surveillance practices have been adjudicated at the national level since the Snowden revelations.

Figure 5 provides a general and theoretical overview of the remedial avenues complainants can choose from when seeking a remedy in the area of surveillance at the national level. It does not cover avenues available to individuals at the European level, such as the ECtHR or the Petition Committee of the European Parliament.[431] These options provide remedies for privacy and data protection breaches caused by unlawful surveillance in different ways. Remedies provided by DPAs and some of the other oversight bodies can subsequently be challenged before the courts.

Various actors have highlighted loopholes in the remedial landscape. In the United Kingdom, for example, the Information Commissioner pointed out in written submissions to the Intelligence and Security Committee of Parliament that "state surveillance of individuals' communications, be this content or metadata, engages significant privacy and data protection concerns. The [Data Protection Act 1998] provides only limited reassurance as a wide ranging exemption from its provisions can be relied on where safeguarding national security is engaged. The current legal and regulatory regime is fragmented and needs review to ensure that it is fit for purpose in providing appropriate and effective oversight and redress mechanisms given the communications

429 Forcese, C. (2012), p. 181.
430 FRA (2011); FRA (2014c).
431 See, for example, European Parliament, Committee on Petitions (2014), No. 1618/2012, 29 August 2014.

Figure 5: Remedial avenues at the national level



Source: FRA, 2015

technologies and networks in use today and likely to be in use in the foreseeable future."[432]

In addition to the complexity of the remedial landscape, recourse to courts raises an issue of specialisation and strict procedural rules on evidence and legal standing, while recourse to non-judicial bodies raises issues of power and independence.[433]

Furthermore, for an individual wishing to seek justice, the secret nature of surveillance activities restricts his or her awareness about surveillance being carried out in the first place,[434] hence the importance of seeking an effective remedy in a wider context of effective oversight, as pointed out by the ECtHR in the *Segerstedt-Wiberg and Others v. Sweden* case.

ECtHR case law: the effective remedy in case of surveillance

The "authority" referred to in Article 13 [of the ECHR] may not necessarily in all instances be a judicial authority in the strict sense. Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy is effective. Furthermore, where secret surveillance is concerned, objective supervisory machinery may be sufficient as long as the measures remain secret. It is only once the measures have been divulged that legal remedies must become available to the individual.

ECtHR, Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, para. 117*

Further discussion and analysis of the issues outlined above are provided in subsequent sections, starting with a precondition to any remedial action: the obligation to inform an individual about surveillance and the right of an individual to access his/her own data.

432 United Kingdom, Information Commissioner's Office (2014), p. 9.
433 Forcese, C. (2012), p. 182.
434 See for example, Dewost, J.-L., Pelletier, H. and Delarue, J.-M. (2015), pp. 13 and 30.

However, the analysis in this section, just as in previous sections, is based on the comparative analysis of different laws, and is not an assessment of their practical implementation. This implementation particularly depends on how the various exceptions permitted by national law are invoked.

3.1. A precondition: obligation to inform and the right to access

The obligation to inform and the right to access one's own data can generally be perceived as strong safeguards for ensuring the effectiveness of a remedial action, and, ultimately, legal scrutiny by judicial or non-judicial bodies. From the point of view of the right to data protection, these safeguards also ensure transparency of data processing and the exercise of other rights of the individual, i.e. the rectification and/or deletion of data being processed unlawfully.[435] In the context of surveillance, even with necessary restrictions, the obligation to inform and the right to access also enhance transparency and accountability of the intelligence services and help to develop citizens' trust in government actions.[436] To safeguard national security, obligations and rights may, in accordance with Article 13 (1) of the Data Protection Directive, be restricted to the extent necessary and properly justified.[437] According to the CJEU, the judicial review guaranteed by Article 47 of the Charter first requires full knowledge by the individual, and subsequently by the court, of the information on which the administration based its decision. The adversarial principle shall be complied with, so that the individual can decide whether there is an argument to make against the national decision. From there the court may review the national decision. At the same time, for overriding reasons connected to state security, it may prove necessary not to disclose certain information to the individual. However, the court shall be able to review whether the invoked reasons are valid, and the national authority shall prove that the disclosure of the information would compromise state security. There is no presumption that the reasons invoked exist and are valid.[438] In *Schrems v Data Protection Commissioner*, the CJEU held that the right to access personal data and obtain rectification or erasure of such data belongs to the essence of the right to data protection; legislation that does not provide any possibility for an individual to pursue legal remedies to gain access to personal data relating to him/her, or to obtain the rectification or erasure of such data and so indirectly check compliance with the law, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.[439]

UN good practice on personal data

Practice 26. Individuals have the possibility to request access to their personal data held by intelligence services. Individuals may exercise this right by addressing a request to a relevant authority or through an independent data-protection or oversight institution. Individuals have the right to rectify inaccuracies in their personal data. Any exceptions to these general rules are prescribed by law and strictly limited, proportionate and necessary for the fulfilment of the mandate of the intelligence service. It is incumbent upon the intelligence service to justify, to an independent oversight institution, any decision not to release personal information.

UN, Human Rights Council, Scheinin, M. (2010)

The ECtHR connects the information provision to the individual with the fact that the information no longer jeopardises the purpose of the surveillance.

ECtHR case law: notification and surveillance

"As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality. [...] [I]t has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases. The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. [I]n so far as the 'interference' resulting from the contested legislation is in principle justified [...], the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the 'interference'."

ECtHR, Klass and Others v. Germany, No. 5029/71, 6 September 1978, paras. 57–58

435 See also Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999, para. 169.
436 UN, Human Rights Council, Scheinin, M. (2010), p. 23.
437 CJEU, C-473/12, *Institut professionel des agents immobiliers (IPI) v. G. Englebert et al.*, 7 November 2013, para. 32.
438 CJEU, C-300/11, *ZZ v. Secretary of the State of Home Department*, 4 June 2013, paras. 53–54, 57, 61 and 64.
439 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, paras. 23, 95.

"Moreover, the impugned provisions interfere with [...] [Article 8 of the ECHR] rights in so far as they provide for the destruction of the data obtained and for the refusal to notify the persons concerned of surveillance measures taken in that this may serve to conceal monitoring measures interfering with the applicants' rights under Article 8 which have been carried out by the authorities."

ECtHR, Weber and Saravia v. Germany, *No. 54934/00, 29 June 2006, para. 79*

"However, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society', as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference. [A]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned."

ECtHR, Weber and Saravia v. Germany, *No. 54934/00, 29 June 2006, para. 135*

"According to the Court's case law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned [...]."

ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, *No. 62540/00, 28 June 2007, para. 91*

The legal frameworks of all EU Member States allow restrictions on the obligation to information and the right to access on the basis of a threat to national security and/or the intelligence services' objectives.

Differences are, however, observed as to the conditions and level of restrictions.[440] Some Member States do not provide for the obligation to inform and the right of access. Others provide for restrictions on the grounds of an existing threat to national security, yet these restrictions are not identical. Finally, some Member States balance the restrictions by giving oversight bodies the mandate to a) check whether the invoked national security threat justification is reasonable in fact and/or b) to exercise the right to access indirectly, i.e. on individuals' behalf.[441]

The obligation to information and the right to access are not provided for in eight Member States (the Czech Republic, Ireland, Latvia, Lithuania, Poland, Slovakia, Spain and the United Kingdom). This is attributable either to national data protection laws, which do not apply, or to derogations enshrined in specific laws. In the United Kingdom, the Independent Reviewer of Terrorism Legislation recommends that an Independent Surveillance and Intelligence Commission be created, which would be in charge of informing an individual of an error on the part of a public authority or communication service providers (CSP); and of notifying individuals of their right to lodge an application to the Investigatory Powers Tribunal, on their own initiative or at the suggestion of a public authority or CSP.[442]

Czech law illustrates this approach: the data protection law is not applicable and the specific laws stipulate that the intelligence service does not have to inform the persons whose rights they interfere with, nor do they have to provide access to the data.[443]

In some Member States, the obligation to inform and/or the right to access are restricted because of rules applicable to classified documents and official secrets. In Latvia, the specific law on the intelligence services stipulates that information gained by the intelligence services is of restricted access or classified as an official secret.[444] In Spain, the data protection law does not apply to classified documents and the specific laws do not provide for rules on information and access to the data. In Ireland, the data protection safeguards do not apply to "personal data that in the opinion of the Minister or the Minister for Defence are, or at any time were, kept for the purpose of safeguarding the security of the State".[445] The restrictions therefore apply even to data kept in the past for this purpose, without for instance, consideration of whether a threat to state security continues to exist.

In the other 20 Member States, the obligation to inform and right to access are provided for in the law, albeit with restrictions. The conditions vary regarding when the individual must be informed or may exercise the right to access, or other qualifying aspects. In the majority of these Member States, data protection laws alone, or in conjunction with specific laws, constitute the legal basis for the restrictions (Austria, Belgium, Bulgaria, Croatia, Cyprus, Greece, Germany, Finland, France, Hungary, Italy, Luxembourg, Malta and Slovenia). In Malta, for instance, the general data protection legislation provides that the obligation to inform and the right to access are not applicable to necessary measures in the interest of national security, while the specific laws do not further regulate this matter.[446] In five Member States, specific laws exempt the intelligence

440 See also UN, GA (2014c), para. 39.
441 See also Venice Commission (2015), pp. 35–36.
442 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 303.
443 Czech Republic, Security Information Service Act, Art. 16 (5).
444 Latvia, Investigatory Operations Law, Art. 24 (1).
445 Ireland, Data Protection Act, Section 1 (4) (a).
446 Malta, Data Protection Act, Section 23.

services' activities from the remit of general data protection legislation (Denmark, Estonia, the Netherlands, Romania and Sweden).

Independent of whether this is done on the basis of a general data protection law or in accordance with specific legislation, individuals' right to access and the services' obligation to inform tend to be restricted on the ground that the information would threaten the objectives of the intelligence services or national security. This restriction applies for the entire period during which such a threat exists. An assessment of the threat should therefore be performed over time to ensure the restriction is justified. The constitutionality of the provision allowing the general directors of the security services to refuse information requests at their discretion, on grounds of national security, was challenged before the Hungarian Constitutional Court. The court stated that the general directors may deny the request at their discretion, but only if the fulfilment of the request affects national security interests or the rights of others. The court held that the lower courts had misinterpreted the provision and did not attribute enough importance to the grounding of the refusals.[447] The ruling of the Constitutional Court prompted Act CIX of 2014, modifying the legislation on national security services; the new provisions are in effect as of 1 February 2015.[448]

In Sweden, the individual shall be notified of signals intelligence only if the search terms used therein are directly related to him/her, and not if reasons of confidentiality prevent notification.[449] This information shall be provided no later than one month after the data was collected. So far, no individuals have yet been informed, due to secrecy reasons.[450]

In Belgium, a 2010 reform[451] initially required informing individuals, upon their request, five years after the end of the surveillance. However, in 2011, following the reasoning of *Klass and Others v. Germany* and *Weber and Saravia v. Germany*, the Belgian Constitutional Court declared this provision unconstitutional. Specifically, it held that requiring the data subject to request notification – and not the intelligence services to provide it on their own initiative – did not comply with the right to respect for privacy.[452]

In six Member States, individuals are notified or information is provided at the end of surveillance, based on the anticipation that the threat to national security will exist throughout the surveillance (Bulgaria, Croatia, Denmark, Germany, the Netherlands, and Romania). In Romania, for instance, if the collected data does not justify a referral to the criminal investigating authorities and does not justify a continuation of the surveillance, surveillance will stop and the individuals under surveillance will be notified as to the surveillance activities and their duration.[453] In Denmark, there is a general obligation to inform the individuals at the end of surveillance,[454] provided the notification would not jeopardise the investigation and it is not disputed.[455]

In Germany, the restriction of the right to information is stipulated in Article 10 of the Basic Law, i.e. the constitution (*Grundgesetz*), and in the G 10 Act. As stated by the Federal Constitutional Court, the right may be restricted because of secret surveillance, but the individual shall be informed after the threat has disappeared.[456] Regarding targeted surveillance, individuals must be informed about the surveillance measures within 12 months after their discontinuation, unless the information would jeopardise the purpose of the surveillance measures or harm the interests of the country.[457] The same rule applies to strategic surveillance; however, the obligation to information is limited to processed data, not to the data immediately deleted after being deemed irrelevant for the purposes for which they were captured.[458]

In some Member States, additional conditions are enshrined in the law. In Bulgaria, notification of the individual and the right to access apply only to unlawful surveillance.[459] In Croatia, the obligation to inform the individual applies only if the individual submits a request, thus resulting in the exercise of the right to access.[460] In Germany, the right to access information

447 Hungary, Constitutional Court (*Alkotmánybíróság*), No. 9/2014 (III. 21.) (*9/2014. (III. 21.) AB határozat*), 17 March 2014.
448 Hungary, Act CIX of 2014 on the modification of Act CXXV of 1995 on the national security services and the modification of other Acts related to the national security control, 1 February 2015.
449 Sweden, Act on Signals Defence Intelligence, Section 11 (a) and (b).
450 Sweden, Swedish Data Inspection Board (*Datainspektionen*) (2010), p. 6.
451 Belgium, Law on the Intelligence and Security Services, Art. 2, as amended on 4 February 2010, Art. 2 of the Act on the Special Intelligence Methods used by the Intelligence and Security Services (*Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité*), 4 February 2010.
452 Belgium, Constitutional Court (Cour constitutionnelle), No. 145/2011, 22 September 2011.
453 Romania, Law No. 51/1991 concerning the national security of Romania, Art. 21 (2).
454 Denmark, Administration of Justice Act, Art. 788 (1).
455 *Ibid.*, Art. 788 (4).
456 Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999, paras. 170 and 287.
457 Germany, G 10 Act, Section 12 (1).
458 Germany, G 10 Act, Section 12 (2).
459 Bulgaria, Special Intelligence Means Act, Art. 34 (g) (3).
460 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 40 (1).

is dependent on the precise circumstances and on whether the individual can prove a special interest.[461]

Two Member States have established timeframes that must be exhausted before the obligation to inform applies or access rights can be exercised (Croatia and the Netherlands). In the Netherlands the duty to notify the individual came into force in 2007. Accordingly, individuals are notified five years after the NIS have carried out certain special surveillance measures, such as opening letters, intercepting telecommunications taking place through an automated process, and intercepting non-cable-bound telecommunications.[462] However, if an individual's personal data are still needed in the investigation, the five-year deadline for notification may be postponed.[463] The duty to issue a report is not compulsory if it is reasonably expected that the information will reveal the sources of a service, including those of other countries; seriously damage relations with other countries and international organisations; or reveal a specific application of a method or the identity of collaborators.[464] On similar grounds, the right of the concerned individual to access their data is provided by law.[465] In a report on the obligation to inform, the Dutch Review Committee stressed that very often there will be grounds to cancel notification, as for instance in case of signals intelligence, which involves third countries, meaning notification may seriously damage relations with these countries. It also emphasised that notification may take place after many years, since the activities of the intelligence service can be long-lasting; for example, operations started in 2002 may be considered on-going in 2009.[466] The Hague District Court has held that, in cases of secret surveillance, there is no absolute duty of notification,[467] and safeguarding secrecy prevails. However, the refusal to provide the data must be justified.[468] The individual may also exercise the right to access their own data indirectly through the DPA on the basis of the general data protection legislation. The DPA, however, may not give information regarding the existence or content of the data, and may solely confirm carrying out the necessary checks. In Croatia, the individual has to request information. In addition, the information is restricted during the time a threat to the fulfilment of the services' tasks exists. With regard to national security, irrespective of the existence of a threat, the services are not obliged to inform the individuals after the surveillance measures end.[469]

Ten Member States provide for the involvement of the oversight body or a court by scrutinising whether the invoked grounds for restricting the rights are reasonable or by indirectly exercising the individual's right to access.

In Austria, the right to access is restricted if access may threaten the security of the state. The individual may, however, turn to the DPA and request to check the legality of the police authorities' reply, which in cases of a threat to state security does not confirm or deny the data processing.[470] When the Legal Protection Commissioner determines that the use of personal data has breached an individual's rights, s/he has the duty to inform the individual concerned or, when for security reasons s/he cannot, to lodge a complaint with the DPA.[471]

In the Netherlands, the Review Committee shall be informed of the interior minister's refusal to disclose the information and the grounds for such.[472] In 2010, the Dutch Review Committee assessed the implementation of the intelligence service's notification obligation and noted that between 2007 (date of the entry into force of this obligation for the services) and 2010, nobody had been notified. The lack of notification was only in exceptional cases based on incorrect grounds, which, however, did not mean that there might not have been other valid grounds for the non-notification of the individuals. The oversight body noted that an active obligation to notify must be balanced against the complexity of other existing legal safeguards, for instance filing a complaint based on an allegation of the intelligence service's improper conduct or applying for an inspection of personal data processed by the intelligence service.[473]

In Germany, the G 10 Commission decides for how long the information is withheld, unless it unanimously decides that, even after five years, the information would endanger national interests.[474] In cases of targeted surveillance in 2013, of 1,944 persons or institutions regarding which the surveillance measures were discontinued, 650 were informed. The G 10 Commission

461 Germany, Federal Act on the protection of the Constitution (*Bundesverfassungsschutzgesetz*), 20 December 1990, as amended, Section 15; Germany, Act on the Federal Intelligence Service, Section 7.
462 The Netherlands, Intelligence and Security Services Act 2002, Art. 34.
463 *Ibid.*, Arts. 47 and 53.
464 *Ibid.*, Art. 35 (7).
465 *Ibid.*, Arts. 47 and 51.
466 The Netherlands, CTIVD (2010), p. 149.
467 The Netherlands, Hague District Court (*Rechtbank Den Haag*), ECLI:NL:RBDHA:2014:8966, 23 July 2014.
468 The Netherlands, Hague District Court (*Rechtbank Den Haag*), ECLI:NL:RBSGR:2011:BP4872, 16 February 2011.
469 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 40 (4).
470 Austria, Data Protection Act 2000 (*Datenschutzgesetz 2000 – DSG 2000*), BGBl. I. Nr. 165/1999, as amended, Section 26 (2) in conjunction with Section 30 (3).
471 Austria, Police Powers Act, Section 91 (d) (3). A case regarding this power is pending before the ECtHR. See ECtHR, *Tretter and Others v. Austria*, No. 3599/10, communicated on 6 May 2013.
472 The Netherlands, Intelligence and Security Services Act 2002, Arts. 35 (7), 47, 50 and 55.
473 The Netherlands, CTIVD (2010), pp. 21–23 and 113 f.
474 Germany, G 10 Act, Section 12.

decided to not yet inform 1,079 persons/institutions, and unanimously agreed 260 would never be informed.[475] In cases of strategic surveillance, the G 10 Commission dealt with seven cases for information related to terrorism. In three cases, the commission decided to postpone providing the information, in one case to reject the information indefinitely, and in three cases it took note that the intelligence service (BND) provided the information. In three cases linked to arms proliferation, the G 10 Commission noted the BND had provided the information, and in two cases linked to human trafficking, the G 10 Commission decided to postpone the provision of information. In three cases related to hostage taking, the G 10 Commission decided to postpone the provision of information and took note that, in the third case, the BND had already provided it.[476]

In Cyprus and Greece**,** the obligation to inform and the right to access, as stipulated by the data protection laws, may be restricted or lifted by a decision of the DPA on the grounds of national security, upon request of the intelligence services. In Cyprus, for instance, the DPA issued a decision in 2002 lifting the obligation to information with respect to the Central Intelligence Service's data files.[477] In Greece, in addition to the role of the DPA, the specific law on interception of communications grants the special oversight body for safeguarding the secrecy of communications (ADAE) the discretion to inform the individual once the surveillance measure has ended, provided this does not compromise the purpose of the investigation, otherwise the information shall be destroyed.[478] Since this is not obligatory, the safeguard relies on the body's discretion to decide whether the individual shall be informed. The annual activities reports from the years 2004–2013 do not mention any activity of the oversight body regarding the provision of information to individuals.[479]

In Denmark, there is a general rule to inform the individual at the end of the surveillance measures. If notification would jeopardise the investigation or there are other arguments against it, the judiciary may permit withholding – or delaying the provision of – the information.[480] In addition to this basic rule, the specific laws foresee that in extraordinary cases an individual may access, in part or in full, the information by filing a claim to the Oversight Committee, even while the surveillance is being carried out.[481] However, when the access request addresses the activities of the Danish Defence Intelligence Service, these rights are granted only to Danish and Nordic citizens, foreigners with a residence permit, and asylum seekers who have resided in the country for more than six months.

In Belgium, France, Italy and Luxembourg, individuals may exercise the right to access their own data indirectly through the DPAs or the competent oversight body (Luxembourg). These bodies implement the necessary controls to ensure data is processed lawfully. However, the individual is not informed which data are processed if doing so would threaten national security. Though a right of indirect access is not granted as such in Portugal and Sweden, the law consequently provides for a similar right: an individual may request the oversight body to check whether his/her data are subject to unlawful surveillance.[482] The Swedish oversight body, the Swedish Defence Intelligence Commission, shall only notify the individual that the check has been carried out, but not whether he or she has been subject to surveillance.[483] The same approach is prescribed in the French law on intelligence, which does not amend the current legal framework on this specific matter.[484] In 2014, the French oversight body dealt with 110 complaints (75 in 2013 and 52 in 2012).[485]

Only two of the five Member States authorised to conduct signals intelligence distinguish between the obligation to inform an individual in case of targeted surveillance versus their obligation to do so when an individual is affected as a result of signals intelligence. These provisions focus on the obligation to inform an individual regarding data collection that is conducted automatically and according to pre-defined filters. In this phase, the laws provide for the lifting of the obligation to inform. In particular, the obligation to inform does not apply if a) the search terms are not directly related to the individual (Sweden) or b) the data are immediately deleted after they have been captured through use of the selectors (Germany).

475 Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 6.
476 Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 8 f.
477 Cyprus, Decision of the Data Protection Authority, 2 September 2002.
478 Greece, Act 2225/1994 on the protection of freedom of correspondence and communications and other provisions, Art. 5 (9).
479 Greece, Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*), Annual reports for the years 2004–2013, www.adae.gr/ektheseeis-pepragmenon/
480 Denmark, Administration of Justice Act, Art. 788 (4).
481 Denmark, Act No. 602 of 12 June 2013 on the Danish Defence Intelligence Service Service (*Lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE)*), 12 June 2013, Arts. 9 and 10.
482 Sweden, Act on Signals Defence Intelligence, Section 10 (a); Portugal, Organic Law 4/2004 of 6th of November amending the Framework Law of the Information System of the Portuguese Republic (*Lei Orgânica No. 4/2004 de 6 de Novembro Altera a Lei Quadro do Sistema de Informações da República Portuguesa*), 6 November 2004, Art. 27.
483 Klamberg, M. (2010), p. 128.
484 France, Interior Security Code, Art. L. 833-4.
485 See France, CNCIS (2015a), p. 89 and CNCIS (2015b), p. 97.

3.2. Judicial remedies

Courts provide an avenue for individuals to complain about interference with their privacy and to seek a remedy, including in the area of surveillance. However, several obstacles stand in place for an individual complaining about signals intelligence: the courts' lack of specialisation; general procedural obstacles, such as costs, delays or complexity; and a lack of concrete evidence and a high burden of proof for establishing the veracity of evidence, or possible invocation of state secrecy privilege, including 'neither confirm nor deny' stances. These major obstacles can, in some cases, be mitigated in systems with specialised tribunals/courts, where judges possess the knowledge necessary to decide on often technical matters and are also allowed to access secret material. Other elements that can facilitate an individual's access to remedies include more relaxed standing proof rules, class actions and effective protection of whistleblowers. The Parliamentary Assembly of the Council of Europe has stated that whistleblowing is "the most effective tool for enforcing the limits placed on surveillance".[486] The Committee of Ministers of the Council of Europe adopted a Recommendation on the protection of whistleblowers, encouraging Member States to set up a protective legal framework.[487] The European Parliament called on Member States to grant whistleblowers international protection from prosecution.[488] Indeed, in the specific context of signals intelligence, in particular where the information is not provided to an individual and access cannot be obtained through oversight bodies, independent journalists and whistleblowers play an essential 'intermediary' role in facilitating access to remedies. The Snowden revelations provide a good example of this since they led to both national and international litigation.[489]

3.2.1. Lack of specialisation and procedural obstacles

Every Member State gives individuals the possibility to complain about privacy violations via the courts, regardless of whether or not these have occurred because of targeted or signals intelligence.

National laws may determine which of the ordinary courts are competent to review surveillance complaints. In France and Germany, the highest administrative court is competent.[490]

When national laws provide DPAs with powers over the activities of intelligence services, depending on the issue at stake, the DPA may need to be approached before the courts,[491] which will then act as appellate bodies tasked with reviewing the decisions of an administrative body.

In *Schrems v Data Protection Commissioner*, [492] for example, the plaintiff complained to the Irish Data Protection Commissioner that the disclosures made by Edward Snowden demonstrated there was no effective data protection regime in the United States. The plaintiff requested the Data Protection Commissioner to exercise his statutory powers to order a cease to the transfer of personal data from Facebook Ireland to its parent company in the United States. The Data Protection Commissioner refused to investigate the claim, and maintained that he was bound by the European Commission's Decision on Safe Harbour principles of July 2000,[493] which provides the legal basis for the transfer of personal data from EU to American companies, and that the data protection regime in the United States was adequate and effective as long as companies that process the data or transfer data to the United States self-certify that they comply with the principles set down in Safe Harbour. The applicant challenged the lawfulness of the Data Protection Commissioner's refusal. The High Court then referred the case to the CJEU. The CJEU held that DPAs are not prevented from investigating a complaint and, in case of doubts as to the validity of a legislative act, from bringing the case before national courts, which may make a reference to the CJEU for a preliminary ruling to examine its validity.[494]

As past FRA research on access to data protection remedies shows, however, ordinary courts' lack of expertise in the area of data protection was one of the major obstacles to effectively remedying data protection violations.[495]

This finding is certainly of relevance in the area of surveillance, where the highly technical nature of intelligence matters requires relevant expertise on the part of the judge. From the perspective of a complainant, judicial lack of expertise in dealing with intelligence

486 PACE, Committee on Legal Affairs and Human Rights (2015b), p. 31.
487 PACE, Committee on Legal Affairs and Human Rights (2015a).
488 European Parliament (2014).
489 See also the concept of 'insider' complaints in Forcese, C. (2012), p. 182. See also PACE, Committee on Legal Affairs and Human Rights (2015a).
490 France, Interior Security Code, Art. L. 801–1; Germany, Code of Administrative Court Procedure, (*Verwaltungsgerichtsordnung*), 21 January 1960, as amended, Section 50 (1) (d).
491 FRA (2014c), Section 5.3.
492 Ireland, High Court, *Schrems v. Data Protection Commissioner*, [2014] IEHC 310, 18 June 2014.
493 European Commission (2000).
494 CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 65–66.
495 FRA (2014c).

services may lead a judge to defer to the national intelligence services and their claim that national security and other special circumstances apply.[496]

Furthermore, for individuals to obtain adequate redress for a suffered harm, they must usually bring sufficient evidence of unlawful surveillance. In the context of targeted or signals intelligence, individuals often do not have the fully-fledged right to be notified that they have been the subject of surveillance measures and/or to have access to such data. There is often no information provided in practice. In the United Kingdom, for instance, there is a well-established policy of 'neither confirm nor deny' responses to questions about sensitive matters of national security. Individuals have therefore little opportunity to submit concrete evidence, which often makes the courts (but in some cases also non-judicial bodies) inaccessible avenues in practice.[497] The Council of Europe Commissioner for Human Rights stated that "such modifications to proceedings can make it difficult or impossible to have a fair trial".[498] The Irish High Court acknowledged the inability to provide evidence in such situations.[499]

A judgment of the Federal Administrative Court in Germany illustrates the difficulties individuals face when confronted with strict procedural rules on providing concrete evidence to prove their victim status.[500] In this case, a complaint was lodged against strategic surveillance of communications under Section 5 of the G 10 Act by the Federal Intelligence Service (BND), after it was reported that 37 million communications were caught in 2010 by the dragnet search, mostly emails, of which only 12 were considered 'relevant'. The complainant argued that it was very likely that he was affected by the dragnet search because of his frequent international email communications as a professional lawyer with contacts abroad; hence, he requested a statement that the BND acted in a disproportionate manner and violated his right to privacy of communications. The Federal Administrative Court, however, held that the complaint was inadmissible since complaints against strategic surveillance of telecommunications under the relevant domestic law were only admissible if it was evident that the complainants had been affected. The court added that the right to an effective remedy does not mean that the burden of proof must be eased on the ground that the individual is not informed when the data collected through the search terms are immediately deleted.

In this context and in light of existing ECtHR jurisprudence on victim status, the possibility to challenge the constitutionality of the mere existence of legislation permitting secret measures, without having to allege that such measures were in fact applied to an individual, is an important safeguard.[501]

ECtHR case law: interference and victim's status

"The Court further notes that the applicants, even though they were members of a group of persons who were likely to be affected by measures of interception, were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8 [of the ECHR], irrespective of any measures actually taken against them."

ECtHR, Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 78*

The applicants in what became known as the *Weber and Savaria* case complained about the expansion of the Federal Intelligence Service's (BND) powers of strategic telecommunications surveillance. The German Constitutional Court ruled that the legal provisions on the competences of the BND regarding surveillance for the purposes of pre-empting money laundering, the use of obtained data, the transfer of data to other authorities and on the limited obligation to notify affected persons, were not compatible with the German Basic Law. The court also demanded stronger oversight by the G 10 Commission.[502] Because of this judgment, the law was substantially revised in June 2001.[503] The court applied similar rules to the burden of proof as the ECtHR.

In addition to these specific procedural obstacles, and the fact that individuals often simply do not know they are a target of or encompassed by surveillance, going to court often exposes individuals to lengthy, time-consuming, complicated and costly procedures.[504]

496 Forcese, C. (2012), p. 186.
497 See FRA (2014c).
498 Council of Europe Commissioner for Human Rights (2015), p. 27.
499 Ireland, High Court, *Schrems v. Data Protection Commissioner*, [2014] IEHC 310, 18 June 2014, para. 42. See also CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, Advocate General's Opinion, 23 September 2015.
500 Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 6 CN 1.13, 28 May 2014.
501 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006; ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978, para. 34.
502 Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999.
503 Germany, G 10 Act.
504 FRA (2011); FRA (2014c).

This is why individuals may prefer to access justice via non-judicial avenues[505] or through intermediaries, such as relevant civil society organisations. The latter may play a vital role in taking such complaints to court when class actions are allowed,[506] as well as in bringing cases of a more general nature requesting access to specific information on the activities and investigative methods of intelligence authorities to contribute to greater transparency and accountability in this area.[507] However, civil society organisations often lack adequate resources, and few are able to offer comprehensive services to victims of data protection violations.[508]

3.2.2. Specialised judges and quasi-judicial tribunals

Two Member States decided to introduce a system of specialised judges or courts to deal with cases in the area of surveillance. Furthermore, although not courts as such, specific quasi-judicial mechanisms in Germany and Belgium are analysed in this section. Their role, composition and powers make them resemble courts, which makes them distinct from other non-judicial bodies analysed in Section 3.3. A clear advantage of these specialised courts and bodies is, among others, their expertise in the area of surveillance, which is not necessarily the case of ordinary courts.

National practices of appointing a specialised judge to adjudicate these matters (Ireland) or establishing specialised tribunals to hear complaints about unlawful surveillance by intelligence authorities (United Kingdom) can be seen as contributing to the development of judicial expertise in the area. Such systems can also facilitate different arrangements on judicial access to classified or top-secret information.[509] Indeed, in some jurisdictions, civil or administrative courts may be empowered to award damages, but in practice, suits in the general courts are made difficult by intelligence services' claims of secrecy due to national security.[510]

CJEU case law: national security and due process

"[I]f, in exceptional cases, a national authority opposes precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision [...], by invoking reasons of State security, the court with jurisdiction in the Member State concerned must have at its disposal and apply techniques and rules of procedural law which accommodate, on the one hand, legitimate State security considerations regarding the nature and sources of the information taken into account in the adoption of such a decision and, on the other hand, the need to ensure sufficient compliance with the person's procedural rights, such as the right to be heard and the adversarial principle."

CJEU, C-300/11, ZZ v. Secretary of the State of Home Department, *4 June 2013, para. 57*

In Ireland, a complaint can be made to the Complaints Referee, a judge of the Circuit Court nominated to hold this specialised position. The referee may investigate whether there has been a contravention of the relevant provisions of the Act on interception of communications.[511] If a complaint is upheld, the Complaints Referee will quash the interception, report the matter to the Taoiseach (prime minister) and recommend a compensatory payment. To date, this has not occurred. In parallel, a civil action for damages for breach of privacy protected by the constitution can also be taken in the High Court. [512]

In the United Kingdom, the Investigatory Powers Tribunal (IPT), although not strictly speaking a court, was established to deal with individuals' complaints against surveillance. The ECtHR not only confirmed that the procedure before the IPT, including existing procedural restrictions imposed by the law on such procedure, taken as a whole, satisfied the requirements of Article 6 (right to a fair trial) and 13 of the ECHR,[513] but also highlighted the positive aspects of the British system.[514] The IPT is composed of specialised counsels (the president and vice president must both hold or have held senior judicial posts).[515] It has the exclusive jurisdiction to hear claims relating to interception and the conduct of the intelligence agencies. The IPT, however, rarely publishes its decisions or holds public hearings. At the same time, the IPT's powers are strictly limited to assessing whether legislation has been complied with and authorities have acted 'reasonably'. The IPT has

505 FRA (2014c).
506 Poland, Administrative Court in Warsaw (*Wojewódzki Sąd Administracyjny w Warszawie*), *Helsinki Foundation for Human Rights v. ABW*, II SA/Wa 710/14, 24 June 2014, pending appeal to the Supreme Administrative Court.
507 Poland, Helsinki Foundation for Human Rights (2015).
508 FRA (2014c).
509 Chesterman, S. (2011), p. 218.
510 See Forcese, C. (2012), p. 186; Bigo, D. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2014).
511 Ireland, Interception of Postal Packets and Telecommunications Messages (Regulation) Act.
512 Ireland, Supreme Court, *McGee v. Attorney General*, [1974] I.R. 284, 19 December 1973.
513 ECtHR, *Kennedy v. UK*, No. 26839/05, 18 May 2010.
514 ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, para. 98.
515 United Kingdom, Regulation of Investigatory Powers Act 2000, Sections 65–70.

only ruled against the intelligence and security services twice: in *Liberty, Privacy International, Bytes for All and Amnesty vs. UK*; and *Belhaj vs. Straw*. The Independent Reviewer of Terrorism Legislation recommended that the IPT should have its jurisdiction expanded, that it be given the power to make declarations of incompatibility, and that its rulings be subject to appeal on points of law.[516]

It has been the long-standing policy of the United Kingdom government to give a 'neither confirm nor deny' (NCND) response to questions about matters sensitive to national security. The IPT recognised the legitimate purpose and value of such a response in several cases. It held that "the NCND policy is needed to help to preserve secrecy", and that it does not interfere with the right to privacy in cases where there is no relevant information held on the complainant.[517] In 2010 for example, 30 % of the 164 complaints received by the IPT were directed against security and intelligence services. The remaining complaints were directed against other types of public authorities that fall under the mandate of the IPT, such as law enforcement agencies (32 %); local authorities (10 %); and other public authorities, such as the Department for Work and Pensions (28 %). There are no specific statistics available in the IPT's annual report as to how many of the complaints directed against an intelligence agency were actually upheld in 2010. General statistics on the outcomes of 2010 complaints indicate, however, that the IPT upheld the complaint and ruled in favour of the complainant in six of 210 cases (which covers all complaints resolved by the IPT in 2010, including those carried over from previous years).[518]

Following the Snowden revelations, various NGOs brought a complaint before the IPT in 2014. The claimants alleged that the use of the Tempora programme[519] is unlawful, as is the subsequent disclosure and receipt of intercepted material to and from the NSA. The IPT issued two partial rulings on the matter. In its first judgment, the tribunal found Tempora's actions legal in principle.[520] However, since the intelligence services adhered to their policy of 'neither confirm nor deny', the tribunal was only able to assess whether the legal framework would allow GCHQ to solicit, receive, store and transmit private communications of individuals located outside the United Kingdom on the basis of an agreed case. The tribunal did not assess the proportionality of its use. The court also ruled on the legality of the British intelligence services receiving data from countries such as the United States, based on communications intercepted by using programmes such as Prism or Upstream. The IPT concluded that the claims were unfounded, based on its finding that there are "sufficient safeguards in place" that afford individuals suitable protection. The decision was based on the disclosure of previously secret policies revealed by the security and intelligence services during the trial. As a result, in its second judgment, the IPT found that GCHQ's access to the data shared by the NSA was unlawful before December 2014, because the policies that govern it were secret before then, and that during that time it had therefore violated Articles 8 and 10 of the ECHR.[521] Privacy International and co-claimant Bytes For All plan to contest the first ruling before the European Court of Human Rights.[522]

In Belgium, the Standing Committee I has a dual function. In its judicial function, its powers are similar to those of the United Kingdom's IPT. It investigates complaints and rules on the legality of intelligence measures, and can order their cessation when an individual has been directly affected by specific or exceptional methods of data collecting. The concept of specific and exceptional methods covers all the intelligence operations relevant to this report.[523] Specific methods include, among others, the inspection of identification data, localisation and call-associated data of electronic communications and requesting the cooperation of an operator, or direct access to data files.[524] Penetrating an IT system is listed among exceptional methods.[525]

The German G 10 Commission also functions, in addition to general courts, as a quasi-judicial institution, whose decisions are binding on the intelligence services and the government. The G 10 Commission is not only involved in the *ex ante* approval of surveillance orders, but also investigates the legality and necessity of applied intelligence measures on its own initiative or upon an individual complaint.[526]

516 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 305.
517 United Kingdom, IPT (2004).
518 United Kingdom, IPT (2010).
519 This includes the upstream surveillance activity by which the British intelligence services, including GCHQ, intercept large fibre optic cables that carry huge amounts of internet users' private communications. FRA (2014a).
520 United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014.
521 United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 6 February 2015.
522 See: https://www.privacyinternational.org/?q=node/555. See also ECtHR, *Bureau of investigative journalism and Alice Ross v. the United Kingdom*, No. 62322/14, communicated on 5 January 2015.
523 Belgium, Standing Committee I (2015), p. 71 and following.
524 Belgium, Act on the Special Intelligence Methods used by the Intelligence and Security Services, Art. 18 (1).
525 *Ibid.*, Art. 18 (2).
526 Germany, G 10 Act, Section 15.

3.3. Non-judicial remedies: independence, mandate and powers

As stated above, in addition to courts (ordinary and specialised) and the two specific quasi-judicial institutions in Germany and Belgium, there are other non-judicial bodies with a human rights remit that deal with violations of the right to protection of personal data, and that have an essential role in facilitating access to justice. These include national data protection authorities (DPAs) and ombudsperson institutions. In the area of strategic surveillance, some countries also give oversight bodies the power to provide remedies – which can be of parliamentary, executive or expert nature – to individuals. The extent to which these bodies can provide an effective remedy, however, depends on their independence and other factors, such as specialised knowledge (or lack thereof), and the power to not only access materials and investigate the issues at stake, but also to issue binding decisions as opposed to non-binding recommendations.

3.3.1. Types of non-judicial bodies

Non-judicial options are usually more accessible for individuals than judicial mechanisms because procedural rules are less strict, bringing complaints is less costly and proceedings are faster. This was confirmed by previous FRA evidence, in particular the access to data protection remedies, where more complaints tend to be lodged with national DPAs, and few complainants go through judicial procedures. At the same time, however, the number of non-judicial bodies reported operating in the area of data protection other than DPAs is small, and many non-judicial bodies only have limited powers to offer remedies.[527]

This research confirms an additional problem with the scope of the DPAs' mandate. Compared to other fields of data processing activities and other data controllers in the public and private sectors, DPAs' powers over intelligence services, including their remedial role, are weak.

As for the remedial role of oversight bodies, the parliamentary committees of several EU Member States, namely Croatia, Hungary, Lithuania and Romania, also function as complaints-handling bodies. Oversight bodies other than parliamentary committees, such as those entailing executive and expert oversight (other than DPAs), may also provide remedies, as is the case in Belgium, Croatia, Germany, Denmark, Hungary, Malta, the Netherlands, Portugal and Sweden.

Finally, in all EU-28 there are general ombudsperson institutions empowered to provide remedies. However, these are often only in the form of a non-binding recommendation in cases of maladministration by a public authority, for instance. Moreover, just as with some DPAs, their mandate may explicitly exclude the issue of national security or the actions of national intelligence authorities. This is true of the United Kingdom Parliamentary Commissioner for Administration, for example.[528] Considerably more relaxed rules on legal standing are a main advantage of turning to ombudsperson institutions, permitting individuals to bring more generic complaints against the intelligence services.[529] In the Netherlands, for instance, everyone has the right to complain to the ombudsman about the activities or alleged activities of the ministers, the heads of the intelligence services, the coordinator and the persons employed by the intelligence services. The complainant must first apply to the responsible minister before filing his/her complaint to the ombudsman.[530] The independence of ombudsperson institutions and their direct accountability to the parliament in most of the 28 EU Member States is also beneficial. But this must be seen in the wider context of their remedial powers, which can be quite limited, as the section on powers and specialisation of non-judicial bodies shows.

3.3.2. The issue of independence

The validity of non-judicial dispute mechanisms can only be accepted if they themselves conform to general requirements of fairness, including impartiality and independence from the intelligence services and the executive. The latter includes a stable mandate expressed through appointment and dismissal conditions. In the case of an executive oversight body with remedial powers, for example, the question of independence arises when it also has the power to warrant surveillance. On the other hand, parliamentary or expert oversight bodies may have more autonomous administrative structures. But autonomy alone does not guarantee the effectiveness of a remedy – sufficient knowledge is also crucial. Furthermore, how members of oversight bodies are appointed, and their place in the administrative hierarchy, are also important aspects to consider when assessing a body's independence.

While some aspects of independence need to be enshrined in the law, others can be re-affirmed in a code of ethics at an institutional level. In September 2014,

527 FRA (2014c), p. 7.

528 United Kingdom, Parliamentary Commissioner Act 1967, 22 March 1967, Section 5.

529 Forcese, C. (2012), p. 184.

530 The Netherlands, Intelligence and Security Services Act 2002, Art. 83 (1) in conjunction with The Netherlands, General Administrative Law Act (*Algemene Wet Bestuursrecht*), 4 June 1992, Art. 9 (1) (3). See also The Netherlands, CTIVD (2014), p. 27.

for instance, the French oversight expert body adopted such a code, spelling out the various criteria that must be met to secure independence.[531] The French Law on intelligence spelled out specific ethical rules, including on CNCTR members' independence, specifying that they should not receive any instructions from any authority, and that members should not have incompatible mandates, links to the intelligence services, or perform any other professions or elective mandates.[532]

In the context of remedial infrastructure in the area of surveillance (see Figure 5), independence can be an issue with oversight bodies that have remedial powers. Some cases show that they are susceptible to conflicts of interest, which may prompt doubts about their impartiality and independence. [533] This does not include DPAs, whose independence in the context of providing remedies in the area of data protection in general was assessed in prior FRA studies.[534]

Executive oversight bodies with remedial powers may have their independence questioned if they also possess the power to warrant surveillance.[535] In Hungary, for example, oversight and complaints-handling functions are both performed by one executive oversight institution: government and its different ministries.

UN good practices on effective remedy

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services are independent of the intelligence services and the political executive [...].

UN, Human Rights Council, Scheinin, M. (2010)

Many parliamentary and expert oversight bodies (excluding DPAs) are by law structurally and formally capable of independent oversight. FRA data shows that the administrative structures of parliamentary and expert bodies are granted more autonomy than executive oversight bodies with remedial powers. Autonomy alone does not guarantee unbiased and strong oversight, however; it must be supported by various factors, including sufficient knowledge.

The appointment of expert oversight bodies and their place in the administrative hierarchy are important aspects to consider when assessing a body's independence. The authority that appoints members or the governing structure of oversight and remedial bodies should not control and supervise the work of the intelligence agencies. Malta and Sweden, where the remedial function of expert bodies is subject to executive control, serve as examples of systems where the controllers and the controlled agencies might not be sufficiently separated.

In Malta, the prime minister appoints the Commissioner of the Security Service, who is, at the same time, responsible for reviewing the legality of the warrants the prime minister issues. Additionally, the prime minister also appoints the head of the security services. The entire system is therefore dependent on one authority. The commissioner is accountable solely to the prime minister, and cannot communicate with the media or be summoned to court. Moreover, decisions of the commissioner cannot be subject to appeal, nor may they be questioned before a court. This goes against the well-established standards requiring decisions of non-judicial dispute mechanisms to be supervised by a judicial body. The 1996 Security Service Act also curtails the commissioner's ability to bring a problem to the public's attention by directing him/her to only report to the prime minister.[536] Similarly in Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government and its chair and vice chair must be or have been judges. The government has full discretion to appoint the chair and vice chair, while the parliament nominates the remaining members.[537]

Determining the optimal distance between the controlled and the controllers is complex, since providing up-to-date expertise requires oversight bodies to work side by side with the intelligence agencies. Therefore, while ties that are too close may lead to a conflict of interest, too much separation might result in oversight bodies that, while independent, are very poorly informed. Chesterman describes the flipside of independence: "The advantages of review are that it is normally conducted by an independent body, and typically results in a public finding. These are also the disadvantages. Independence can mean unfamiliarity with the agency being examined, leading to practical and political problems such as access to information or sensitivity to context".[538] Other relevant considerations are the term for which the members and the head of oversight bodies are appointed, and the dismissal rules.

Expert bodies such as the Belgian Standing Committee I, the Danish Oversight Committee, the Croatian Council for Civic Oversight of Security and Intelligence Agencies, and the Portuguese Council for the Oversight of the Intelligence System of the Portuguese Republic, are appointed for a fixed tenure, and their members enjoy personal and functional independence. Forcese suggests an expert body be staffed by persons of

531 France, CNCIS (2015a), p. 65 and following.
532 France, Interior Security Code, Art. L. 832–1 and Art. L. 832–2.
533 Forcese, C. (2012).
534 FRA (2014d); FRA (2012).
535 Born, H. and Leigh, I. (2005), p. 68.
536 Malta, Security Service Act, Section 12.
537 Sweden, Act on Signals Defence Intelligence, Section 10.
538 Chesterman, S. (2011), p. 313.

diverse backgrounds, but with a minimum quota having legal training.[539]

The composition of parliamentary oversight committees in Hungary, Croatia, Italy, Lithuania and Romania, although independent from the intelligence services and the executive, is based on the current composition of the parliament, and less on expertise. In some cases this shortcoming in expertise is compensated by the opportunity to hire external advisers, such as in Hungary.[540] Still, according to some, "[C]omplaints handling may require close scrutiny of minutiae, rules of procedural fairness, and evidentiary considerations relating to, for example, the credibility of witnesses, which are better handled in a more quasi-judicial environment",[541] such as the United Kingdom's Investigatory Powers Tribunal (IPT). As for parliamentary oversight bodies with remedial powers in particular, according to the Venice Commission, "The constitutional principle of separation of powers can make it problematic for a parliamentary body to play such a quasi-judicial role".[542]

3.3.3. Powers and specialisation of non-judicial remedial bodies

Any non-judicial entity tasked with providing a remedy must have the power to conduct a thorough review of the case, which includes having access to all relevant materials and having the power to grant a binding remedy.[543] Although this section focuses on the powers of non-judicial remedial bodies, the question of specialisation of such bodies – which represent a challenge in case of ordinary courts – is also briefly touched upon.

UN good practices on effective remedy and data protection

Practice 10. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services [...] have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.

Practice 25. An independent institution exists to oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein.

UN, Human Rights Council, Scheinin, M. (2010)

539 Forcese, C. (2012), pp. 188–189.
540 Hungary, homepage of the Parliamentary Committee on National Security, www.parlament.hu/web/nemzetbiztonsagi-bizottsag.
541 Forcese, C. (2012), p. 190.
542 Venice Commission (2015), p. 32.
543 UN, Human Rights Council, Emmerson, B. (2014), para. 61.

The UN Office of the High Commissioner for Human Rights points out: "[F]or remedies to be effective, they must be capable of ending ongoing violations, for example, through ordering deletion of data or other reparation. [S]uch remedial bodies much have [t]he capacity to issue binding orders."[544]

ECtHR case law: lack of effective remedy

"Turning to the present case, the Court observes that the Parliamentary Ombudsperson and the Chancellor of Justice have competence to receive individual complaints and have a duty to investigate them to ensure that the relevant laws have been properly applied. By tradition, their opinions command great respect in Swedish society and are usually followed. However, [...], the Court found that the main weakness in the control afforded by these officials is that, apart from their competence to institute criminal proceedings and disciplinary proceedings, they lack the power to render a legally binding decision. In addition, they exercise general supervision and do not have specific responsibility for inquiries into secret surveillance or into the entry and storage of information on the Security [Service] register. As it transpires [...], the Court found neither remedy, when considered on its own, to be effective within the meaning of Article 13 of the Convention."

ECtHR, Segerstedt-Wiberg and Others v. Sweden*, No. 62332/00, 6 June 2006, para. 118*

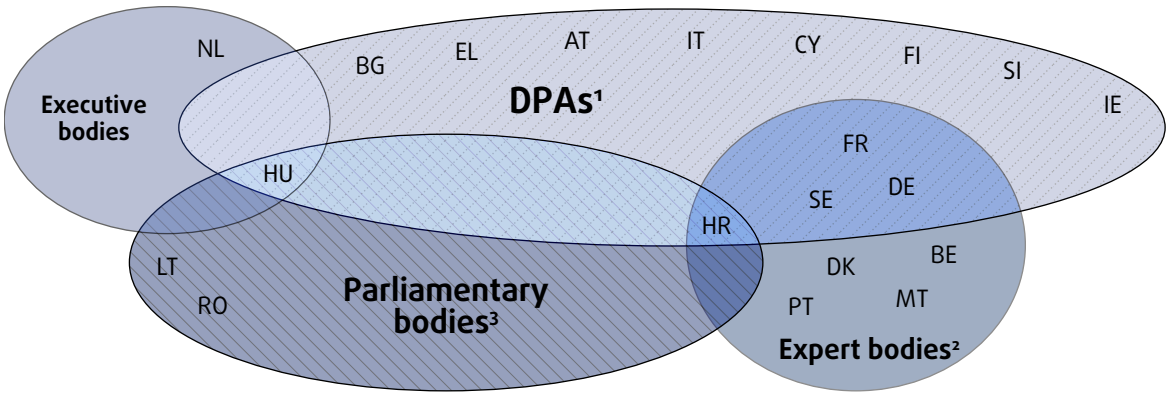
Figure 6 shows which of the different oversight bodies (including DPAs) have the power to hear complaints in different Member States. In some, more than one type of oversight body is mandated to hear individual complaints. But, as indicated in the explanatory notes, not all of these bodies have the power to issue binding decisions regarding these complaints. Additionally, several EU Member States have oversight bodies with no remedial powers. These include the Czech Republic, Estonia, Latvia, Luxembourg, Poland, Slovakia, Spain and the United Kingdom. Furthermore, the below categorisation is made on the basis of relevant provisions of surveillance laws, and is therefore not an assessment of their practical implementation.

As Figure 6 shows, only the Romanian parliamentary committee has the power to receive complaints and issue binding decisions. The extent to which this avenue can provide an effective remedy also depends on whether members of parliament who belong to these special parliamentary committees have experience in the field of intelligence and qualified supporting staff.

Among the independent expert bodies (excluding DPAs), the German G 10 Commission and the Danish Oversight Committee are among those that have the power to receive complaints and issue binding decisions. The G 10 Commission is competent to handle

544 UN, OHCHR (2014), para. 41.

Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member State



Notes:

1. *The following should be noted regarding national data protection authorities: In Germany, the DPA may issue binding decisions only in cases that do not fall within the competence of the G 10 Commission. As for 'open-sky data', its competence in general, including its remedial power, is the subject of on-going discussions, including those of the NSA Committee of Inquiry of the German Federal Parliament*
2. *The following should be noted regarding national expert oversight bodies: In Croatia and Portugal, the expert bodies have the power to review individual complaints, but do not issue binding decisions. In France, the National Commission of Control of the Intelligence Techniques (CNCTR) also only adopts non-binding opinions. However, the CNCTR can bring the case to the Council of State upon a refusal to follow its opinion. In Belgium, there are two expert bodies, but only Standing Committee I can review individual complaints and issue non-binding decisions. In Malta, the Commissioner for the Security Services is appointed by, and accountable only to, the prime minister. Its decisions cannot be appealed. In Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliament.*
3. *The following should be noted regarding national parliamentary oversight bodies: only the decisions of the parliamentary body in Romania are of a binding nature.*

Source: *FRA (2015)*

complaints regarding both targeted and strategic surveillance. In 2013, the G 10 Commission received 21 complaints linked to targeted surveillance, but found no violation of the right to privacy (Article 10 of the constitution). The commission noted that one case related to strategic surveillance was pending before the Federal Administrative Court.[545]

The Belgian Standing Committee I has the same powers when reviewing the legality of specific and exceptional methods, and also receives complaints regarding, or denunciations of, the functioning, actions, conduct or failure to act of the intelligence services. In the former case, its decisions are binding, while in the latter, it produces non-binding opinions or recommendations to the competent authorities.[546] Its role is not aimed at compensating the victim. This can be done before a judge. It provides moral compensation to the individual, and a useful basis for a judicial claim. The role of the oversight body in the case of complaints is to uphold constitutional rights and the law. Denunciations are aimed at, but not limited to, whistleblowers wishing to complain about their own administration. When dealing with these, the Standing Committee I tries to improve the efficiency of the intelligence services. Some of Standing Committee I's conclusions have triggered legislative reforms or changes in management. The complaints and denunciations follow neither strict rules of procedure nor formalities. The Standing Committee I receives an average of 15 complaints and denunciations per year, and three in four are rejected.[547]

The Standing Committee I's annual report describes in detail the five inquiries initiated by individuals that were concluded in 2014, and mentions those still pending. That same year, the Belgian oversight body received 31 complaints. 28 were rejected because they were ill-founded or the Standing Committee I found that it was not competent.[548] The Snowden revelations triggered four investigations by the Standing Committee I. One of them was founded on a complaint by the president of the Brussels Bar, who wanted to understand how mass surveillance data could be used in the context of criminal proceedings.[549] The Standing Committee I must inform individuals about their investigations' results. According to one Standing Committee I member, the investigation reports always take into account the

545 Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 6 and following.
546 Vande, G. W. (2013), p. 255.
547 *Ibid.*, p. 258.
548 Belgium, Standing Committee I (2015), p. 7 and following.
549 *Ibid.*, p. 40–45.

necessary confidentiality of the intelligence services' operations and the need for transparency.[550]

The Dutch Review Committee (CTIVD) acts as an "independent complaints advisory committee"[551] in the sense that individuals cannot complain directly to the CTIVD. They must first complain to the responsible minister, who then transmits the complaint to the Review Committee. After its investigation, it provides the responsible minister with an advisory opinion on the matter. It is up to the minister to take the final decision, but, if the minister disagrees with the Review Committee's conclusions, the advisory opinion is sent to the complainant. In its annual report covering the period from April 2013 to March 2014, the CTIVD mentioned the 20 complaints handled during that period. Five of them were either partially or fully well-founded. In one of the latter cases, the responsible minister negotiated the allocation of damages with the complainant. The minister followed the committee's opinion in all 20 cases.[552] The annual report covering the period 2014–2015 refers to 10 complaints, of which four were partially or fully well-founded.[553] In the context of some of these complaints, the CTIVD raises the issue of secrecy surrounding the facts included in the CTIVD's opinion; in such cases, the minister decides which information may be provided to the individual. CTIVD stated it would favour declassifying information contributing to better understanding of the working methods of the services, and in particular cases suggested declassifying the information. In some of the cases, the responsible minister did not follow the Review Committee's suggestions.[554]

In Hungary the remedial function is also attributed to the executive oversight body, since the responsible ministers (Interior or Defence) are also responsible for handling individual complaints.

The above-mentioned expert and executive bodies are equipped with relatively wide investigatory powers, which cover direct access to intelligence files. Sweden additionally has the capacity to immediately stop ongoing signals intelligence from the National Defence Radio Establishment, and to decide on the destruction of material if it emerges that the surveillance is being conducted in a manner that contravenes the regulations. The Maltese Commissioner has full authority to scrutinise the services and demand any information on investigations. The Belgian, Danish and German expert bodies have access to classified information, records and the premises of the intelligence services.[555]

In addition to the supervisory role, the DPAs of 13 Member States have the power to hear complaints and issue binding decisions on personal data processing by intelligence services. In three Member States, however, the power to access files and premises is limited. In particular, these investigatory powers are limited in France, Germany and Ireland, if national/state security would be threatened or the files are processed for the purpose of safeguarding state security (Ireland). In five Member States, access is accompanied by enhanced requirements, e.g. the presence of the DPA head (Cyprus, Germany, Greece) or a member of the DPA who has been a member of the Council of State, the Court of Cassation or the Court of Auditors (France), or an officer duly authorised in writing (Germany).

In addition, as shown in the FRA report on *Access to data protection remedies* and in current findings, when data protection violations are caused by a public entity, individuals can seek remedies both via DPAs and via ombudsperson institutions across the EU-28, including in Austria, Belgium, the Czech Republic, Finland, Hungary, Italy, Portugal, Lithuania, the Netherlands, Slovenia and Sweden.[556] However, given their lack of specialisation in data protection issues, they are often not able to provide individuals with expert advice.[557] Furthermore, they usually deal with administrative failures rather than with the actual merits of surveillance, making the complainant's own participation in the process much weaker than in courts.[558] A clear exception to this is the Dutch ombudsperson institution, which has this role directly enshrined in the intelligence law. The powers of ombudsperson institutions can be quite limited, and typically conclude with non-binding recommendations on remedies and guides for future action – such as in Slovenia[559] or Lithuania[560] – rather than a binding, enforceable decision. In Hungary, the ombudsperson institution (Commissioner for Fundamental Rights) both merely has the power to issue non-binding recommendations, and is subject to a law that further restricts its investigatory powers – by excluding specific documents and materials from inspection – when its inquiry affects the national intelligence service.[561]

550 Vande, G. W. (2013), p. 258.
551 The Netherlands, CTIVD (2015), p. 19.
552 The Netherlands, CTIVD (2014), p. 9 and following. So far, the Minister has always followed the Review Committee's advice.
553 The Netherlands, CTIVD (2015), p. 19 and following. The reform currently in discussion would permit CTIVD to handle complaints directly, and grant it binding powers. See also The Netherlands, CTIVD (2015), p. 29.
554 *Ibid.*, pp. 22–23.
555 See Wills, A. *et al.*, Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 145.
556 FRA (2014c), pp. 20 and 34.
557 *Ibid.*, p. 34.
558 Born, H. and Leigh, I. (2005), p. 105.
559 Slovenia, Human Rights Ombudsman Act (*Zakon o varuhu človekovih pravic*), 20 December 1993, Art. 39.
560 Lithuania, Law of the Republic of Lithuania on Intelligence, Art. 23.
561 Hungary, Act CXI of 2011 on the Commissioner for Fundamental Rights (*Az alapvető jogok biztosáról szóló 2011. Évi CXI. törvény*), 26 July 2011, Art. 23.

FRA key findings

According to the applicable international standards, anyone who suspects that he/she is the victim of a privacy or data protection violation has to have the opportunity to seek to remedy the situation. The right to an effective remedy – which allows individuals to seek redress for a violation of their rights – is an essential component of access to justice. A remedy must be 'effective' in practice and in law.

As previous FRA reports on access to data protection remedies and on access to justice show, a number of remedial avenues are available to victims of privacy and data protection violations. Non-judicial bodies play an important remedial role in the area of surveillance, given the practical difficulties with accessing general courts. Non-judicial bodies across the 28 EU Member States include expert (including DPAs), executive and parliamentary bodies, as well as ombudsperson institutions. In some Member States, the number of non-judicial bodies with remedial roles in the area of surveillance is relatively encouraging, but should be viewed in light of the following findings.

The complexity of the remedial landscape does not facilitate the implementation of effective remedies, nor does the amount of data gathered by intelligence services performing SIGINT. Fragmentation and compartmentalisation of different remedial avenues have made it difficult to seek remedies. In fact, the collected data shows that only a limited number of cases challenging surveillance practices have been adjudicated at the national level since the Snowden revelations.

Obligation to inform and the right to access

The right to be notified and to access information is crucial to alert individuals to surveillance measures and to start a remedial action. The European Court of Human Rights (ECtHR) has, however, accepted that these rights can justifiably be limited (see ECtHR, *Klass and Others v. Germany*, No. 5029/71, 6 September 1978). FRA findings show that the secrecy surrounding the work of intelligence services indeed limits these rights. Another factor is the sheer amount of data collected through SIGINT compared with more traditional forms of surveillance.

- In eight Member States, the obligation to inform and the right to access are not provided for at all by law; rules on classified documents or on official secrets apply. In the other 20 Member States, legislation provides for the obligation to inform and the right to access, in some cases within specific timeframes, albeit with restrictions. These restrictions include various grounds, such as national security, national interests or the purpose of the surveillance measure itself.

- Only two Member States have specific provisions on the obligation to inform in the context of signals intelligence: in one, individuals are not informed if the selectors used are not directly attributable to the individual; in the other, the individual is not informed if personal data obtained are immediately deleted after collection and not further processed.

- The oversight bodies of 10 EU Member States, including six national DPAs, review restrictions on the right to be informed and the right to access information by checking whether the invoked national security threat is reasonable, and/or by exercising indirectly the individual's right to access. In the latter case, the bodies assess whether access to the data may be granted or whether the refusal to do so is legitimate, and also scrutinise the lawfulness of the data processing. In one Member State, a court warrant – certifying that notification would jeopardise the investigation or there are other arguments against it – is required.

- Two other Member States do not grant a right of access to information as such. The law, however, provides for a right that produces the same result: an individual may request the oversight body to check whether his/her data are subject to unlawful surveillance.

- In some Member States, the oversight body involved in indirectly exercising an individual's right to request access to data neither confirms nor denies the data processing. The replies are usually limited to stating that the complaint has been handled and/or checked.

Judicial remedies

Every Member State gives individuals the opportunity to complain about privacy violations via the courts, regardless of whether these have occurred due to targeted or signals intelligence. Courts provide an avenue for individuals to complain about interference with their privacy, including challenging supervisory body decisions on their claims of privacy violations.

They also give individuals an opportunity to seek remedies – including in the area of surveillance.

- Past FRA research has, however, identified the judges' lack of specialisation in data protection as a serious obstacle to effectively remedying data protection violations. This finding is relevant for surveillance, where, in addition to the necessary secrecy linked to intelligence, relevant expertise in ICT or in intelligence, for instance, is essential.

- Only two Member States have mitigated the lack of specialisation with respect to remedies by involving judges/tribunals that both have the necessary knowledge at their disposal to decide on (often) technical matters, and are allowed to access secret material.

Non-judicial remedies

Non-judicial options are usually more accessible to individuals than judicial mechanisms because the procedural rules are less strict, bringing complaints is less costly and proceedings are faster. Previous FRA evidence confirms this, in particular in the context of data protection, as more complaints tend to be lodged with national DPAs and only few complainants pursue judicial proceedings. The number of non-judicial bodies – other than DPAs – reportedly operating in the area of data protection is small, however, and many non-judicial bodies only have limited power to offer remedies.

- The oversight bodies (including DPAs) in charge of dealing with complaints are independent institutions in the great majority of Member States.

- Where an executive oversight body has remedial powers, the question of independence arises when it also has the power to warrant surveillance. Parliamentary and expert oversight bodies have more autonomous administrative structures – but autonomy does not guarantee an effective remedy unless also supported by sufficient knowledge. How members of oversight bodies are appointed, and their place in the administrative hierarchy, are also important aspects to consider when assessing a body's independence.

- DPAs in 13 EU Member States have the power to examine individual complaints and issue binding decisions. But in three of these, the power to access files and premises is limited. In five Member States, additional requirements – mandating the presence of the head or a member of the DPA during inspections at intelligence service premises – apply.

- Five out of the seven Member States that entrust their expert oversight bodies (other than DPAs) with specific remedial powers do so by allowing these bodies to issue binding decisions. In two EU Member States, an executive oversight body also has remedial powers. Parliamentary committees in four Member States are entitled to hear individual complaints, but only one can resolve them with binding decisions.

- Ombudsperson institutions, which exist in all 28 EU Member States, mostly deal with administrative failures rather than with the actual merits of surveillance. Only one Member State provides the ombudsperson institution with remedial powers via the relevant intelligence law. In addition, the ombudsperson institutions' powers can be quite limited, and proceedings typically conclude with non-binding recommendations that aim to put matters right and guide future action, rather than with a binding, enforceable judgement. This obviously impacts the effectiveness of the remedies they are able to provide.

- Other elements that can facilitate an individual's access to remedies include more relaxed rules on the evidentiary burden and class actions, as well as effective whistle-blower protection. The Parliamentary Assembly of the Council of Europe considers whistleblowing to be the most effective tool for enforcing the limits placed on surveillance.

Conclusions

This report maps the legal frameworks on surveillance and the relevant safeguards in place to protect privacy and data protection in the 28 EU Member States. The privacy and data protection safeguards illustrate the way other fundamental rights are also guaranteed by Member States' law. The analysis presents the legal framework on both targeted surveillance and signals intelligence in five Member States that have detailed legislation on this surveillance method. The report analyses the legal regimes in place, not their day-to-day implementation. The necessary fieldwork research will be presented in an upcoming FRA report.

In this area of restricted EU competence, the report highlights the great diversity among Members States regarding how intelligence services are organised and perform their essential tasks. The Member States are all bound by minimum international human rights law standards developed by the United Nations, which are of universal application, and which the Union promotes.[562] Likewise, the Council of Europe (including the ECtHR) standards provide a minimum standard. EU law, as interpreted by the CJEU, also has an impact. Given that a limited number of applicable international regulations, aside from existing international human rights law, apply, the role of self-regulatory measures and soft law should be further assessed, as suggested by some authors.[563]

Surveillance measures interfere greatly with individuals' rights, but are secret in nature. Therefore, individuals are bound to rely on a degree of trust in public authorities, which in turn must safeguard his/her fundamental rights. In its case law on secret surveillance, the ECtHR recognises the specificity of the surveillance context by focusing on the legality of the interference and on the safeguards in place.

Clear and accessible legislation, strong oversight mechanisms, proper control mechanisms, as well as effective remedies are only some of the elements essential for the kind of accountability that encourages the level of trust society should have vis-à-vis its intelligence service. Achieving this may undeniably be difficult. The British Reviewer of Terrorism Legislation noted that, due to the secrecy intelligence services operate in, "it cannot be excluded that practices take place which are completely unknown to commentators or which have no legal sanction whatsoever".[564] The difficulty in producing clear and accessible legislation, which is merely the first step in attaining a transparent system, is therefore an obstacle.

How applicable are the ECtHR's standards – mostly developed in the context of targeted surveillance – to signals intelligence? This is the underlining question of this report. Cases dealing with 'mass surveillance', as revealed by Edward Snowden, are pending before the ECtHR.

This report presented various oversight systems chosen by EU Member States. Oversight bodies contribute to a better understanding of how intelligence services work. As stated by the Dutch oversight body, "An overstrong culture of secrecy not only creates scope for unacceptable practices, it may also give rise to myths and misunderstandings. As Snowden's revelations have shown, this may eventually come to work against the intelligence and security services themselves."[565] The work of these bodies also demonstrates that surveillance methods can be controlled if the oversight mechanisms are provided with enough powers and means. Above all, independence and proper means to work are crucial.

Exchanges on practices between actors help clarify and enhance relevant control standards. Despite the great diversity and the predominantly national competences of oversight bodies, exchanges can help promote promising practices. When it comes to exchanges between oversight bodies, already existing networks, such as the European Network of National Intelligence Reviewers (ENNIR),[566] can be fostered. Such exchanges and cooperation should, however, not be limited to oversight bodies. Similar exchanges on the manner in which intelligence services uphold fundamental rights in their work could also be beneficial.

In the context of signals intelligence, oversight solutions vary in the five Member States studied in more detail. The specificity of this surveillance technique presents a particular challenge for oversight bodies in charge of controlling its legality. Legal frameworks do not provide strong powers in the context of SIGINT. As stated by Chesterman,

> *"Most of the structures set up to limit the powers of intelligence agencies tend to assume a model of individualized searches [...]. The move to more systematic surveillance of the entire population requires a different regime. Warrants will still be*

562 See Council of the European Union (2015).
563 See Brown, I. *et al.* (2015) and Laurent, S.-Y., CNCIS (2015a).
564 Anderson, D., Independent Reviewer of Terrorism Legislation (2015), p. 148.
565 The Netherlands, CTIVD (2015), p. 32.
566 See the European network of national Intelligence Reviewers (ENNIR) www.ennir.be/.

> *important for narrowly targeted surveillance or to authorize searches of property, but accountability for systematic surveillance will necessarily be more general".*[567]

It should include detailed reporting, the use of technology to keep track of access to data and what is done with it, clear lines of internal authority, and adequate oversight by the legislature. For Chesterman, the key is to be able to hold the services accountable.[568] The Venice Commission cited the German and Swedish systems as models which could possibly be built upon.[569] However, recent revelations have demonstrated shortcomings in the German control system. Huber, a member of the German oversight body, summarised the challenges as follows:

> *"Effective control of these strategic measures by way of parliamentary bodies or other independent entities in practice proves very difficult, if not impossible.* [Eine effektive Kontrolle dieser strategischen Maßnahmen durch parlamentarische Gremien oder sonstige unabhängige Stellen erweist sich in der Praxis als sehr schwierig, wenn nicht sogar als aussichtslos. – FRA translation]"[570]

The reactions to the Snowden revelations have also underscored the need to adopt and strengthen legal frameworks, and this report shows that a number of legal reforms have been carried out. These, however, should not be limited to reacting to scandals. Periodical assessments of the functioning and legitimacy of the frameworks that govern intelligence service activities must become an integral part of the oversight systems. How can the legal frameworks be further reformed to address the lack of adequate oversight? Reform processes in the EU Member States also need to take technological developments into account, and provide intelligence services and oversight mechanisms with adapted tools. Protecting individuals while also safeguarding fundamental rights is the complex challenge lawmakers need to meet.

567 Chesterman, S. (2011).
568 *Ibid.*
569 Venice Commission (2015). However, commentators have also criticized the German system. See Venice Commission (2015), p. 19 and 34.
570 Huber, B. (2015), p. 4.

References

Access, Electronic Frontier Foundation, and Privacy International (2014), International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), May 1994.

Anderson, D., Independent Reviewer of Terrorism Legislation (2015), *A question of trust: Report of the investigatory powers review*, London, 11 June 2015.

Article 19 (1996), Johannesburg Principles on national security, freedom of expression and access to information, freedom of expression and access to Information, Policy brief, London, 1 November 1996.

Article 29 Working Party (2010), *Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of Art. 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive*, 00058/10/EN, 13 July 2010.

Article 29 Working Party (2014a), Joint statement of the European data protection authorities assembled in the Article 29 Working Party, 26 November 2014

Article 29 Working Party (2014b), Opinion 04/2014 on surveillance of electronic communications of intelligence and national security purposes, 10 April 2014.

Article 29 Working Party (2014c), Working Document on surveillance of electronic communications for intelligence and national security purposes, 5 December 2014.

Austria, Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung*, BVT) (2014), *Verfassungsschutzbericht 2014,* Vienna.

Austria, Federal Agency for State Protection and Counter Terrorism (*Bundesamt für Verfassungsschutz und* Terrorismusbekämpfung, BVT) (2015), *Verfassungsschutzbericht für das Jahr 2014,* Vienna.

Bäcker, M. (2014), Erhebung, Bevorratung und Übermittlung von Telekommunikationsdaten durch die Nachrichtendienste des Bundes. Stelungnahme zur Anhörung des NSA-Untersuchungsauschusses am 22 Mai 2014, position paper submitted to the NSA Committee of Inquiry.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2011), *Rapport d'activités 2010 Activiteitenverslag 20140*, Antwerp and Cambridge, Intersentia.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité - Comité Permanent R*) (2012), *Activity Report 2010 Activity Report 2011 – Investigations, Control of Special Intelligence Methods and Recommendations*, Antwerp and Cambridge, Intersentia.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2014), *Rapport d'activités 2013 Activiteitenverslag 2013*, Antwerp and Cambridge, Intersentia.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2015), *Rapport d'activités 2014 Activiteitenverslag 2014*, Antwerp and Cambridge, Intersentia.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. and Scherrer, A., Policy Department C: Citizens' Rights and Constitutional Affairs (2013), *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, Brussels, European Parliament Directorate-General for Internal Policies.

Bigo, D., Carrera, S., Hernanz, N. and Scherrer, A., Policy Department C: Citizens' Rights and Constitutional Affairs (2014), *National security and secret evidence in legislation and before the courts: Exploring the challenges,* PE 509.991, Brussels, European Parliament Directorate-General for Internal Policies.

Born, H. and Caparini, M. (2007), *Democratic control of intelligence services: Containing rogue elephants*, Hampshire-Burlington, Ashgate Publishing Company.

Born, H., Fluri, P. and Johnsson, A. (eds.), Geneva Centre for the Democratic Control of Armed Forces (DCAF) (2003), *Parliamentary oversight of the security sector: Principles, mechanisms and practices*, Handbook, Geneva.

Born, H. and Leigh, I. (2005), *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*, Oslo, Publishing House of the Parliament of Norway.

Born, H., Leigh, I. and Wills, A. (eds.) (2011), *International intelligence cooperation and accountability*, London and New York, Routledge.

Born, H., Leigh, I. and Wills, A. (2015), *Making international intelligence cooperation accountable*, Geneva, Centre for the Democratic Control of Armed Forces (DCAF).

Born, H., Lock, K. J. and Leigh, I. (eds.) (2005), *Who's watching the spies?: Establishing intelligence service accountability*, Washington, Potomac Books Inc.

Born, H. and Wills, A. (eds.) (2012), *Overseeing intelligence services: A toolkit*, Handbook, Geneva, Centre for the Democratic Control of Armed Forces (DCAF).

Bozhilov, N. (2007), 'Reforming the intelligence services in Bulgaria: The experience of 1989-2005', in: Born, H. and Caparini, M., *Democratic control of intelligence services: Containing rogue elephants*, Hampshire-Burlington, Ashgate Publishing Company.

Brouwer, H. (2014), 'A call for more transparency: A Dutch perspective on large scale intelligence gathering and international cooperation', Speech delivered at the Intelligence Review Agencies Conference, London, 8 July 2014.

Brown, I., Halperin, M., Hayes, B., Scott, B. and Vermeulen, M. (2015), 'Towards multilateral standards for surveillance reforms', Oxford Internet Institute Discussion Paper, January 2015.

Cameron, I. (2000), *National security and the European Convention on Human Rights*, The Hague, Kluwer Law International.

Cameron, I. (2011), 'Annex A-VIII: Parliamentary and specialised oversight of security and intelligence agencies in Sweden', in: Wills, A., Vermeulen, M., Born, H., Scheinin, M., Wiebusch, M. and Thorton, A., Policy Department C: Citizens' Rights and Constitutional Affairs, *Parliamentary oversight of security and intelligence agencies in the European Union*, Brussels, European Parliament Directorate-General for Internal Policies, pp. 278–288.

Cameron, I. (2013), 'Foreseeability and safeguards in the area of security: Some comments on the ECHR case law', in: Van Laethem, W. and Vanderborght, J. (eds.), Vast Comité I, Comité Permanent Contrôle des Services de Renseignements et de Sécutrité, *Inzicht in toezicht: Regards sur le contrôle*, Antwerp and Cambridge, Intersentia, pp. 163–180.

Cate, F. H., Dempsey, J. X. and Rubinstein, I. S. (2012), 'Systematic government access to private-sector data', *International Data Privacy Law*, Vol. 2, No. 4, pp. 195–199.

Cayford, M., van Gulijk, C. and van Gelder, P. H. A. J. M. (2015), 'All swept up: An initial classification of NSA surveillance technology' in: Nowkowski, T., Młyńczak, M., Jodejko-Pietruczuk, A. and Werbińska-Wojciechowska, S. (eds.), *Safety and reliability: Methodology and applications*, London, Taylor & Francis Group, pp. 643–650.

Chesterman, S. (2011), *One nation under surveillance: The new social contract to defend freedom without scarifying liberty*, Oxford, Oxford University Press.

Council of Europe Commissioner for Human Rights (2014), 'The rule of law on the Internet and the wider digital world', Issue paper, Strasbourg, Council of Europe.

Council of Europe Commissioner for Human Rights (2015), 'Democratic and effective oversight of national security services', Issue paper, Strasbourg, Council of Europe.

Council of Europe, Committee of Ministers (2013), Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, 11 June 2013.

Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), 'Freedom of expression and democracy in the digital age: Opportunities, rights, responsibilities', Keynote speech by Nils Muižnieks, Council of Europe Commissioner for Human Rights,CommDH/Speech(2013)12, Belgrade, 7-8 November 2013.

Council of Europe (1981), Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28 January 1981.

Council of Europe (2001), 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, CETS No. 181, 8 November 2001.

Council of the European Union (2015), Council conclusions on the Action Plan on Human Rights and Democracy (2015-2019), Doc. 10897/15, Brussels, 20 July 2015.

Cousseran, J.-C. and Hayez, P. (2015), *Renseigner les démocraties, renseigner en démocratie*, Paris, Odile Jacob.

Croatia, Security and Intelligence Agency (*Sigurnosno-obavještajna agencija)* (2014), Public Report 2014, 31 August 2014.

Delmas-Marty, M. (2015), 'La démocratie dans les bras de Big Brother : Propos recueillis par Johannès, F.', *Le Monde*, 4 June 2015.

de With, H. and Kathmann, E. (2011), 'Annex A-III: Parliamentary and specialised oversight of security and intelligence agencies in Germany' in: Wills, A., Vermeulen, M., Born, H., Scheinin, M., Wiebusch, M. and Thornton, A., Policy Department C: Citizens' Rights and Constitutional Affairs, *Parliamentary oversight of security and intelligence agencies in the European Union*, PE 453.207, Brussels, European Parliament Directorate-General for Internal Policies, pp. 218–229.

Dewost, J.-L., Pelletier, H. and Delarue, J.-M. (2015), 'Vingt-cinq années d'exercice de la CNCIS – Le contrôle des techniques de renseignement', in : CNCIS (2015b), *23e rapport d'activité : Années 2014-2015*, Paris, La documentation française, pp. 11–32.

Dietrich, J.-H. (2015), 'Of toothless windbags, blind guardians and blunt swords: The ongoing controversy about the reform of intelligence services oversight in Germany', Intelligence and National Security', *Intelligence and National Securtiy,* pp. 1–19.

EU Action Plan on Human Rights and Democracy, adopted by the Foreign Affairs Council of 20 July 2015, Council of the European Union (2015), Doc. 10897/15, Brussels, 20 July 2015.

European Commission (2000), Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000/520/EC), C(2000) 2441, 26 July 2000.

European Commission for Democracy through Law (Venice Commission) (2007), *Report on the democratic oversight of the security services,* Study No. 388/2006, Doc. CDL-AD(2007)016, Strasbourg, Council of Europe, 11 June 2007.

European Commission for Democracy through Law (Venice Commission) (2015), *Update of the 2007 report on the democratic oversight of the security services*, Study No. 719/2013, Doc. CDL-AD(2015)006, Strasbourg, Council of Europe, 7 April 2015.

European Commission, FP7-SECURITY, 'Surveillance: Ethical issues, legal limitations, and efficiency', Ref. No. 284725, SURVEILLE project, 1 February 2012 to 30 June 2015.

European Conference of Data Protection Authorities (2014), Resolution on the revision of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), Strasbourg, Council of Europe, 5 June 2014.

European Court of Human Rights: Research Division (2013), *National security and European case-law*, Council of Europe.

European Data Protection Supervisor (EDPS) (2015), *Leading by example: The EDPS strategy 2015-2019*, Brussels.

European Group on Ethics in Science and New Technologies (EGE) (2014), *Ethics of security and surveillance technologies*, Opinion No. 28, Brussels, European Commission, 20 May 2014.

Europol Joint Supervisory Body (2014), *Data protection inspection report: September 2014*, Report No. JSB/Ins.14/41, Brussels, 9 December 2014,

European Network of National Intelligence Reviewers (ENNIR), Intelligence review in Germany, 12 June 2012.

European Parliamentary Research Service (EPRS), Science and Technology Options Assessment (STOA) (2014a), 'Part 1 – Risks and opportunities raised by the current generation of network services and applications' in: Mass Surveillance, PE 527.409, European Parliament.

EPRS, STOA (2014b), 'Part 2 – Technology foresight, options for longer term security and privacy improvements' in: Mass Surveillance, PE 527.410, European Parliament.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013a), *Working document 1 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights*, 11 December 2013.

European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013b), *Working document 5 on democratic oversight of Member State intelligence services and of EU intelligence bodies*, 20 December 2013.

European Parliament, Committee on Petitions (2014), 'Notice to Members: Petition No. 1618/2012 by Jan Douwe Kooistra (Dutch) on the right to protection of personal data', No. 1618/2012, Doc. PE537.416v01-00, 29 August 2014.

European Parliament, Directorate General for Internal Policies (2014), National security and secret evidence in legislation and before the courts: exploring the challenges, Study for the LIBE Committee, 2014.

European Parliament (2001), *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*, A5-0264/2001, 11 July 2001.

European Parliament (2014), *Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))*, P7_TA (2014)0230, 12 March 2014.

Foegle, J.-P. (2015), 'De Washington à Paris, la "protection de carton" des agents secrets lanceurs d'alerte', *Revue des droits de l'homme*, 6 June 2015.

Forcese, C. and LaViolette, N. (2006), Ottawa Principles on Anti-terrorism and Human Rights (2006), Toronto, 1 October 2006.

Forcese, C. (2012), 'Tool 9: Handling complaints about intelligence services', in: Born, H. and Wills, A. (eds.), *Overseeing intelligence services: A toolkit*, Geneva, DCAF, pp. 181–200.

FRA (European Union Agency for Fundamental Rights) (2010), *Data protection in the European Union: The role of national data protection authorities (Strengthening the fundamental rights architecture in the EU II),* Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2011), *Access to justice in Europe: An overview of challenges and opportunities*, Luxembourg, Publications Office.

FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package,* FRA Opinion 2/2012, Vienna, 1 October 2012.

FRA (2014a), *Fundamental rights: Challenges and achievements in 2013 – Annual report,* Luxembourg, Publications Office.

FRA (2014b), 'Ad hoc information request: National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies,' *Franet Guidelines*, Vienna, 18 August 2014.

FRA (2014c), *Access to data protection remedies*, Luxembourg, Publications Office.

FRA (2014d), *Opinion of the European Union Agency for Fundamental Rights on the situation of equality in the European Union 10 years on from initial implementation of the equality directives,* FRA Opinion 1/2013, Vienna, 1 October 2013.

FRA (2015), *Fundamental rights: Challenges and achievements in 2014 – Annual report*, Luxembourg, Publications Office.

France, National Commission for the Control of Security Interceptions (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS) (2015a), *22e rapport d'activité : Années 2013-2014*, Paris, La documentation française.

France, National Commission for the Control of Security Interceptions (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS) (2015b), *23e rapport d'activité : Années 2014-2015*, Paris, La documentation française.

France, National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés*, CNIL) (2015), *Rapport d'activité 2014*, Paris, La documentation française.

France, Urvoas, J.-J., Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement*) (2014), *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014* (Annual Report 2014), Doc. No. 2482 (Assemblée nationale), Doc. No. 201 (Sénat), Assemblée Nationale and Sénat, 18 December 2014.

French Data Network (*Réseau de données français*), La Quadrature du Net and Fédération des fournisseurs d'accès à Internet associatifs (2015), *Amicus Curiae transmis au Conseil constitutionnel dans le cadre des saisines visant la « loi relatif au renseignement »*.

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit*) (2013), *Activity report on data protection for the years 2011 and 2012.*

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit)* (2015), *Activity report on data protection for the years 2013 and 2014*.

Germany, Federal Parliament (*Deutscher Bundestag*) (2013), *Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2011 bis Oktober 2013)*, Drucksache No. 18/217, 19 December 2013.

Germany, Federal Parliament (*Deutscher Bundestag*) (2015), *Bericht gemäß § 14 Absatz 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Article 10-Gesetz-G 10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5, 7a und 8 dieses (Berichtszeitraum 1. Januar bis 31. Dezember 2013),* Drucksache No. 17/12773, 14 March 2013.

Germany, Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK), 88th, (2014), *Entschließung: Effektive Kontrolle von Nachrichtendiensten herstellen!,* Hamburg, 8-9 October 2014.

Greece, Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*), Annual reports for the years 2004–2014.

Heumann, S. and Wetzling, T., Stiftung neue Verantwortung (2014), 'Strategische Auslandsüberwachung: Technische Möglichkeiten, rechtlicher Rahmen und parlamentarische Kontrolle', *Europäische Digitale Agenda: Privacy Project*, May 2014.

Hoffmann-Riem, W. (2014), *Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 22 Mai 2014*, position paper submitted to the NSA Committee of Inquiry.

Huber, B. (2013), 'Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite', *Neue Juristische Wochenzeitschrift*, Vol. 32, No. 35, pp. 2572–2577.

Huber, B. (2015), 'Von der Überwachung einzelner Personen zur umfassenden strategischen Rasterfahndung', Paper delivered at the Conference on the Democratic oversight of Intelligence services in the European Union, Brussels, European Parliament, 28-29 May 2015, pp. 1-6.

Hustinx, P. (2014), 'EU data protection law: The review of Directive 95/46/EC and the proposed general data protection regulation'.

Institute for Information Law (2015), *Ten standards for oversight and transparency of national intelligence services*, Amsterdam, University of Amsterdam.

International Conference of Data Protection and Privacy Commissioners, 31st, (2009), *Resolution: International Standards on the Protection of Personal Data and Privacy,* Madrid, 4-6 November 2009.

International Conference of Data Protection and Privacy Commissioners, 36th, (2014), *Resolution: Privacy in the digital age,* Balaclava Fort, 13-16 October 2014.

Italy, Italian Government (*Governo italiano*) (2013), 'Sicurezza dati personali: Protocollo d'intenti tra l'Autorità Garante e il Direttore Generale del Dis', Press release, 11 November 2013.

Italy, Parliamentary Committee for the Security of the Republic (*Comitato parlamentare per la sicurezza della Repubblica*, COPASIR) (2014), *Relazione annuale (Attività svolta dal 6 giugno 2013 al 30 settembre 2014)*, Doc. XXXIV No.1, Senate of the Republic (*Senato della Repubblica*), Chamber of Deputies (*Camera dei Deputati*), 11 December 2014.

Klamberg, M. (2009), *FRA:s signalspaning ur ett rättsligt perspektiv* (FRA's signals intelligence from a legal perspective), SvJT 2009, Juridicum.

Klamberg, M. (2010), 'FRA and the European Convention on Human Rights: A paradigm shift in Swedish electronic surveillance law' (published as *'Övervåking i en Rettsstat'*), in: Schartum, D. W. (ed.), *Nordisk årbok i rettsinformatikk (Nordic Yearbook of Law and Information Technology),* Bergen, Fagbokforlaget, pp. 96–134.

Krempl, S. (2015), 'NSA-Ausschuss: Peter Schaar sieht große Lücken bei BND-Kontrolle', *Heise Online*, 16 January 2015.

La Quadrature du net (2015), 'Three French NGOs challenge French international surveillance', Press release, 3 September 2015.

Laurent, S.-Y. (2014), *Atlas du Renseignement*, Condé-sur-Noireau, Presses de Sciences Po.

Laurent, S.-Y., 'Liberté et sécurité dans un monde anomique de données', in: Commission nationale de contrôle des interceptions de sécurité (CNCIS) (2015), *22e rapport d'activité: Années 2013-2014*, Paris, La documentation française.

Leigh, I. (2013), 'A view across the channel: Intelligence oversight in the United Kingdom', in : Van Laethem, W. and Vanderbroght, J. (eds.), Vast Comité I, Comité Permanent Contrôle des Services de Renseignements et de Sécutrité, *Inzicht in toezicht: Twintig jaar democratische controle op de inlichtingendiensten – Regards sur le contrôle: Vingt ans de contrôle démocratique sur les services de renseignement*, Antwerp and Cambridge, Intersentia, pp. 431–441.

Löning, M., Stiftung neue Verantwortung (2015), 'Eine Reformagenda für die deutschen Geheimdienste: Rechtstaatlich, demokratisch, effektiv', *Europäische Digitale Agenda: Privacy Project*, Impulse, 15 April 2015.

Lowenthal, M. (2015), *Intelligence: From secrets to policy* (6th ed.), Thousand Oakes and London, CQ Press and Sage Publications.

Omand, D. (2015), 'Understanding digital intelligence and the norms that might govern it', *Global Commission on Internet Governance Paper Series*, Paper No. 8, Waterloo and London, Centre for international Governance Innovation and Chatham House, 19 March 2015.

Open Society Justice Initiative (2013), Global Principles on National Security and the Right to Information (Tshwane Principles), Tshwane, South Africa, 12 June 2013.

Parliamentary Assembly of the Council of Europe (PACE) (1999), 'Control of internal security services in the Council of Europe Member States', Report Doc. 8301, 23 March 1999. PACE, Committee on Legal Affairs and Human Rights (2015a), *Improving the protection of whistleblowers*, Report Doc. 13791, Strasbourg, 6 June 2015.

PACE, Committee on Legal Affairs and Human Rights (2015b), *Mass surveillance*, Report Doc. 13734, Strasbourg, 21 April 2015.

Peers, S. (2013), The extent of national competence as regards internal security, Response to European Parliament inquiry, 18 November 2013.

Phythian, M. (2009), 'The British intelligence services', in: Jäger, T. and Daun, A., *Geheimdienste in Europa: Transformation, Kooperation und Kontrolle,* Heidelberg, VS Verlage, pp. 13–34.

Poland, Helsinki Foundation for Human Rights (2015), 'PAC: statistical data on ISA's covert investigative methods still unavailable', Newsletter, 24 June to 1 July 2015.

Poland, Supreme Audit Office (*Naczelna Izba Kontroli*) (2014), 'Nadzór nad służbami specjalnymi', Press release, 26 August 2014.

Poland, The Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego*, ABW) (2010), *Annual Report 2009,* Warsaw.

Raab, C., Hallinan, D., Amicelle, A., Clavell, G. G., Galetta,A., De Hert, P. and Jones, R. (2015), 'Effects of surveillance on civil liberties and fundamental rights in Europe', in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, London and New York, Routledge, pp. 259–318.

Schaar, P. (2014), *Überwachung total: Wie wir in Zukunft unsere Daten schützen*, Berlin, Aufbau Verlag.

Schätz, A. (2007), 'Nachrichtendienste im Transformationsprozess?', *Österreichische Militärische Zeitschrift*, 4/2007, p. 397.

Schaus, A. (2014), 'Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec

la Belgique', in : *Rapport d'activités 2013*, Comité permanent de contrôle des services de renseignements et de sécurité (Comité Permanent R) and Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), Antwerp and Cambridge, Intersentia, pp. 188–212.

Schenke, W.-R., Graulich, K. and Ruthig, J. (2014), *Sicherheitsrecht des Bundes*, Munich, Beck.

Schwartz, P. (2012), 'Systematic government access to private-sector data in Germany', *International Data Privacy Law*, Vol. 2, No. 4, pp. 289–301.Sule, S. (2006), *Spionage: Völkerrechtliche, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtäaftsspionage*, Baden-Baden, Nomos Verlag.

Sweden, Swedish Data Inspection Board (*Datainspektionen*), Data Inspection report of the government commission (*Datainspektionens redovisning av regeringsuppdraget*), Fö2009/355/SUND, 6 December 2010.

Sweden, Ministry of Justice (*Justitiedepartementet*) (2012), *En tydligare organisation för Säkerhetspolisen* (A clearer organization of the Security Service), No. SOU 2012:77, 28 November 2012.

The Guardian (2013), 'Clapper admits secret NSA surveillance program to access user data', 7 June 2013.

The Netherlands, Ministry of the Interior and Kingdom Relations (2014), 'Constitution to extend protection to e-mails', Press release, 11 July 2014.

The Netherlands, Review Committee for the Intelligence and Security Services (CTIVD) (2010), *Annual Report 2009-2010*, The Hague, 31 March 2010.

The Netherlands, CTIVD (2014a), *Annual Report 2013-2014*, The Hague, 31 March 2014.

The Netherlands, CTIVD (2014b), *Review Report on investigative activities of AIVD on social media*, No. 39, The Hague, 16 July 2014.

The Netherlands, CTIVD (2015), *Annual Report 2014-2015*, The Hague, 9 June 2015.

United Kingdom, House of Commons Library (2013), Intelligence and Security Committee, Standard Note SN/HA/2178.

United Kingdom, Information Commissioner's Office (2014), *The Information Commissioner's submission to the Intelligence and Security Committee of Parliament: Privacy and security inquiry*, 31 January 2014.

United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2013), 'Statement on GCHQ's alleged interception of communications under the US PRISM programme', 17 July 2013.

United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), *Privacy and security: A modern and transparent legal framework*, London, 12 March 2015, London, June 2015.

United Kingdom, Intelligence Services Commissioner (2015), *Report of the intelligence services commissioner (covering the period of January to December 2014)*, No. HC 225 SG/2015/74, London, June 2015.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2015), *Report of the interception of communications commissioner (covering the period January to December 2014)*, No. HC 1113 SG/2015/28, London, March 2015.

United Kingdom, IPT (2010), *Investigatory Powers Tribunal 2010 report*.

UN (United Nations), General Assembly (GA) (2014a), Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age, A/RES/68/167, 21 January 2014.

UN, GA (2014b) Resolution on the Right to Privacy in the digital age, Doc. A/RES/69/166, 18 December 2014.

UN, GA (2014c), The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, Doc. A/69/276, 7 August 2014.

UN, Human Rights Committee (2014), Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23 April 2014.

UN, Human Rights Committee (2015a), Concluding observations on the fifth periodic report of France, CCPR/C/FRA/CO/5, 21 July 2015.

UN, Human Rights Committee (2015b), Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, CCPR/C/GBR/CO/7, 21 July 2015.

UN, Human Rights Committee (2015c), Concluding observations on the sixth periodic report of Sweden, CCPR/C/SWE/CO/6, 7 May 2009.

UN, Human Rights Council, Emmerson, B. (2014), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Doc. A/69/397, 23 September 2014.

UN, Human Rights Council, Kaye, D. (2015), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye: Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to develop*, Doc. A/HRC/29/32, 22 May 2015.

UN, Human Rights Council (2015), Resolution on the right to privacy in the digital age, Doc. A/HRC/RES/28/16, 30 March 2015.

UN, Human Rights Council, Scheinin, M. (2009), *Report of the Special Rapporteur on the promotion and protection*

of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, Doc. A/HRC/10/3, 4 February 2009.

UN, Human Rights Council, Scheinin, M. (2010), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, Doc. A/HRC/14/46, 17 May 2010.

UN, Office of the High Commissioner for Human Rights (OHCHR) (2014), *The right to privacy in the digital age,* A/HRC/27/37, 30 June 2014.

UN, Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE), Representative on Freedom of the Media, the Organization of American States (OAS), the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information (2015), 'Joint declaration on freedom of expression and responses to conflict situations', Statement, 4 May 2015.

United States, National Research Council (2015), *Bulk collection of signals intelligence: Technical options*, Washington, The National Academies Press.

United States, The White House (2014), 'Presidential policy directive – Signals intelligence activities', Directive No. PPD-28, Office of the Press Secretary, 17 January 2014.

Urvoas, J.-J. (2015), 'Contrôler les services, la juste place du Parlement', in : CNCIS (2015b), *23e rapport d'activité : Années 2014-2015*, Paris, La documentation française, pp. 33–42.

Vande, G. W. (2013), 'Le traitement des plaintes et des dénonciations: Une mission distincte pour le Comité ?', in: Van Laethem, W. and Vanderbroght, J. (eds.), Vast Comité I, Comité Permanent Contrôle des Services de Renseignements et de Sécutrité, *Inzicht in toezicht – Regards sur le contrôle*, Antwerp and Cambridge, Intersentia, pp. 253–267.

Vermeulen, M. (2014), 'Les révélations de Snowden, interception massive de données et espionnage politique', in : *Rapport d'activités 2013*, Comité permanent de contrôle des services de renseignements et de sécurité (Comité Permanent R) and Belgian Standing Intelligence Agencies Review Committee (Standing Committee I), Antwerpen and Cambridge, Intersentia, pp. 143–187.

Wills, A., Vermeulen, M., Born, H., Scheinin, M., Wiebusch, M. and Thornton, A., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), *Parliamentary oversight of security and intelligence agencies in the European Union*, PE 453.207, Brussels, European Parliament Directorate-General for Internal Policies.

Wright, D. and Kreissl, R. (2015), 'European responses to the Snowden revelations', in: Wright, D. and Kreissl, R. (eds.), *Surveillance in Europe*, London and New York, Routledge, pp. 6–50.

Case law index

Case law of the Court of Justice of the European Union

Case law of the European Court of Human Rights

Case law of national courts

Legal instruments index

Council of Europe

European Union

National legislation

Annex: Overview of security and intelligence services in the EU-28

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
AT	Federal Agency for State Protection and Counter Terrorism/ *Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (BVT) (part of the police)			Military Intelligence Service/ *Heeresnachrichtenamt* (HNA) Military Defence Agency/ *Heeresabwehramt* (HAA)
BE	State Security/ *Staatsveiligheid /Sûreté de l'Etat* (SV/SE)			General Intelligence and Security Service of the armed forces/ *Algemene Dienst Inlichting en Veiligheid/ Service général du renseignement et de la sécurité des Forces armées* (ADIV/SGR or SGRS)
BG	State Agency for National Security / *Държавна Агенция "Национална сигурност* (SANS) State agency "Technical operations" / *Държавна агенция „Технически операции* (SATO)			Military information service
CY	Central Intelligence Service/ *Κεντρική Υπηρεσία Πληροφορικών* (ΚΥΠ)			
CZ	Security Information Service/*Bezpečnostní informační služba* (BIS)	Office for Foreign Relations and Information/*Úřad pro zahraniční styky a informace* (ÚZSI)		Military Intelligence / *Vojenské zpravodajství* (VZ)
DE	Federal Office for the protection of the Constitution/ *Bundesamt für Verfassungsschutz* (BfV)		Federal Intelligence Service/ *Bundesnachrichtendienst* (BND)	Military Counter-Intelligence Service/*Militärischer Abschirmdienst* (MAD)
DK			Danish Security and Intelligence Service/*Politiets Efterretningstjeneste* (PET) (part of the police)	Danish Defence Intelligence Service/*Forsvarets Efterretningstjeneste* (FE)
EE	Estonian Internal Security Service/ *Kaitsepolitseiamet (KAPO)*	Information Board/ *Teabeamet (TA)*		Military Intelligence Branch of the Estonian Defense Forces/*Kaitseväe peastaabi luureosakond*
EL	National Intelligence Service/ *Εθνική Υπηρεσία Πληροφοριών* (ΕΥΡ)			Directorate of Military Intelligence of the National Defence General Staff/ *Διεύθυνση Στρατιωτικών Πληροφοριών του Γενικού Επιτελείου Εθνικής Άμυνας*
ES	National Center for the Protection of Critical Infrastructures /*Centro Nacional de Protección de Infraestructuras Críticas* (CNPIC)		National Intelligence Centre/*Centro Nacional de Inteligencia* (CNI) Intelligence Centre on Organised Crime and Terrorism/ *Centro de Inteligencia Contra el Terrorismo y el Crimen Organizado* (CITCO)	Intelligence Centre of the Armed Forces/ *Centro de Inteligencia de las Fuerzas Armadas* (CIFAS)

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
FI	Finnish Security Intelligence Service/*Suojelupoliisi/ Skyddspolisen* (SUPO) (service belonging to the police)			Finnish Defence Intelligence Agency/ *Tiedustelulaitos/ underrättelsetjänst* (FDIA)
FR	Directorate General of Interior Security/ *Direction générale de la sécurité intérieure* (DGSI)	Directorate General of External Security/ *Direction de la sécurité extérieure* (DGSE)		Directorate of Military Intelligence/ *Direction du renseignement militaire* (DRM)
HR	Security Intelligence Agency/ *Sigurnosno-obavještajna agencija* (SOA)			Military Security Intelligence Agency/*Vojna sigurnosno-obavještajna agencija* (VSOA)
HU	Constitution Protection Office/ *Alkotmányvédelmi Hivatal* Special Service for National Security/ *Nemzetbiztonsági Szakszolgálat* (NBSZ) Counter Terrorism Centre/ *Terrorelhárítási Központ* (TEK) (service belonging to the police)		Information Office/ *Információs Hivatal* (MKIH)	Military National Security Service/ *Katonai Nemzetbiztonsági Szolgálat* (KFH)
IE	(Garda Síochána National Surveillance Unit (NSU) – belonging to the police)			Directorate of Intelligence (G2)
IT	Information and Internal Security Agency/ *Agenzia informazioni e sicurezza interna* (AISI)	Information and External Security Agency/*Agenzia informazioni e sicurezza esterna* (AISE)		Department information and security/*Reparto informazioni e sicurezza* (RIS)
LT			State Security Department/ *Valstybės Saugumo Departamentas* (VSD)	Second Investigation Department under the Ministry of National Defence /*Antrasis operatyvinių tarnybų departamentas prie Krašto apsaugos ministerijos* (AOTD prie KAM)
LU			State Intelligence Service/ *Service de renseignement de l'état* (SREL)	
LV	Security Police/ *Drošības policija*	Constitutional Protection Bureau/ *Satversmes aizsardzības birojs* (SAB)		Military Intelligence and Security Service/ *Militārās izlūkošanas un drošības dienests* (MISS)
MT			Security Service	
NL			General Intelligence and Security Service/ *Algemene Inlichtingen- en Veiligheidsdienst* (AIVD)	Military Intelligence and Security Service/ *Militaire Inlichtingen- en Veiligheidsdienst* (MIVD)
PL	Internal Security Agency/ *Agencja Bezpieczeństwa Wewnętrznego* (ABW) Central Anti-Corruption Bureau/*Centralne Biuro Antykorupcyjne* (CBA)	Foreign Intelligence Agency /*Agencja Wywiadu* (AW)		Military Counter-intelligence Service/*Służba Kontrwywiadu Wojskowego* (SKW) Military Intelligence Service/*Służba Wywiadu Wojskowego* (SWW)
PT			Service of Security Intelligence/ *Serviço de Informações de Segurança* (SIS)	Service of Strategic Intelligence and Defense/ *Serviço de Informações Estratégicas e de Defesa* (SIED)

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
RO	Romanian Intelligence Service/ *Serviciul Roman de Informatii* (SRI) Department for Information and Internal Protection/ *Departamentul de Informații și Protecție Internă* (DIPI)	External Intelligence Service/ *Serviciul de Informații Externe* (SIE)		Defense General Directorate for Information/ *Direcția Generală de Informații a Apărării* (DGIA)
SE	Security Service/ *Säkerhetspolisen,* (SÄPO)		Defence Radio Establishment/ *Försvarets Radio Anstalt* (FRA)	Military Intelligence Agency/*Militära underrättelsetjänsten* (MUST)
SI			Slovene Intelligence and Security Agency/ *Slovenska obveščevalno-varnostna agencija* (SOVA)	Intelligence and Security Service of the Ministry of Defence/ *Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo* (OVS MORS)
SK	National Security Authority/ *Národný bezpečnostný úrad* (NBÚ)		Slovak Information Service/*Slovenská informačná služba* (SIS)	Millitary Intelligence/ *Vojenské spravodajstvo* (VS)
UK	British Security Service (BSS) or MI5	Secret Intelligence Service (SIS) or MI6 Government Communications Headquarters (GCHQ)		Defence Intelligence (DI)

A summary of the report's key findings is available on the FRA website at http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services-summary.
The summary will be available in all EU languages as of January 2016.

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

doi:10.2811/009038 TK-04-16-020-EN-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

Protecting the public from security threats and safeguarding fundamental rights involves a delicate balance. Brutal terror attacks and technological innovations making possible large-scale communications data monitoring have further complicated the matter, triggering concerns about violations of the rights to privacy and data protection in the name of national security protection. The Snowden revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, made clear that enhanced safeguards of these rights are needed.

This report, drafted in response to the European Parliament's call for thorough research on fundamental rights protection in the context of surveillance, maps and analyses the legal frameworks on surveillance in place in EU Member States. Focusing on so-called 'mass surveillance', it also details oversight mechanisms introduced across the EU, outlines the work of entities tasked with overseeing surveillance efforts, and presents the remedies available to individuals seeking to challenge such intelligence activity. By demonstrating the complex considerations involved, this report underscores how difficult it can be to address what are often seen as competing priorities, and contributes to the continuing debate on how to best reconcile them.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 158030-0 – Fax +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office
doi:10.2811/009038
ISBN 978-92-9491-224-4