FREEDOMS

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

Volume II: field perspectives and legal update

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.

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

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

Luxembourg: Publications Office of the European Union, 2017

FRA – print:	ISBN 978-92-9491-766-9	doi:10.2811/15232	TK-04-17-696-EN-C
FRA – web:	ISBN 978-92-9491-765-2	doi:10.2811/792946	TK-04-17-696-EN-N

Printed by Imprimerie Centrale in Luxembourg

Printed on process chlorine-free recycled paper (PCF)

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

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

Volume II: field perspectives and legal update

Foreword

Intelligence services perform vital work, and the growing threats of terrorism, cyber-attacks and sophisticated criminal networks have rendered more urgent their efforts to protect our security. Technological advancements have also made their work more complex, and the transnational nature of today's threats has made it ever more challenging.

But intelligence work to counter these threats, particularly large-scale surveillance, can also interfere with fundamental rights, especially privacy and data protection. As this report underscores, effective oversight and remedies can help minimise the risk of such interference.

The report is the second publication addressing a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including its oversight.

With technological advances constantly introducing both new threats and new ways to fight those threats, legislators have been kept busy. Many of the legislative changes enacted since 2015 have increased transparency. But legal frameworks remain diverse and, according to some interviewees, too complex and imprecise. Moreover, while safeguards have in some cases been strengthened, room for improvement remains – particularly in the context of international intelligence cooperation. Similarly, remedies are available where individuals' rights have been infringed, but remain inherently limited.

Clarifying the applicable legal requirements, introducing solid safeguards and giving teeth to remedies would all help ensure that intelligence work is conducted in a rights-compliant manner. This, in turn, would reinforce the credibility of the information obtained by intelligence services – bolstering trust amongst the public, encouraging effective cooperation, and – ultimately – strengthening national security.

We are extremely grateful to the key partners and individual experts who took the time to participate in our interviews, providing invaluable real-life perspectives on the continuing effort to protect fundamental rights and national security.

Michael O'Flaherty
Director

Country codes

Country code	Country
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

Acronyms and abbreviations

Acronym/ abbreviation	Name	English translation
AIVD	Algemene Inlichtingen en Veiligheidsdienst	General Intelligence and Security Service (the Netherlands)
BND	Bundesnachrichtendienst	Federal Intelligence Service (Germany)
BNDG	Bundesnachrichtendienst Gesetz	Law on the Federal Intelligence Service (Germany)
CIVD	German Federal Intelligence Service	
CJEU	Court of Justice of the European Union	
CNCTR	Commission nationale de contrôle des services de renseignement	National Commission of Control of the Intelligence Techniques (France)
CNIL	Commission nationale de l'informatique et des libertés	French Data Protection Authority
COPASIR	Comitato parlamentare per la sicurezza della Repubblica	Parliamentary Committee for the Intelligence and Security Services and for State Secret Control (Italy)
CTIVD	De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten	Oversight Committee for the Intelligence and Security Services (the Netherlands)
DGSE	Direction générale de la sécurité extérieure	General Directorate for External Security (France)
DPA	Data Protection Authority	
ECHR	European Convention on Human Rights	
ECtHR	European Court of Human Rights	
FDN	French Data Network	
GCHQ	Government Communications Headquarters	
GDPR	General Data Protection Regulation	
GISS	General Intelligence and Security Service (Belgium)	
IOCCO	Interception of Communications Commissioners Office	
IPA	Investigatory Powers Act	
IPC	Investigatory Powers Commissioner	
IPT	Investigatory Powers Tribunal	
ISC	Internet Systems Consortium	
NCND	Neither confirm nor deny	
OCAM	Coordination Unit for Threat Analysis	
PKGr	Parlamentarisches Kontrollgremium	Parliamentary Control Panel (Germany)
PKGrG	Parlamentarisches Kontrollgremium Gesetz	Parliamentary Control Panel Act (Germany)
PNR	Passenger Name Records	
QPC	Question prioritaire de constitutionnalité	Priority preliminary ruling on the issue of constitutionality (France)
RIPA	Regulation of Investigatory Powers Act 2000	
SIGINT	Signals Intelligence	
SIN	Commission on Security and Integrity Protection	
SIS	Secret Intelligence Service	
SIUN	Statens Inspektion för försvarsunderrättelseverksamheten	The State Inspection for Defence Intelligence Operations (Sweden)
SSEUR	Signals Intelligence Seniors Europe	
TET	Tilsynet med Efterretningstjenesterne	Danish Intelligence Oversight Board

Contents

Figures and tables

Executive summary

With terrorism, cyber-attacks and organised crime posing growing threats across the European Union, the work of intelligence services undoubtedly remains vital. Technological advancements have introduced both new threats and means of fighting those threats, meaning such work has also become increasingly complex. In addition, the globalisation of conflicts and the transnational nature of threats faced have made international cooperation between intelligence services both more common and indispensable – within and beyond the EU's borders.

Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communications and metadata to hacking and database mining. But – as the 2013 Snowden revelations underscored – these activities may also seriously interfere with diverse fundamental rights, particularly to privacy and data protection.

This report constitutes the second part of a research effort triggered by a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis (*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks)*. In addition, it presents findings from over 70 interviews with experts – conducted largely in 2016 – in seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom. The report focuses on large-scale technical collection of intelligence, referred to as general surveillance of communications.

Intelligence laws remain diverse and complex

Much has happened since 2015. New threats and new technology have triggered extensive reforms across several Member States, particularly France, Germany, the Netherlands and the United Kingdom, and Finland is in the midst of an overarching reform.

These intelligence law reforms have increased transparency. Nonetheless, the legal frameworks regulating intelligence work in the EU's 28 Member States remain both extremely diverse and complex. International human rights standards require defining the mandate and powers of intelligence services in legislation that is clear, foreseeable and accessible. But experts voiced concerns about a persisting lack of clarity as a major source of uncertainty.

According to both European Convention of Human Rights (ECHR) and EU law, the mere existence of legislation allowing for surveillance measures constitutes an interference with the right to private life, and European courts consider the collection of data by intelligence services to amount to an interference. Such interference needs to be justified to be human rights compliant.

Targeted surveillance – which applies to concrete targets based on some form of individualised suspicion – is regulated in some detail by almost all EU Member States. By contrast, only five Member States currently have detailed legislation on general surveillance of communications. Safeguards do limit the potential for abuse, and these have been strengthened in some Member States – though less so in case of foreign-focused surveillance. Similarly, safeguards are generally weaker – and less transparent – in the context of international intelligence cooperation, suggesting a need for more regulation of such cooperation.

Oversight bodies ensure some accountability, but room for improvement remains

Various entities oversee the work of intelligence services across the EU-28, including the judiciary, expert bodies, parliamentary committees and data protection authorities. In a field dominated by secrecy, such oversight is crucial: it helps ensure that intelligence services are held accountable for their actions, and encourages the development of effective internal safeguards within the services.

The judiciary and expert bodies are most commonly involved in overseeing surveillance measures. Specialised parliamentary committees generally focus on assessing governmental strategic policies – 21 Member States have set up such committees for this purpose. Data protection authorities have significant powers over intelligence services in seven Member States, but their powers are limited or non-existent in the rest of the EU – mainly due to an exception for national security matters enshrined in data protection law.

Almost all interviewees from oversight bodies maintained that they are able to resist external influence, but some lawyers, civil society, and academics questioned both their independence and their effectiveness. Interviewed experts emphasised that full access to all relevant data and information is key to effective oversight – as is the ability to benefit from such access. With oversight bodies largely staffed by legal specialists, the inability to do so sometimes boils down to limited technical capacities. Interviewees

acknowledged that these pose a problem – and that the sensitivity of the work can discourage individuals from seeking external expertise.

The power to issue binding decisions is also vital. While all EU Member States have at least one independent body in their oversight framework, some lack such decision-making powers. The importance of public scrutiny was also highlighted, with some interviewees deeming insufficiently informative the reports issued by oversight bodies. In addition, the respondents underlined the importance of countering the fragmentation of oversight through cooperation among the various actors involved in the oversight process, both nationally and internationally.

FRA's research revealed that oversight of international intelligence cooperation is less fully developed – 17 Member States do not require oversight of such activity, while others limited its scope. Some Member States have introduced safeguards specifically tailored to international intelligence sharing, but only requiring prior approval from the executive has been embraced in significant numbers (27 Member States).

Towards accessible and effective remedies

The need for secrecy in the intelligence field can affect both the effectiveness of oversight and individuals' abilities to seek remedies for violations. While the right to seek remedy is not absent in the context of secret surveillance, it is inherently limited. Interviewed experts indicated that individual remedial bodies receive about 10 to 20 complaints a year.

Non-judicial remedies are generally more accessible than judicial mechanisms because they are cheaper, faster and involve less strict procedural rules. Twenty-five Member States do allow individuals to lodge complaints regarding surveillance with such bodies. To be effective, remedial bodies also require certain powers – specifically, to access classified information and issue binding decisions. Expert bodies or data protection authorities have such powers in most Member States.

Nonetheless, lawyers, civil society representatives and academics consulted during FRA's research tended to question the effectiveness of existing remedies. They noted that few individuals are even aware that remedies are available. In addition, the rights to access information on individual files and to be notified about surveillance are not consistently implemented. Both of these can be curtailed based on various grounds linked to national security.

The lack of expertise in dealing with secrecy and with technical matters is also an issue, both with judicial and non-judicial actors. In the judicial context, Member States have found several ways to address this issue, including by developing alternative adversarial procedures to allow for the use of classified information; creating cooperation mechanisms, including with intelligence services, to tackle the lack of expertise; and establishing quasi-judicial bodies.

Such solutions underline that hurdles to obtaining effective remedies can be overcome. Similarly, establishing truly clear legal frameworks, developing appropriate safeguards, and ensuring potent oversight is feasible – and the best way to ensure that enhanced security measures made possible by surveillance fully comply with fundamental rights.

FRA opinions

Providing for a clear legal framework

Intelligence services help protect national security. To do this successfully, they often need to work in secrecy. However, international and European human rights standards require the mandate and powers of intelligence services to be clearly defined in a legal framework, and for this framework to establish safeguards against arbitrary action to counterbalance secrecy. The European Court of Human Rights (ECtHR) has held that national legal frameworks must be clear, accessible and foreseeable. It obliges Member States to enshrine minimum safeguards in law, such as specifying the nature of offences that may lead to interception orders and defining the categories of people who may be put under surveillance. FRA's fieldwork shows that surveillance legislation is considered complex and that a clearer legal framework with meaningful definitions is needed.

FRA opinion 1

EU Member States should have clear, specific and comprehensive intelligence laws. National legal frameworks should be as detailed as possible on intelligence services' mandates and powers, and on the surveillance measures they can use. Fundamental rights safeguards should feature prominently in intelligence laws, with privacy and data protection guarantees for collecting, retaining, disseminating and accessing data.

Ensuring broad consultation and openness during the legislative process

The preparation of intelligence legislation should involve an open debate among key stakeholders. During discussions on draft intelligence laws, governments should take the time to clarify the needs of intelligence services and to explain which fundamental rights guarantees the bill has established. FRA data show that most EU Member States have reformed their intelligence and counter-terrorism legislation in recent years. Some of these legislative processes unfolded during FRA's fieldwork. The interviewed experts emphasised the need for a broader inclusion of key actors and stakeholders in the development of intelligence legislation. In some Member States, online public consultations and lively parliamentary discussions are taking place instead of new legislation being fast-tracked. FRA's *Fundamental Rights Report 2017* underlined the need for such an approach.

FRA opinion 2

EU Member States should undertake broad public consultations with a full range of stakeholders, ensure transparency of the legislative process, and incorporate relevant international and European standards and safeguards when introducing reforms to their legislation on surveillance.

Providing independent intelligence oversight with sufficient powers and competences

Setting up a strong oversight mechanism is an essential part of an intelligence accountability system. The oversight framework should reflect the powers of the intelligence services. European Court of Human Rights case law provides that oversight bodies should be independent and have adequate powers and competences. FRA's research findings show that all EU Member States have at least one independent body in their oversight framework. However, the findings also identified limits to full independence, with some oversight bodies remaining strongly dependent on the executive: the law does not grant them binding decision-making powers, they have limited staff and budget, or their offices are located in government buildings.

FRA opinion 3

EU Member States should establish a robust oversight framework adequate to the powers and capacities that intelligence services have. The independence of oversight bodies should be enshrined in law and applied in practice. EU Member States should grant oversight bodies adequate financial and human resources, including diverse and technically-qualified professionals. Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate. Member States should ensure that the oversight bodies' decisions are binding.

Bolstering oversight with sufficient technical expertise

Particularly in light of rapidly evolving technology in the digital area, technical expertise and capacity among oversight bodies is crucial. FRA's fieldwork indicates that limits on oversight bodies' IT expertise and their technical capacity to fully access intelligence data poses, and will continue to pose, a major challenge. Interviewed experts stated they sometimes need to rely on external expertise to complement their own legal expertise. FRA's legal research shows that some EU Member State laws explicitly require oversight bodies to have technical expertise.

FRA opinion 4

EU Member State laws should ensure that oversight bodies have staff with the required technical expertise to assess independently the intelligence services' often highly technical work.

Ensuring oversight bodies' openness to public scrutiny

The European Court of Human Rights has underlined that intelligence services and oversight bodies should be held accountable for their work. They should be transparent and effectively inform parliaments and the public about their activities. FRA's research shows that in some Member States, enhanced transparency is achieved while respecting necessary secrecy. Experts interviewed during FRA's fieldwork consider enhanced transparency to be particularly important. However, oversight bodies' approaches to transparency vary considerably across Member States, ranging from publishing regular reports to having websites or using social media.

FRA opinion 5

EU Member States should ensure that oversight bodies' mandates include public reporting to enhance transparency. The oversight bodies' reports should be in the public domain and contain detailed overviews of the oversight systems and related activities (e.g. authorisations of surveillance measures, on-going control measures, ex-post investigations and complaints handling).

Fostering continuity of oversight

The European Court of Human Rights has held that effective oversight requires 'continuous control' at every stage of the process. FRA's research findings show extremely diverse oversight structures across EU Member States. When different bodies are involved in the various steps of oversight – from approving a surveillance measure to the oversight of its use – possible gaps or overlaps can result. Such shortcomings undermine the adequacy of the safeguards. FRA's fieldwork highlights that institutional and informal cooperation between the oversight bodies within individual Member States is crucial.

FRA opinion 6

EU Member States should ensure that the oversight bodies' mandates complement each other, so that overall they provide continuous control and ensure proper safeguards. Such complementarity can be achieved with informal cooperation between oversight bodies or statutory means.

Enhancing safeguards for protected professions

The European Court of Human Rights has held that enhanced safeguards are needed to protect journalistic sources in the context of surveillance. This principle similarly applies to other professions which, due to overarching principles such as parliamentary privileges, independence of the judiciary and confidentiality in lawyer-client relations, also require greater protection. FRA's research shows that while diverse approaches exist, several EU Member States have laws stipulating enhanced authorisation and approval procedures for, as well as stricter controls on, the processing of data collected through surveillance of individuals belonging to protected professions.

FRA opinion 7

EU Member States should establish specific legal procedures to safeguard the professional privilege of groups such as members of parliament, members of the judiciary, lawyers and media professionals. Implementation of these procedures should be overseen by an independent body.

Ensuring efficient whistleblower protection

The European Court of Human Rights has held that whistleblowing by civil servants should be ensured. Whistlebowers can significantly contribute to a well-functioning accountability system. FRA's research revealed different whistleblowing practices across EU Member States. Interviewed experts expressed diverging views about whistleblower protection.

FRA opinion 8

EU Member States should ensure efficient protection of whistleblowers in the intelligence services. Such whistleblowers require a regime specifically tailored to their field of work.

Subjecting international intelligence cooperation to rules assessed by oversight bodies

FRA's comparative legal analysis shows that almost all Member States have laws on international intelligence cooperation. However, only a third require intelligence services to draft internal rules on processes and modalities for international cooperation, including safeguards on data sharing. When they exist, these rules are generally secret. Only a few Member States allow for external assessments of international intelligence cooperation agreements.

FRA opinion 9

EU Member States should define rules on how international intelligence sharing takes place. These rules should be subject to review by oversight bodies, which should assess whether the processes for transferring and receiving intelligence respect fundamental rights and include adequate safeguards.

Defining in law oversight bodies' competences over international intelligence cooperation

FRA's comparative legal analysis shows that most Member States' laws do not have clear provisions on whether oversight bodies can oversee international cooperation exchanges. Eight EU Member States establish oversight bodies' competences over international intelligence sharing – either with or without limitations; laws in three EU Member States exclude any form of independent oversight. In the remaining 17 Member States, legal frameworks are subject to interpretation to determine oversight bodies' competences over international intelligence sharing.

FRA opinion 10

EU Member States should ensure that legal frameworks regulating intelligence cooperation clearly define the extent of oversight bodies' competences in the area of intelligence services cooperation.

Exempting oversight bodies from the third-party rule

In international intelligence service cooperation, the third-party rule prevents a service from disclosing to a third party any data received from a partner without the source's consent. FRA's research underlines that the third-party rule protects sources and guarantees trust among intelligence services that cooperate. However, FRA's data show that oversight bodies are often considered as 'third parties' and therefore cannot assess data coming from international cooperation. In some Member States, oversight bodies are no longer considered as 'third parties' and so have full access to such data.

FRA opinion 11

Notwithstanding the third-party rule, EU Member States should consider granting oversight bodies full access to data transferred through international cooperation. This would extend oversight powers over all data available to and processed by intelligence services.

Providing for effective remedies before independent bodies with remedial powers

The European Court of Human Rights has held that an effective remedy is characterised by investigative and decisional powers granted to judicial and non-judicial bodies. In particular, the remedial body should have access to the premises of intelligence services and the data collected; be given the power to issue binding decisions; and inform complainants on the outcome of its investigations. The individual should be able to appeal the body's decision. FRA's data show that 22 EU Member States have at least one non-judicial body with remedial powers. In six Member States, though, these bodies lack the powers to issue binding decisions and access classified data.

FRA opinion 12

EU Member States should ensure that judicial and non-judicial bodies with remedial powers have the powers and competences to effectively assess and decide on individuals' complaints related to surveillance.

Ensuring availability of non-judicial bodies with remedial powers

FRA's data show that non-judicial oversight mechanisms are more accessible to individuals than judicial remedies as they are simpler, cheaper and faster. FRA's comparative legal analysis shows that in the area of surveillance, individuals can lodge a complaint with a non-judicial body in 25 EU Member States. In ten Member States, one single non-judicial body has remedial powers, while in most Member States, individuals can lodge a complaint with two or more bodies with remedial powers.

FRA opinion 13

EU Member States should ensure that both judicial and non-judicial remedial bodies are accessible to individuals. Notably, Member States should identify what potential gaps prevent individuals from having their complaints effectively reviewed, and ensure that non-judicial expert bodies can complement the remedial landscape where needed.

Allowing for awareness of completed surveillance measures

FRA's comparative legal analysis shows that all EU Member States have a national security exception in their freedom of information laws. FRA's findings also show that all Member States limit either individuals' right to be notified or their right to access their own data based on the confidentiality of intelligence data and protection of national security or of on-going surveillance operations. Some Member States' laws provide for alternative ways to make individuals aware of surveillance measures and so enable them to seek an effective remedy.

FRA opinion 14

EU Member States should ensure that the legitimate aim and proportionality tests are conducted by intelligence services before limiting access to information based on national security. A competent authority should assess the confidentiality level. Alternatively, controls should be carried out by oversight bodies in the name of complainants when notification or disclosure are not possible.

Ensuring a high level of expertise among remedial bodies

Remedial bodies need to have a good understanding of surveillance techniques. FRA's fieldwork has identified ways to informally address shortcomings in technical expertise. Exchanges between remedial bodies, expert bodies, and intelligence services, while respecting each other's role and independence, have proven to deepen the technical understanding of reviewers and foster mutual trust. National practices of appointing specialised judges or establishing specialised courts or chambers to hear complaints about surveillance by intelligence services contribute to the development of judicial expertise in the area. Such systems can also facilitate different arrangements on judicial access to classified information.

FRA opinion 15

EU Member States should ensure that where judicial or non-judicial remedial bodies lack relevant expertise to effectively assess individuals' complaints, specific systems are established to address these gaps. Cooperation with expert oversight bodies, technical experts or members of the intelligence services can support effective remedial systems.

Supporting other human rights actors

FRA's fieldwork underlines that national human rights institutions, civil society organisations and, in some cases, ombudsperson institutions can play a crucial role in an enhanced intelligence services accountability system. However, FRA's fieldwork also shows that civil society organisations often lack adequate resources, with few able to offer comprehensive services to victims of alleged unlawful surveillance.

FRA opinion 16

EU Member States should broaden the operational space for national human rights bodies and institutions and civil society organisations, which can play a strong role as 'watchdogs' in the oversight framework.

Introduction

Intelligence services play a crucial role in protecting national security and helping law enforcement to uphold the rule of law. This is particularly true across the European Union (EU) today, with terrorism, cyber-attacks and organised crime groups located outside of the Union all posing serious threats to Member States.

EU Member States working both nationally and in partnership – and in cooperation with other states, such as the United States – are increasingly using digital intelligence methods to fight these threats. Intelligence services' capabilities include collection, interception and analysis of communications and metadata, hacking and computer network exploitation, as well as data mining of databases containing personal information. Such methods have implications for the fundamental rights of European citizens – such as privacy and freedom of expression – and their use must always be justified in a way that respect to those rights is ensured. Strong safeguards are necessary to ensure that they are used in accordance with law, and that interference with some rights to protect others, such as the right to life, only takes place when justified as necessary and proportionate, as allowed for by the ECHR.

The 2013 Snowden revelations showed that the United States (US) and some EU Member States were involved in what is colloquially referred to as 'mass surveillance' activities. This prompted discussions at several institutions, especially national parliaments. The inquiry committee of the German parliament published a particularly encompassing report in June 2017.[1] The EU also reacted strongly. At the time, the European Commission, the Council of the EU and the European Parliament all reported on the revelations. They expressed concern about mass surveillance programmes, sought clarification from US authorities, and worked on "rebuilding trust" in transatlantic relations.[2] The Snowden revelations also damaged the trust of EU citizens towards public authorities, intelligence services and technological companies providing communication software and hardware.

"The culture in the secret services is one of secrecy, and the present culture in society is to be as open as possible. The key element for the existence of the secret services today is what is called trust. Trust in society that they act between the borders of the law. For that you need to become more transparent than you were before."

(FRA interview with expert body, 2016)

(In)effectiveness of mass surveillance

"More generally, [...] it was found that massive eavesdropping measures, besides raising compatibility issues with fundamental rights and compliance with necessity and proportionality principles, as at various time delineated by European case law, prove to be inefficient.

The equation that a greater volume of available data and information would automatically result in better results in terms of security and prevention was not demonstrated."

Italy, COPASIR (2017), p. 12

"The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive or slower."

Anderson, A. (2016), p. 1

On 12 March 2014, the EP adopted a resolution on the US National Security Agency (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.[3] The resolution drew on the in-depth inquiry that the EP tasked the Civil Liberties, Justice and Home Affairs Committee (LIBE) with conducting during the second half of 2013, shortly after the revelations on mass surveillance were published in the press.[4]

The wide-reaching resolution launched a "European Digital Habeas Corpus – Protecting fundamental rights in a digital age" focusing on eight key actions. The resolution also 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".[5]

In 2015, FRA published the report *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (hereinafter the '2015 FRA report').[6] The 2015 FRA report presents the legal safeguards that the 28 EU Member States had for ensuring that surveillance measures do not violate fundamental rights. Since then, EU Member States have suffered serious terrorist attacks, triggering a state of emergency in France; have

1 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b).
2 FRA (2014a), p. 81 and following; FRA (2015a).
3 European Parliament (2014), hereafter: the resolution.
4 See FRA (2014a).
5 European Parliament (2014), paras. 132 and 35.
6 FRA (2015a).

faced migration pressures across the Mediterranean, prompting suspension of Schengen area free movement arrangements; and have been confronted with a rising tide of cyber-attacks, intensifying concern about this threat. Several Member States have introduced legislation to strengthen intelligence gathering in response to public pressure over these developments, while expanding the scope of their laws to explicitly cover more of their intelligence services' digital activity and improving oversight and other safeguards against abuse in light of the 2015 FRA report.

Methodology

The present report builds on the 2015 FRA report by providing a socio-legal analysis. Specifically, it:

- updates the 2015 FRA report's legal findings; and
- analyses findings from fieldwork interviews with key actors in the area, such as expert bodies, parliamentary committees, the judiciary, data protection authorities, national human rights institutions, as well as civil society organisations, academia, and media representatives.

FRA staff carried out the fieldwork in 2016, conducting over 70 interviews in seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom. The interviews addressed how intelligence legal frameworks are being implemented in practice and whether they comply with fundamental rights. For a thorough presentation of the methodology, see Annex 1.

The draft report was reviewed by a number of experts. They include Prof. Nico van Eijk, Director of the Institute for Information Law, University of Amsterdam; Prof. Ian Leigh, Durham Law School , Durham University; Prof. Sir David Omand, Visiting Professor, Department of War Studies, King's College, London; and Thorsten Wetzling, Project Director at the Stiftung Neue Verantwortung.

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

Five of the seven EU Member States – France, Germany, the Netherlands Sweden and the United Kingdom – were selected because they have detailed legislation on general surveillance of communications. They illustrate fundamental rights safeguards Member States introduce, particularly the oversight of intelligence services, when collecting large quantities of data. Italy and Belgium do not have as detailed legislation on the general surveillance of communications by civil intelligence services. However, the structures of their oversight systems are good examples of two different approaches to overseeing the surveillance measures at the services' disposal. In contrast to the 2015 FRA report, the present report also covers international cooperation between intelligence services.

This FRA project encountered several challenges. The intelligence field involves sensitive topics, resulting in secrecy, little knowledge about European intelligence services' data collection, and different organisational and professional cultures among the main actors, such as intelligence services and oversight bodies, within and across Member States. Recent reforms of intelligence legislation in many Member States have brought further changes to working practices; the comparative tried to capture the changes up to the time of publication. Moreover, the number of experts in the area is limited – in some cases concentrated on a single person (or a few) who represents a specific function in the system. This made access to potential respondents more difficult and made necessary intensive preparatory work in building up trustful and cooperative relationships in each Member State and institution. Finally, in some instances, Member States' interpretation of the applicability of EU law and FRA's mandate posed additional challenges to accessing national expertise – in particular that of active intelligence service representatives, who did not take part in any of the interviews.

Scope of analysis

This report, together with the 2015 FRA report, constitutes the agency's response to the EP's request to study the impact of 'surveillance' on fundamental rights. However, given the context in which the resolution was drafted, so-called 'mass surveillance' is the main focus of the parliament's work. During the data collection phase for FRA's first report in 2014, FRA used the parliament's definition of 'mass surveillance' to delineate the research's scope.

> The EP resolution refers to: *"[F]ar-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."* European Parliament (2014), para. 1

The European Parliament's definition – highlighted as an excerpt – encompasses two essential aspects: first, a reference to technical collection of intelligence, and second, emphasis on untargeted collection. The distinction between targeted and untargeted collection remains disputed when it comes to techniques enabling general surveillance of communications.

> *"Even though the inquiry committee's investigations have neither found systematic fundamental rights violations nor evidence of 'mass surveillance' or uncontrolled data accumulation or transmission by the BND, the opposition has continually fuelled such fears: with incorrect claims on the consequences of the law and unfounded equating of the BND and the NSA. "*
>
> *Germany, Federal Parliament* (Deutscher Bundestag) *(2017b), p. 1316*

Formulating a precise definition also constituted a methodological challenge for FRA. The methods used by intelligence services have evolved since 2015, and so has the corresponding terminology. This report uses the term 'general surveillance of communications' to refer to what the 2015 FRA report called 'signals intelligence' (SIGINT), since the latter is no longer fully accurate in light of the range of methods currently used by intelligence services.

This report focuses on the work of intelligence services. It does not address the work of law enforcement authorities. Nor does it cover the obligations of commercial entities which are, by law, required to provide intelligence services with raw data – obligations which amount to general surveillance of communications – and are otherwise involved in surveillance programmes. The private sector's role in surveillance requires a separate study. Some commercial entities – especially telecommunication service providers – produce regular 'transparency reports', which outline the requests they receive from public authorities to access data related to users of their commercial services.[7]

> *"A right is only worth as much as its delimitations and enforcement mechanisms allow it to be. This is crucial in the area of governmental surveillance, since we need safeguards without borders as well as remedies across borders."*
>
> *UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci, p. 12*

Given that the secret monitoring of communications – as the ECtHR refers to such activity[8] – interferes with the fundamental right to privacy, this report focuses on analysing the safeguards included in EU Member States' legal frameworks, and on the different ways states safeguard fundamental rights in practice.

Fundamental rights safeguards

Given the scope of the EP's request, the report focuses on privacy and data protection. Other fundamental rights – such as freedom of expression, freedom of religion and freedom of association – are also affected but are not the primary object of the analysis.[9] A fundamental right must be properly safeguarded to be effectively exercised. This report also analyses, as per the EP's request, effective remedies that individuals can pursue to enforce their rights.

The 2015 FRA report referred to existing international and European standards applicable to surveillance.[10] While updating the analysis to take into account the evolution of United Nations (UN) and European standards, this report refers to the *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* (UN Good practices),[11] of which the Human Rights Council took note in 2012.[12] This set of soft law standards remains, to this date, the only encompassing document in the field at universal level.[13]

The ECtHR has well-developed case law on Article 8 of the ECHR (right to respect for private and family life) – including its procedural aspects[14] – and Article 13 of the

7 For an overview of telecommunications, internet and mobile companies' transparency reports, see Ranking Digital Rights (2017).

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

9 See European Parliament (2014), para. T. See also FRA (2015a), p. 9, United Nations (UN) General Assembly (GA) (2016); UN Human Rights Council (2017); UN, Human Rights Council (2016), UN, Human Rights Council (2017), Report of the Special Rapporteur David Kaye; UN, Human Rights council (2017), Report of the Special Rapporteur Joe Cannataci; UN, Human Rights Council (2017), Report of the Special Rapporteur Ben Emmerson; 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); Mills, A. and Sarikakis, K. (2017).

10 FRA (2015a), p. 9.

11 UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin.

12 UN, Human Rights Council (2012), Resolution on the protection of human rights and fundamental freedoms while countering terrorism, 23 March 2012.

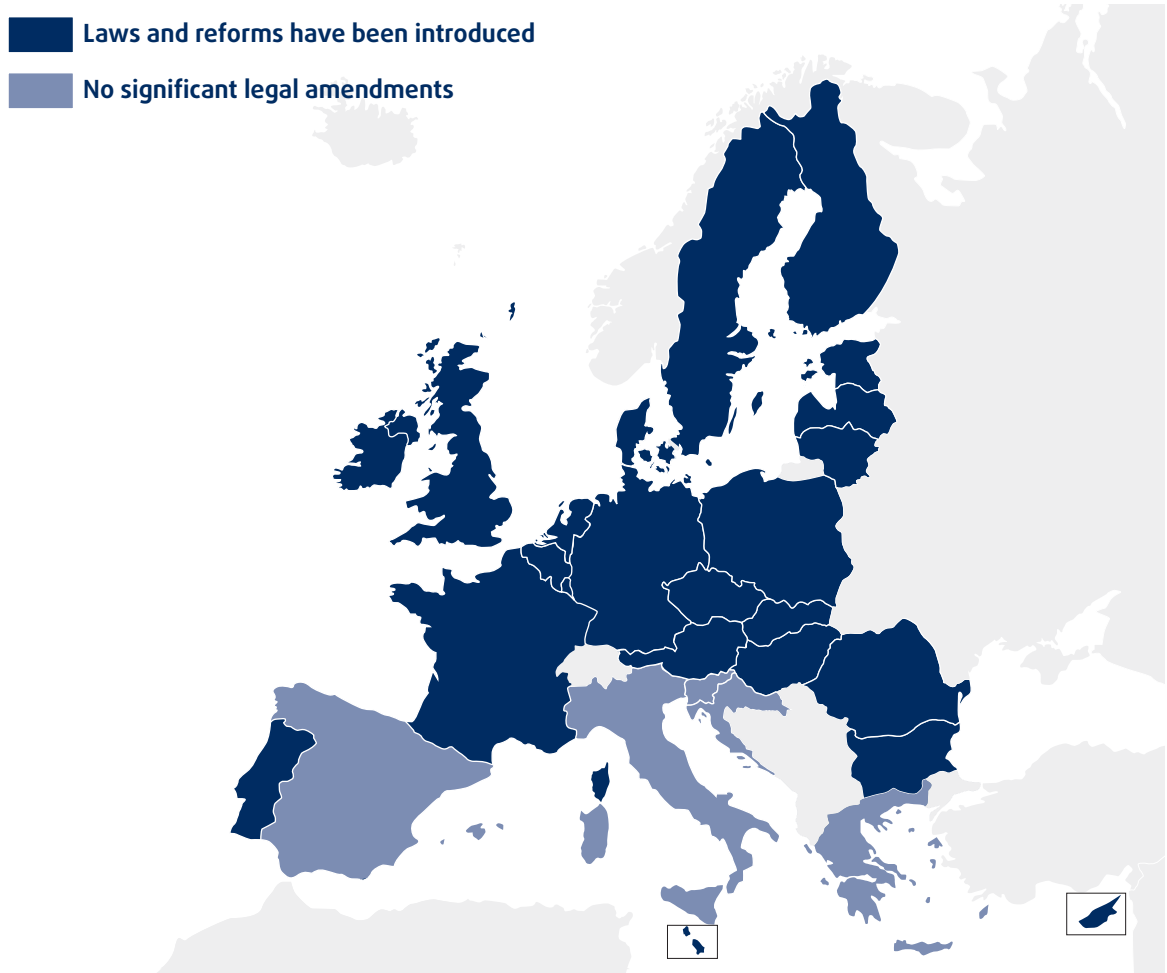
13 See UN, GA (2014a); UN, GA (2016c); UN, Human Rights Council (2009), Report of the Special Rapporteur Martin Scheinin; UN, Office of the High Commissioner for Human Rights (OHCHR) (2014); UN, Human Rights Council (2014), Report of the Special Rapporteur Ben Emmerson; UN, Human Rights Committee (2014); UN, Human Rights Committee (2015); UN, Human Rights Council (2016), Report of the Special Rapporteur Joe Cannataci; UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci.

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

ECHR (right to an effective remedy).[15] Nonetheless, cases on general surveillance of communications still need to be adjudicated.[16] Since publication of the 2015 FRA report, the ECtHR handed down a seminal judgment in *Roman Zakharov v. Russia*.[17] In this judgment, the court's Grand Chamber summarised and clarified past case law, while finding that the Russian legal framework was not compatible with human rights standards.

As stated in the 2015 FRA report, the ECtHR's human rights standards – which should be considered minimum standards – have served as a benchmark for Member States' legislative reforms. Figure 1 presents an overview of reforms of legal frameworks on surveillance that have taken place in the EU-28 since the 2015 FRA report. In light of heightened security pressures, an overwhelming majority of EU Member States have reformed or are in the process of reforming their legal frameworks.

Figure 1: EU Member States' legal frameworks on surveillance reformed since October 2015



Source: FRA, 2017

15 For a discussion of the ECtHR case law, see Council of Europe (2016), pp. 55-93. See also von Bernstorff, J. and Asche, J., Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 79 and following.

16 See the pending cases: ECtHR, *Centrum För Rättvisa v. Sweden*, No. 35252/08; ECtHR, *Big Brother Watch and Others v. the United Kingdom*, No. 58170/13; ECtHR, *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom*, No. 62322/14; ECtHR, *10 Human Rights Organisations and Others v. the United Kingdom*, No. 24960/15; ECtHR, *Association confraternelle de la presse judiciaire v. France*, No. 49526/15.

17 ECtHR, *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015.

Surveillance activities and national security: applicability of EU Law

"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."

Anderson, D. (2015), p. 71

The 2015 FRA report gave an overview of privacy and personal data protection in primary and secondary EU law. It also referred to the 'national security' exemption, which limits the applicability of EU legal instruments.[18] The EU Data Protection Reform adopted in 2016[19] maintains this exemption in Article 2 (2) of the General Data Protection Regulation (GDPR) and in Article 2 (3) of the Data Protection Directive for Police and Criminal Justice Authorities, which excludes the "processing of personal data in the course of an activity which falls outside the scope of Union law" from its scope. This provision should be read in conjunction with Recital 14 in the *Data Protection Directive* for Police and Criminal Justice Authorities, which explains that Article 2 (3) means that "activities concerning national security, activities of agencies or units dealing with national security issues [...] should not be considered to be activities falling within the scope of this Directive."

The 2015 FRA report demonstrated that the debate regarding the limits of the 'national security' exemption, particularly in relation to counter-terrorism measures, involves both intelligence services and law enforcement authorities.[20] Since 2015, following several terrorist attacks in Europe, the EU has created a Security Union to counter terrorism efficiently.[21] In that context, the Council of the EU appointed a Commissioner for Security Union in 2016. The commissioner's task is to create an effective and sustainable Security Union, placing fundamental rights at the centre of the framework.[22]

Recent EU-level initiatives with national security relevance

Several initiatives have been introduced at EU level since 2015 as part of a broad effort to bolster Member States' national security. These include:

- **Policies/policy proposals**: European Agenda on Security (2015); European Commission's suggestion to open Counter Terrorism Group to 'interaction' with law enforcement authorities through Europol (2016)
- **Specialised bodies**: appointment of Commissioner for Security Union (2016); creation of European Parliament special committee to tackle deficiencies in the fight against terrorism (2017)
- **EU agencies**: EU Intelligence and Situation Centre (INTCEN); EU Satellite Centre (SatCen)
- **Legislation**: adoption of Passenger Names Record Directive 2016/681 (2016)

Source: FRA, 2017

The exchange of existing intelligence among Member States for counter-terrorism purposes and access to such data by law enforcement authorities are challenging issues for the Security Union. Data collected by a Member State's intelligence services fall under the exclusive competence of that Member State. The European Commission has stated that solutions to the lack of clarity in the relationship between the law enforcement community and intelligence community should be urgently identified. At present, exchanges of data among national intelligence services take place voluntarily and outside the EU's legal framework, through – for instance – the Club de Berne and the derived Counter Terrorism Group (CTG). The CTG is an intelligence-sharing forum that focuses on counter-terrorism intelligence and encompasses all EU Member States, as well as Norway and Switzerland. The Commission has suggested opening the CTG to 'interaction' with law enforcement authorities, through the existing Europol framework.[23] Meanwhile, in July 2017, the European Parliament created a special committee to tackle deficiencies in the fight against terrorism. The committee is tasked with assessing the extent of terrorist threats on European soil and

18 FRA (2015a), p. 10.

19 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119 (*General Data Protection Regulation, GDPR*); and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119 (*Data Protection Directive for Police and Criminal Justice Authorities*).

20 FRA (2015a), p. 10. For an analysis of the competence of the EU on national security and intelligence services, see also Sule, S. (2017), pp. . 16-20.

21 European Commission, Juncker, J.-C. (2016), 'Juncker after Brussels terror attacks: "We need a Security Union"', Joint Press Conference with French Prime Minister Manuel Valls, 24 March 2016.

22 King J. (2016), 'Introductory remarks by the Commissioner-designate Sir Julian King to the LIBE Committee', Press release, Strasbourg, 12 September 2016.

23 European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council, "Enhancing Security in a world of mobility; improved information exchange in the fight against terrorism and stronger external border", COM(2016)602, Brussels, 14 September 2016, p. 15.

examining the factors that led to recent terrorist attacks in Europe. The committee will look into various aspects, such as deficiencies in intelligence information sharing among Member States and the impact of such sharing on fundamental rights.[24]

At legislative level, the creation of the Security Union led to the adoption of the Passenger Name Records (PNR) Directive.[25] PNR data are collected by airlines from passengers during check-in and reservation procedures. Intelligence services can subsequently access PNR data collected by airlines and use them for intelligence purposes. The PNR Directive establishes at EU level a common legal framework for exchanging PNR data among Member States, as well as sharing PNR data with Europol. The PNR data may then be used for the fight against terrorism and serious crime under certain conditions set by the directive.

National security was also at issue in a 2016 Court of Justice of the European Union (CJEU) judgment. In joined cases *Tele2 Sverige* and *Home Secretary v. Watson*,[26] the CJEU found that requiring telecommunication companies to retain all electronic communications data, meaning data about telephone calls, emails and websites visited by their clients, was not in conformity with the *e-Privacy Directive*[27] and the EU Charter of Fundamental Rights, violating the right to respect for private life and protection of personal data. The court stated that, in the case of serious crime, Member States can impose a general obligation on providers of electronic telecommunications services to retain data only if deployed against specific targets. Retention measures must be necessary and proportionate regarding the categories of data to be retained, the means of communication affected, the persons concerned and the chosen duration of retention. Furthermore, national authorities' access to the retained data must be conditional and meet certain data protection safeguards. The court explicitly distinguished cases where the data are retained to protect 'national security' from other types of 'serious crime'.[28] Where 'national security' is at stake, the court concluded that access may also be granted to data of persons other than the specific targets; however, as a safeguard, there must be objective evidence of these data's effective contribution to the fight against a specific 'national security' threat.

'National security' is also relevant to the transfer of personal data to a third country on the basis of a decision that the third country provides an adequate level of protection of personal data (adequacy decision). Under the GDPR, to assess the level of protection of personal data, the European Commission must take into account any relevant legislation concerning national security as well as the implementation of such legislation. In particular, the Commission looks at whether the third country guarantees effective and enforceable data subject rights, and effective and judicial redress for the data subjects whose personal data are being transferred.[29] The *EU-US Privacy Shield* is an example of such an adequacy decision. This decision allows for free flow of data for commercial purposes between the EU and the US.[30] The *EU-US Privacy Shield* was the result of the annulment of the *Safe Harbour* Adequacy Decision by the CJEU in *Schrems*.[31] The CJEU looked into personal data transfers to the US on the basis of the *Safe Harbour* Adequacy Decision and subsequent access to the data by national intelligence services for reasons of national security. The CJEU held that legislation must provide effective oversight and redress mechanisms. Failing to provide an effective remedy violates Article 47 of the Charter.

The 'national security' exemption thus cannot be seen as entirely excluding the applicability of EU law. Individuals' records of calls, text messages, e-mails and any other forms of electronic communication that are retained by their telecommunications providers and subsequently transferred to intelligence services for national security purposes could enjoy the standards of protection offered by the GDPR.

24 European Parliament (2017), European Parliament Decision of 6 July 2017 on setting up a special committee on terrorism, its responsibilities, numerical strength and term of office, P8_TA-PROV(2017) 0307, Strasbourg, 6 July 2017.

25 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016 (*PNR Directive*).

26 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016.

27 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31 July 2002 (*Directive on privacy and electronic communications*).

28 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 119.

29 GDPR, Art. 45.

30 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ 2016 L207, 1 August 2016.

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

As explained in the 2015 FRA report, if EU law is not applicable, Council of Europe conventions might be.[32] These include the ECHR and the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108),[33] and its 2001 Additional Protocol related to transborder data flows to non-parties to Convention 108 and the mandatory establishment of national data protection supervisory authorities.[34] Convention 108 is currently being amended to, on the one hand, better address challenges resulting from the use of new information and communication technologies and, on the other hand, to strengthen its implementation.[35] The reform maintains the general and technologically neutral nature of the convention's provisions; it does not impose or discriminate in favour of the use of a particular type of technology. At the same time, it aims to be coherent with other legal frameworks, such as the EU's. In line with the GDPR, the reformed Convention 108 will include an exception to the protection of personal data for the processing activities for national security.[36] However, such an exception must be provided for by law, respect the essence of fundamental rights and freedoms, and constitute a necessary and proportionate measure in a democratic society. The reformed Convention 108 will also require processing activities for national security purposes to be subject to independent and effective review and supervision. Convention 108 is of great importance to the EU legal order given that all EU Member States ratified it following a 1999 amendment, and that the EU could become a party thereto.[37]

Report structure

The report is structured as follows:

- **Part 1** provides an overview of intelligence services and surveillance laws in all EU Member States. Highlighted findings from fieldwork interviews conducted at national level in selected EU Member States offer insights into how experts view legal frameworks in terms of their compliance with human rights standards.

- **Part 2** presents existing statutory safeguards, focusing on oversight of intelligence services. Most fieldwork findings are presented in this part. While the 2015 FRA report treated oversight mechanisms according to the type of institution involved, this report presents oversight mechanisms according to their role in oversight.

- **Part 3** analyses the available remedies for an individual in cases of alleged unlawful surveillance. The fieldwork findings on the availability and effectiveness of remedial avenues provide empirical evidence.

The report's annexes present the research data collection methodology (Annex 1), the intelligence services in the EU-28 (Annex 2), and key features of expert oversight bodies' and parliamentary oversight committees' annual reports (Annex 3 and Annex 4).

32 FRA (2015a), p. 11.
33 Council of Europe, Convention for the protection of individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981 (*Convention 108*); CJEU, C-387/05, *European Commission v. Italian Republic*, 15 December 2009, para. 45.
34 Council of Europe, Convention 108, 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, 2001.
35 Council of Europe, Draft Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (*Draft Modernised Convention 108*).
36 *Ibid*. Art. 9.
37 Council of Europe, Amendments to the Convention for the protection of individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form.

PART I: THE LEGAL FRAMEWORK FOR INTELLIGENCE

KEY FINDINGS

Intelligence services' legal frameworks

- All EU Member States regulate by law the organisation of their intelligence services to comply with rule of law and human rights standards.
- The organisation of intelligence services varies significantly in the EU Member States. In some, two intelligence services carry out the work, while in others, five, six or more bodies may apply surveillance measures.
- International human rights standards require that intelligence services' mandate and powers be defined in legislation. The law has to be clear, foreseeable and accessible. Interviewees raised concerns relating to the complexity, as well as the lack of clarity and comprehensiveness, of some legal frameworks.
- The mere existence of a law allowing for surveillance measures – either targeted (with prior suspicion) or untargeted (without prior suspicion) – constitutes an interference with the fundamental rights to privacy and data protection.
- Under EU data protection law, the collection of data by intelligence services in itself constitutes an interference.
- Almost all EU Member States have a legal framework on targeted surveillance.
- France, Germany, the Netherlands, Sweden and the United Kingdom have detailed legislation on general surveillance of communications.
- Legal safeguards are more extensive for domestic surveillance than for foreign-focused surveillance.
- France, Germany, the Netherlands and the United Kingdom have reformed their legislation extensively since 2015. Several other Member States have started significant reforms. These aim, among others, to adapt to new technological developments and respond to new threats. Reforms increased transparency on surveillance powers granted to intelligence services. Interviewed experts acknowledged that legal reforms have brought improvements. However, interviewees believe that lack of clarity – and hence the need for quality legal rules governing the work of intelligence services – remains an issue.
- The concept of national security is not harmoniously defined across EU Member States. The scope of national security is rarely defined, and sometimes other, similar terms are used. Interviewed experts confirmed the need for clearer definitions of – among other terms – national security, including at EU level.

International cooperation frameworks

- Almost all EU Member States' laws allow for international intelligence cooperation. Only few detail in their legislation the procedures intelligence services must follow to establish international cooperation.
- Before establishing cooperation agreements, intelligence services from eight Member States have to follow confidential internal rules. A small number of EU Member States' laws prescribe a review of international cooperation agreements by independent bodies.

1 Intelligence services in the EU-28: a diverse landscape

UN good practices on mandate of intelligence services

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 (2010), Report of the Special Rapporteur Martin Scheinin

The organisation of intelligence communities within the EU-28 has not fundamentally changed since publication of the 2015 FRA report, and FRA's subsequent fieldwork research did not address this topic. This chapter therefore reiterates some of the earlier report's main findings, and provides updates where warranted.

This report uses generic terminology, referring to 'intelligence services' for both 'intelligence services' that focus on foreign threats and 'security services' that focus on domestic threats.[38] The report focuses only on these entities' intelligence collection, analysis and dissemination functions, and not on any other activities involved in directly countering and disrupting threats.[39]

Annex 2 lists the existing intelligence services in the EU Member States. The table does not list Member State assessment and coordination bodies, such as the United Kingdom Joint Intelligence Committee; the Department for Security Information (DIS) in Italy; or the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*) in France, who is a part of the French intelligence community.[40]

By law, all EU Member States regulate the organisation of their country's intelligence services. Almost all have established at least two different bodies for conducting civil and military intelligence. In practice, the line separating the mandates of civil and military services is increasingly blurred;[41] many digital techniques – such as the geolocation of mobile devices – are used by both. Since this report is concerned with surveillance and not with wider national security intelligence gathering, it focuses – to the extent possible – on civil intelligence services. It does not cover the latter's work on military targets or the work of purely military intelligence services, given that they fall outside the scope of the EP resolution that sparked this research.

In some Member States, civil intelligence services are further divided into separate services – often with a domestic or foreign mandate. In some cases, these separate services have access to common platforms for technical and digital intelligence gathering operations. Moreover, some Member States grant the power to conduct intelligence operations to units that are not part of the civil intelligence services and that specialise

38 See Cousseran, J.-C. and Hayez, P. (2015), p. 41 and UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin, p. 4.

39 Born, H. and Wills, A. (eds.) 2012.

40 France, Defence Code (*Code de la Défense*), Art. D 1122-8-1. See also France, CNCTR (2016), p. 33 and France, DPR & CNCTR (2017), p. 13.

41 See Council of Europe (2016), p. 61; Cousseran, J.-C. and Hayez, P. (2015), p. 30.

in countering defined threats, such as organised crime, corruption or the fight against terrorism.

In France, for example, implementing regulations of the 2015 intelligence law established two intelligence 'circles'. The 'first circle' (*premier cercle*) is composed of six so-called specialised intelligence services (*services spécialisés de renseignement*), such as the *Direction générale de la sécurité interieure (DGSI)* and the *Direction générale de la sécurité exterieure (DGSE)*.[42] The six services have access to most intelligence techniques prescribed by the Interior Security Code.[43] The 'second circle' (*second cercle*) services have access to a number of intelligence techniques depending on their mandate.[44] These are police,*gendarmerie* and security services that are not part of the French intelligence community. Since 2017, the 'second circle' has been widened to include two offices placed under the authority of the director of prison administration (*directeur de l'administration pénitentiaire*), under the minister of justice. These can be authorised to use certain intelligence techniques to prevent terrorism, crime and organised crime in prisons.[45]

A state's constitutional organisation also plays a role in the organisation of the services. In Germany, for example, aside from the federal services, each regional state (*Land*) has an intelligence service.

Another key element 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 in one service and the risk of arbitrary use of information obtained in secrecy.

Maintaining a separation between police and intelligence services

"[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."

PACE (1999), p. 2

42 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 811-1. See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 40.
43 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 811-2.
44 *Ibid*. See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 51.
45 See France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 811-2 III. See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 54. See for critical views on this widening of the intelligence circles: France, DPR & CNCTR (2017), p. 49 and 60 and following.

The majority of intelligence services in the EU Member States have their own structure, organisation and accountability, independent of the police and other law enforcement authorities. Calls for enhanced cooperation between police and intelligence services in the fight against terrorism sometimes make it difficult to see the dividing lines between the two entities. The wave of terrorist attacks across Europe in the past few years has brought law enforcement and intelligence services closer together, with security professionals widely regarding joint investigations of terrorist networks and suspects as constituting best practice.

Differences between surveillance by police and by intelligence services

"[Surveillance by intelligence services] 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."

Council of Europe (2016), p. 64

Since publication of the 2015 FRA report, Cyprus has established its intelligence services in law. The law provides for strict organisational separation between the police and the intelligence services.[46] Few Member States make exceptions to this rule. Those that do include Austria, Denmark, Finland and Ireland, where the body responsible for conducting intelligence activities is officially part of the police and/or law enforcement authorities.

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 private life and personal data protection.[47] In Germany, for instance, the police and intelligence services have used shared databases frequently since 2004.[48]

46 Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*) N. 75(I)/2016, Art. 3.
47 Sule, S. (2006), pp. 128 and 236.
48 Töpfer, E. (2013), pp. 5 and following.

2

Surveillance measures in the digital age

The 2015 FRA report presented the key features of the surveillance measures that were at the core of the Snowden revelations.[49] When referring to large-scale technical collection of intelligence, it used the term 'signals intelligence'. This report instead uses the term 'general surveillance of communications' to refer to such activity.

Signals intelligence is a traditional term originally used for the interception and analysis of radio signals – but is still widely used, even where the signals in question are transmitted by other means, such as fibre optic cables. The term is mentioned in some Member States' legislation – for example, Sweden, which refers to '*signalspaning*' – literally, 'signal reconnaissance'. When 'signals intelligence' is not used, institutions and commentators use various terms to refer to these surveillance techniques. The UN refers to 'mass digital surveillance',[50] 'online surveillance',[51] 'bulk interception',[52] or 'bulk telephone metadata collection'.[53] The UN Special Rapporteur on privacy uses the terms 'mass surveillance' and 'bulk hacking' when discussing, for example, the powers included in the United Kingdom's Investigatory Powers Act.[54] The Special Rapporteur also refers to 'bulk processing'.[55] The Committee of Ministers of the Council of Europe refers to 'broad surveillance of citizens';[56] 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';[57] and the Parliamentary Assembly of the Council of Europe entitled its report 'mass surveillance'.[58] The European Parliament refers to 'mass surveillance' in its 2014 resolution on the topic,[59] and Bigo *et al.* in their commissioned report for the European Parliament refer to large-scale surveillance and 'cyber-mass surveillance'.[60] The ECtHR refers to 'exploratory or general surveillance'[61] and 'strategic monitoring' to identify risks (as opposed to individual monitoring of specific persons, with suspicion).[62]

The Venice Commission uses the concept of 'strategic surveillance' to emphasise that "signals intelligence can now involve monitoring of 'ordinary communications' ".[63] 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 on identified individuals and groups",[64] 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 go through selectors or discriminants applied by algorithms. This touches on the second key aspect of the European Parliament's definition in its 2014 resolution, which requires an explanation of the

49 FRA (2015a), p. 15-16.
50 UN, Human Rights Council (2017), Report of the Special Rapporteur Ben Emmerson, p. 10.
51 *Ibid.*
52 *Ibid.*
53 *Ibid.* p. 11.
54 UN, GA (2016a), Report of the Special Rapporteur Joe Cannataci, paras. 28-29.
55 *Ibid.* para. 29.
56 Council of Europe, Committee of Ministers (2013).
57 Council of Europe, Conference of Ministers responsible for Media and Information Society (2013), para. 13 (v).
58 Council of Europe (2016).
59 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, P7_TA(2014) 0230, Strasbourg, 12 March 2014.
60 Bigo, D. *et al.* (2013), p. 14.
61 ECtHR, *Klass and others v. Germany,* No. 5029/71, 6 September 1978, para. 51.
62 ECtHR, *Weber and Saravia v. Germany*, No. 54934/00, 29 June 2006, para. 4.
63 Council of Europe (2016), p. 61.
64 *Ibid.* p. 61, fn. 4.

distinction between targeted and untargeted collection. The UK Independent Reviewer of Terrorism Legislation Anderson highlighted the difference between the concept of bulk powers, as prescribed by the United Kingdom's legal framework, and 'mass surveillance', in a 2016 report (see excerpted quote).

Bulk powers versus mass surveillance

"[T]he exercise of a bulk power implies the collection and retention of large quantities of data which can subsequently be accessed by the authorities. On this broad definition, the characterisation of a power as a bulk power does not depend on whether data is collected and stored by the Government or by a private company. […]

But the [Investigatory Powers Bill] proceeds on a narrower definition of bulk powers, limited to those powers which provide for data in bulk to be acquired by the Government itself.

Whether a broader or narrower definition is preferred, it should be plain that the collection and retention of data in bulk does not equate to so-called "*mass surveillance*". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers [CSPs]) is not given on an indiscriminate or unjustified basis."

Anderson QC, D. (2016), Report of the bulk powers review, p. 3-4

Technological developments and the need to respond to new national security threats, particularly in the context of counter-terrorism, prompted intelligence gathering techniques to evolve. Intelligence services now focus more on network traffic – the data moving across a network at a given point in time.

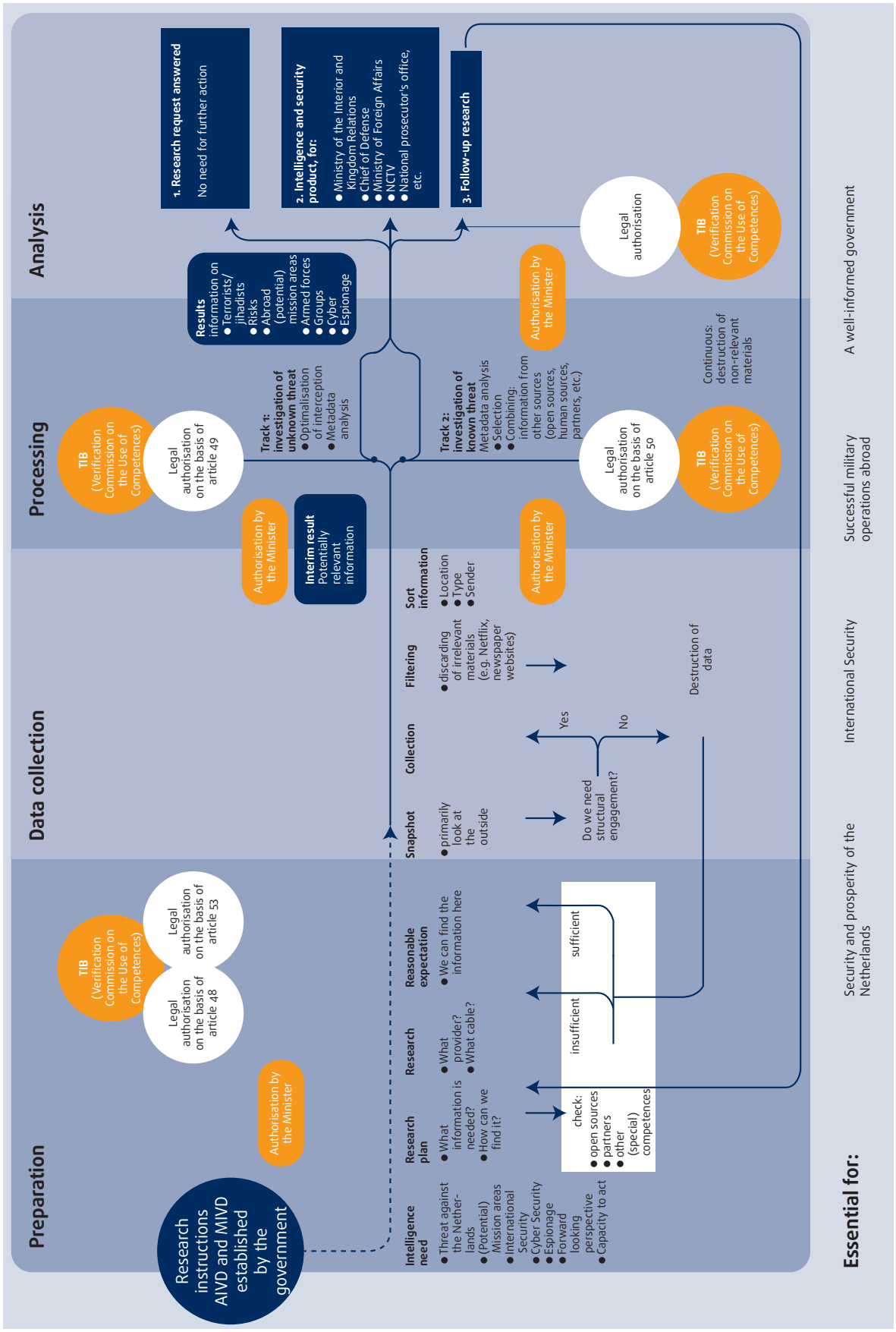
The 2015 FRA report referred to a publication of the US National Research Council to illustrate the conceptual model of signals intelligence.[65] Meanwhile, the Dutch government published an alternative figure when it submitted the Dutch draft intelligence bill, reflecting the Dutch process of cable communications interception after the Intelligence and Security Services Act 2017 enters into force (see Figure 2).[66] It shows that the Dutch intelligence services will intercept communications transmitted via cables when they will not have sufficient information from other sources. Figure 2 also shows that the collected data are filtered before they are stored, to disregard irrelevant materials for the fulfilment of the intelligence services' mandate. The final stage before storage consists of sorting the data according to the information they provide (for example, location or identity). Concerning the processing of the stored data, Figure 2 shows that selection is conducted to identify the possibly relevant information for a particular investigation. Once the final analysis of the gathered intelligence is completed, intelligence services continue with 'follow-up research'.

In 2015 and 2016, the CJEU delivered judgments in the *Schrems*[67] and *Tele2*[68] cases, respectively. In *Schrems*, the CJEU examined the interference with EU citizens' right to private life and protection of personal data resulting from surveillance activities by US authorities – specifically, the collection of and access to data of EU citizens transferred to the US pursuant to the Safe Harbour Decision.[69] The CJEU used the terms 'storage of data on a generalised basis'[70] and 'access to data on a generalised basis'[71] to describe the bulk collection of data and unrestricted access to the data by public authorities, respectively. In *Tele2*, the CJEU used the terms 'general and indiscriminate retention of electronic communications data',[72] *'generalised retention'*[73] and 'access not restricted genuinely and strictly to one of the [specified] objectives'.[74] Korff *et al.* used the term 'generic access to communication data' for the purposes of their article, based on the CJEU's terminology in *Schrems*.[75]

The great variety of terms used highlights that what one deems appropriate terminology depends on one's point of view. The differences in terminology reflect the varying objectives and perspectives regarding the same or overlapping phenomena. From the intelligence services' point of view, 'signals intelligence' refers to a type of technology used to collect data. This technology is used for a specific ('strategic') purpose, at a given scale (mass/bulk), and within legal boundaries. In this report, FRA uses, to the extent possible, the terminology adopted in national laws, while having

65 FRA (2015a), p. 16.
66 The Netherlands, National Government (*Rijksoverheid*) (2016), Infographic about AIVD and MIVD's method of interception of information (*'Gemoderniseerde Wet op de inlichtingen- en veiligheidsdiensten: extra bescherming veiligheid én privacy'*), Press Release 28 October 2016.
67 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015.
68 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016.
69 European Commission (2000), Commission Decision of 26 July 2000 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, OJ 2000 L 215 (*Safe Harbour Decision*).
70 CJEU, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, 6 October 2015, para. 93.
71 *Ibid.* para. 94.
72 CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, para. 62.
73 *Ibid.* para. 113.
74 *Ibid.* para. 114.
75 Korff, D. et al (2017), p. 14.

Figure 2: Intelligence cycle in the Netherlands



Source: *National government (Rijksoverheid) of the Netherlands, 2016 (original figure available on their website)*

in mind the 'systems' referred to by the European Parliament in its 2014 resolution.[76]

While the FRA 2015 report describes the distinction between targeted and untargeted surveillance in detail,[77] this report covers both types of surveillance by intelligence services.

In the context of general surveillance of communications, distinguishing between targeted and untargeted surveillance can be problematic, given that a target can be defined after collecting and filtering certain data. This in turn raises the question of when an interference with fundamental rights can be established.

Notes on terminology

General surveillance of communications

Intelligence can be collected with technical means and at large scale. This surveillance technique is referred to in different ways, including 'signals intelligence', 'strategic surveillance', 'bulk investigatory powers', 'mass digital surveillance' and 'storage of data on a generalised basis'. Whenever possible, FRA uses the national laws' terminology, but also uses – as a generic encompassing term – 'general surveillance of communications'.

Targeted and untargeted surveillance

Based on whether or not a target exists, surveillance measures can be divided into targeted and untargeted surveillance. 'Targeted surveillance' presupposes the existence of prior suspicion of a targeted individual or organisation. 'Untargeted surveillance' starts without prior suspicion or a specific target.

76 European Parliament (2014), para. 1.
77 FRA (2015a), p. 17-18.

3

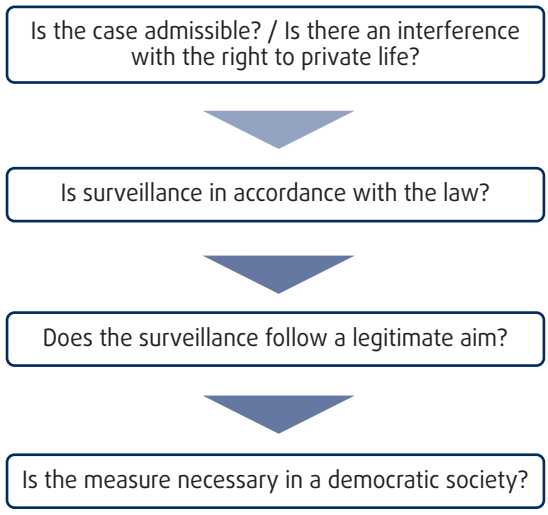
Interference with the right to respect for private life

Surveillance measures and surveillance legal frameworks can ultimately be subjected to the control of the ECtHR. Once domestic remedies have been exhausted, individuals can bring a case before the ECtHR, alleging that surveillance measures are violating their human rights. Before considering whether a particular surveillance measure is justified under the ECHR, the ECtHR will assess whether the applicant can be considered a 'victim' under the ECHR to determine whether their case is admissible.

Due to the necessarily secret character of surveillance measures, applicants always struggle to demonstrate that they were under surveillance. The court often joins the question of whether an applicant can be considered a "victim" (i.e., has victim's status) with the question of the existence of an interference with the right to private life. Figure 3 presents the different stages of the ECtHR's review. This chapter focuses on the definition of the interference with the right to respect for private life.

The ECtHR has held, in the context of examining *in abstracto* claims,[78] that the mere existence of a law permitting surveillance in itself constitutes interference. The ECtHR sets two conditions for deeming legislation that permits surveillance measures an interference

Figure 3: Stages of control by ECtHR in the context of surveillance



Source: *FRA, 2017*

78 ECtHR, *Roman Zakharov v. Russia* [GC], No. 47143/06, 5 December 2015 (Grand Chamber), paras. 229-231; ECtHR, *Kennedy v. United Kingdom*, No. 26839/05, paras. 118-129 and the judgments cited therein.

with a right. First, the scope of the legislation must be such that the applicant can possibly be affected by it. Second, the ECtHR looks at the availability of effective remedies at the national level. If there are no effective remedies, the ECtHR considers interference with the right to private life to occur with the mere existence of legislation permitting surveillance. In practice, once intelligence services intercept a signal and start collecting data, they interfere with the right to private life. The CJEU has followed the same point of view.[79]

ECtHR case law: interference with the right to private life

"[T]he Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. [...] [W]here the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified [...]. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto*, is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 4 December 2015, para. 171*

Under the GDPR, any processing of personal data – including collection of data – amounts to interference. Intelligence services sometimes collect data by requesting telecommunications providers to transfer their customers' data to them. Under EU data protection law, such data collection constitutes an interference.

At the same time, a question arises as to the definition of 'collection' of data. Figure 2 indicates that, in the Netherlands, the collection of data includes the stage when intelligence services extract data from an intercepted signal, filter and, eventually, store it.

Among EU Member States, the general understanding is that the interception of a signal is a form of data collection. This is reflected, for example, in the respective laws of France, Germany and the United Kingdom regarding interception of interception of electronic communications. In France, after foreign electronic communications are gathered from an intercepted signal, their exploitation is subject to authorisation by the prime minister.[80] If communications using connections based on subscriptions from the French territory are identified, these are immediately deleted.[81] Finally, the collected, transcribed or extracted data must be destroyed within a time period specified by law.[82] In Germany, the intelligence services capture telecommunications data and store them without any other prior processing.[83] They must then, within a certain time period, identify the data and delete those not relevant to the purposes for which the surveillance measure was implemented. In the United Kingdom, the intelligence services intercept electronic communications in the course of their transmission.[84] Subsequently, they select certain intercepted data for examination. The selected data are then disclosed to authorised persons.

However, the mere collection of data by intelligence services is not universally accepted as the starting point of an interference with the right to private life. As previously noted, intelligence services store the data they have collected and, when needed, later access them for analysis. Some suggest that an interference begins only when intelligence services actually access and analyse the previously collected data. For example, the governments of the United Kingdom and Ireland argued before the CJEU – in a case concerning

79 CJEU, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger*, 8 April 2014; CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige and Watson v. Home Secretary*, 21 December 2016, para. 100.

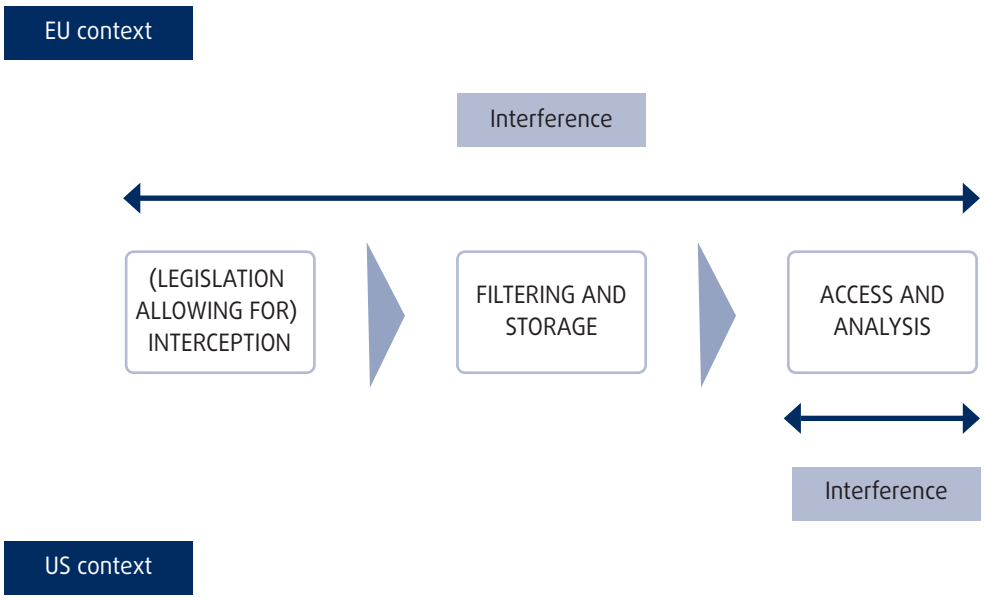
80 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-2.
81 *Ibid.* Art. L. 854-1.
82 *Ibid.* Art. L. 854-5.
83 Germany, Federal Intelligence Act (*Gesetz über den Bundesnachrichtendienst*) (BNDG), s. 2.
84 United Kingdom, Investigatory Powers Act 2016, Part 6, Chapter 1.

the EU-Canada PNR Agreement[85] – that there is no interference until intelligence services start using collected data. The CJEU reaffirmed the position that communication of personal data to a third party, such as a public authority, constitutes an interference with the right to respect for private life, regardless of the subsequent use of the information communicated.[86]

Figure 4 shows the difference in the perception of the notion of an interference in the EU and US contexts. In the United States, an interference is considered to occur when intelligence services use the data, and not when they collect them.[87] In practice, this means that an interference with the right to private life is established when intelligence services access and analyse the previously collected data.

The differences in the understanding of the notion of an interference are important when European courts assess surveillance measures. According to both ECHR and EU law, an interference with the right to private life is established with the existence of legislation allowing for surveillance measures, and this opens the way to a control on the merits of the case. Therefore, European courts consider the mere collection of data by intelligence services to constitute an interference.

Figure 4: Different understandings of 'interference' (EU and US)



Source: FRA, 2017

85 CJEU, *Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, Opinion of the Advocate General, 8 September 2016, paras. 171-172.

86 CJEU, *Opinion 1/15 on the Draft Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, Opinion of the Court (Grand Chamber), 26 July 2017, paras. 124-125.

87 United States, National Research Council (2015), p. 36.

4

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.

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.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The establishment of an interference with the right to private life opens the way for the ECtHR to assess whether it can be justified under the ECHR (see Figure 3). When it does so, the court examines whether the interference:

- is in accordance with the law;
- pursues a legitimate aim; and
- is necessary in a democratic society to achieve that aim.

Given the seriousness of the interference in cases of surveillance, the ECtHR has developed a set of minimum safeguards for interferences to be deemed in accordance with the law. These criteria have been established in the context of targeted surveillance, but they also apply to general surveillance of communications. The court summarised them in *Roman Zhakarov v. Russia*. The CJEU has embraced a similar approach.

ECtHR case law: quality of the law

"[A]ny interference can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which paragraph 2 of Article 8 refers and is necessary in a democratic society in order to achieve any such aim [...].

The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects [...].

The Court has held on several occasions that the reference to "foreseeability" in the context of interception of communications cannot be the same as in many other fields. Foreseeability 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 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 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 [...].

In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in law in order to avoid abuses of power: the nature of 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 destroyed [...]."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 4 December 2015, paras. 227-231*

CJEU on quality of the law

"[N]ational legislation must, first, lay down clear and precise rules governing the scope and application of [...] a data retention measure and imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse. That legislation must, in particular, indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary."

CJEU, Joined Cases C-203/15 and C-698/15, Tele2 Sverige and Watson v. Home Secretary, *21 December 2016, para. 109*

Given the complexity of the issue, it can be difficult for a lay person to understand surveillance legal frameworks. In light of this reality, the ECtHR has not excluded the possibility for a law to be considered sufficiently clear if individuals can obtain the necessary understanding of the law by seeking legal advice.[88]

FRA's fieldwork[89] in seven EU Member States confirmed that expectations for lay persons to understand surveillance legislation – even with legal advice – are unrealistic. Most actors working in the field agree that such legislation hardly meets the standards of clarity and foreseeability. Officials interviewed also deemed such pieces of legislation as particularly complex compared to legislation encountered in other areas of their professional expertise and experience.

"The law governing the intelligence services is difficult to understand, inconsistent and has no regulatory concept."

(Academia)

Interviewees tended to be critical of current legislation. The views most differed by the type of institution represented: the further removed respondents were from the respective oversight system, the more critical they were. In this regard, civil society organisations (mainly represented by legal professionals or lawyers involved in law suits), academics and practicing lawyers were more critical than representatives of oversight bodies or executive control.

Representatives of the aforementioned public institutions tended to be less critical. The data collected provide possible explanations for this perspective. First,

88 ECtHR, *Kafkaris v. Cyprus* [GC], No. 21906/04, 12 February 2008, para. 140 and *Del Rio Prada v. Spain* [GC], No. 42750/09, 21 October 2013, para. 79.

89 Annex 1, section on 'Social fieldwork methodology', presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

representatives of the public administration work with the direct implementation of the laws, which equips them with a better understanding, the ability to provide more explanations, and examples of everyday practices. Also, they work in a specific institutional context and have built up working relationships or cooperation with others in the field. This also helps develop mutual trust with the actors in the field, including intelligence services. They are therefore in a better position to ensure compliance with standards and implementation of best practices.

"But if we put it this way, an ordinary well-educated non-lawyer looking at the legislation would not be able to understand from this that there is such a broad signal intelligence capability and they certainly wouldn't without the benefit of detailed legal advice be able to understand the ramification of what is proposed." (Lawyer)

Respondents nearly unanimously deemed the current legal framework complex – with regard to a variety of characteristics. Some noted that it is difficult to legislate simply in the area of intelligence collection. As a result, legislation is kept 'general', 'vague' or 'obscure'. Some referred to the complexity in terms of recent developments, recent changes (legislative reforms) or the need for changes in the area.

Respondents mentioned that a number of different pieces of legislation regulate the field and oversight, and that legislation sometimes contains cross-references to other legislation or to codes of conduct. As one lawyer put it: 'in terms of different pieces of legislation and institutions, it is quite a jungle out there'. Several respondents mentioned the length of the legislation, particularly the most recent legislation.

Others referred to the need for better definitions of concepts (e.g. related to 'national security'), and fewer vague terms ('it is full of very vague terms, [there is] very little in terms of thresholds') and other inconsistencies or imprecise areas. According to one lawyer, the vague wording leaves a lot of provisions open to interpretation – which is linked to the tendency to 'expand the scope of' the laws.

Adding to the complexity is the lack of cooperation between oversight bodies and inconsistencies across powers for the number of actors involved in the area. For example, some Data Protection Authorities (DPAs) mentioned ongoing discussions on how to reduce the complexity of legislation and suggested that DPAs could shoulder more work, if the necessary powers were attributed to them. According to respondents, the legal framework is also complex because the laws are incomplete (e.g. they do not address technical arrangements for oversight, although they define surveillance techniques).

"[The law] has failed numerous tests in terms of clarity and foreseeability." (Expert body)

The different actors were asked about the clarity of their respective national legal frameworks in terms of the effectiveness of the day-to-day oversight of the work of intelligence services. In relation to the content of the legislation, opinions diverge. More respondents felt that the legal framework lacks clarity than considered it sufficiently clear.

"The main aspects that characterise the law's lack of clarity are the imprecision with which the law on the intelligence services deals with a certain number of issues and the excessively vast scale of the surveillance." (Lawyer)

Respondents who stated that the legal framework lacks clarity noted the vagueness of the laws, e.g. broad definitions of terms, mandates of institutions, and many different ambitions. They considered the laws to be incomplete and in certain cases non-compliant with European case law standards. A lack of consistency and transparency was also mentioned. The definitions provided by the legal text of both the powers and mandate of the intelligence services were considered insufficiently clear. Some believe the [current] lack of clarity is intentional – to ensure the greatest possible freedom to manoeuvre. These respondents called for an improvement of current legal frameworks. Lawyers, civil society representatives and academics tended to be most critical, and more often stated that legislation lacks clarity.

"You read the text and you do not really understand what it means. You read it again, you get a bit of a glimpse, but the cascades of cross-references to other laws hinder your understanding. The terms are vague." (Civil society organisation)

Nonetheless, a significant share of respondents considered the legal framework to be clear. They tended to be representatives of parliamentary committees, expert bodies, and executive control. They noted that certain parts or aspects of the legislation are clearer than others, e.g. no clear division of competences between specific bodies, or some forms of surveillance under the legislation being slightly clearer than others. Institutions with specific mandates tended to find the legislation clear in terms of their own work. For example, data protection authorities, ombuds institutions and expert bodies suggested that the legislation is clear as far as it is related to their specific – and, in most cases, limited – function.

"That legal framework is clear for those who work for the [ombuds institution]. The framework is perhaps less clear to members of the public. There is frequent consultation between institutions to determine which institution is competent to deal with a particular matter." (Ombuds institution)

"Talking about data protection, and not violations of fundamental rights in general, the text of the law, albeit complex, is clear and comprehensible overall."

(Data protection authority)

"The general framework is sufficiently clear and it requires no further adjustments." (Judiciary)

Even though interviewed experts from oversight and executive control institutions from different Member States – e.g. Belgium, France, the Netherlands and Sweden – view the current legislation and oversight setting positively, they acknowledged several problems. Many of these echo the complaints voiced by individuals with overall more critical views. They referred to their respective system as 'quite sophisticated', 'quite unique' and 'very credible', noting that 'the construction is well-thought through'.

However, some stated that, even if clear, the legislation was outdated and needed to be updated (or was in the process of discussion). Some said it was still not able to respond to current situation while implementation of recent legislative reforms which is not yet clear. Respondents often referred to the problem of general inconsistency, fragmentation of the legal framework, and the need to improve current practices in terms of coordination among different institutions. This includes clarifying the division of competences and avoiding overlapping functions. Some respondents also stated that the legislation regulating the oversight of intelligence services lacks clarity.

4.1. Member States' laws on surveillance

In some Member States, the legal basis that frames the intelligence services' mandate and powers consists of one unique legal act governing their organisation and means – Cyprus is a recent example.[90] In others, complex frameworks consisting of several laws and regulations stipulate specific aspects of the services' mandate, organisation, competences or means (e.g. the United Kingdom). However, most Member States organise the work of their intelligence services in two laws: one on their mandate and organisation, the other on means of action and the conditions for using them. For instance, the Act on the Security Services of the Czech Republic sets out the general legal framework for the intelligence services in that Member State. The powers of each intelligence service are further detailed in two separate acts.[91]

A review of legal frameworks regulating surveillance methods used by intelligence services shows that 27 of 28 Member States have codified their use; Cyprus is the exception. In Cyprus, a recently adopted law codifies the existence of operations conducted by intelligence services. However, it does not regulate the surveillance methods used by the intelligence services, nor does it explicitly sanction or prohibit surveillance.[92] In Portugal, a law adopted in July 2017 lays down the conditions for intelligence services to access metadata of an existing target.[93]

As far as general surveillance of communications is concerned, the 2015 FRA report showed that France, Germany,[94] the Netherlands, Sweden and the United Kingdom have detailed legislation governing the use of measures aiming at general surveillance of communications.[95] France, Germany and the United Kingdom have significantly reformed their intelligence laws since 2015. Several other EU Member States have started wide-reaching reform processes – such as Finland, which will be the sixth Member State with detailed legislation on general surveillance of communications if the proposed reform is adopted.

"The reform of the legal framework has been very positive. It has brought clarity and changed the world of intelligence services, changed the approach and the methodology. No more deviated secret services." (Parliamentary committee)

"The [new] legislation is positive to the extent that it makes explicit things which were previously implicit." (Lawyer)

The reforms in the Member States were triggered by various factors. The intelligence services needed to adapt to

90 Cyprus, Law providing for the establishment and functioning of the Cyprus Intelligence Service (*Νόμος που προβλέπει για τη θέσπιση και τη λειτουργία της Κυπριακής Υπηρεσίας Πληροφοριών*) N. 75(I)/2016.

91 Czech Republic, Act on the Security Information Service (*Zákon o bezpečnostní informační službě*), No. 154/1994, 7 July 1994; and Czech Republic, Act on Military Intelligence (*Zákon o Vojenském zpravodajství*), No. 289/2005, 16 June 2005.

92 Cyprus, Cypriot Intelligence Services Act 2016 (*Ο περί της Κυπριακής Υπηρεσίας Πληροφοριών Νόμος του 2016*).

93 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Lei Orgânica n.º 4/2017 de 25 de agosto *Aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de Agosto* (Lei da Organização do Sistema Judiciário).

94 The NSA inquiry committee's report provides additional explanation on the legal framework and its implementation before the 2016 reform: Germany, Federal Parliament (2017a), p. 687 and following.

95 FRA (2015a), p. 20.

new technologies to better respond to new threats (particularly in a counter-terrorism context). Public authorities reacted to the Snowden revelations with enhanced transparency on the intelligence services' powers in an effort to regain the population's trust which had been undermined by the revelations. In the case of Germany, discussions on the legal framework's shortcomings in the NSA inquiry committee prompted legal reform in 2016, even before completion of the committee's report in June 2017. Overall, the reforms contributed significantly to enhanced clarity in the respective laws. Fieldwork participants from the Member States at issue acknowledged that the reforms brought improvements. However, they stated that the lack of clarity – and hence the need for quality legal rules governing the work of intelligence services – remains an issue.

4.2. Targeted surveillance regulated by almost all Member States

Targeted surveillance, as regulated in the Member States' laws, refers to concrete targets (individuals, group of individuals or legal entities) 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 some Member States (e.g. the United Kingdom), a single targeted surveillance measure can cover a considerably wide scope of targets.

In Belgium, the State Security (*Sûreté de l'Etat*) can research, analyse and treat intelligence that is connected with the activities of an individual or a group of individuals who "threaten or could threaten", among others, the state's internal or external security.[96] Such activities are explicitly identified in the Intelligence Services Act: espionage; intrusion; terrorism; extremism; proliferation; harmful sectarian organisations; and criminal organisations.[97]

The definitions of each of these activities are also set out in the law.[98] The Belgian Standing Committee I confirms, via its oversight activities, that the intelligence services have been complying with the requirement to focus their activities on an individual or a group of individuals.[99]

The Belgian law envisages the use of ordinary, specific and/or exceptional methods of surveillance. Within the context of ordinary surveillance measures, intelligence services can request from public authorities the relevant information they need for their missions. They can also access the databases of the public sector.[100] Specific measures are comparatively more intrusive into individuals' private life. They include identification or localisation, by technical means, of the services and electronic communication methods to which an individual is subscribed. The intelligence services may request this information from telecommunications providers. The collection of electronic communications data, such as the location of the recipient of a call, is also considered a specific measure.[101] The most intrusive targeted surveillance methods in Belgium are exceptional measures. These permit intelligence services to interfere with a computer system or listen to and record electronic communications.[102]

In Italy, the law does not explicitly distinguish among the methods of surveillance depending on the threat. The Agency for information and external security (*Agenzia informazioni e sicurezza esterna*, AISE) and the Agency for information and internal security (*Agenzia informazioni e sicurezza interna*, AISI) may carry out tapping activities and preventive controls on communications – such as interception of phone calls and e-mails – "when these are deemed essential for performing the tasks assigned to them".[103] The surveillance methods are similar to those used in judicial proceedings. The tasks assigned to AISE and AISI are set out in legislation.[104] The intelligence services may use surveillance methods only to ensure the defence of the independence, integrity and security of the Republic from foreign threats or the defence of the internal security of the Republic and its democratic institutions from all kinds of threats, subversive activity and forms of criminal or terrorist aggressions. Nevertheless, the use of surveillance measures is allowed only where applied to a single target or a group of targets previously specified by the intelligence services.[105]

In the United Kingdom, a targeted interception warrant is not necessarily related only to a single person or set of premises. The target can be "a group of persons who

96 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 8 (1).
97 *Ibid.*
98 *Ibid.* Art. 8 (1) (a) – (g).
99 Belgium, Standing Committee I (2015), pp. 20-21.
100 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 14.
101 *Ibid.* Art. 18 (2) and (3).
102 *Ibid.* Art. 18 (10).
103 Italy, Implementing provisions of the Code of Criminal Procedure *(Disposizioni di attuazione del codice di procedura penale)*, Art. 226 read in conjunction with Italy, Legislative Decree no. 144 of 27 July 2005, Art. 4 converted into Law no. 155 of 31 July 2005, as amended.
104 Italy, Law no. 124 of 3 August 2007 on "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*), Arts. 6-7.
105 Italy, Implementing provisions of the Code of Criminal Procedure *(Disposizioni di attuazione del codice di procedura penale)*, Art. 226.

share a common purpose or who carry on, or may carry on, a particular activity" or "more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation".[106] This type of targeted interception warrant can be called 'thematic'.[107] The potential scope of thematic interception warrants can be quite broad given that the "[d]escriptions of persons, organisations or sets of premises [in the warrant] must be as granular as *reasonably practicable* in order to sufficiently enable proper assessment of the proportionality and intrusion involved in the interception."[108]

In Portugal, a recently adopted law grants powers to the intelligence services to conduct targeted surveillance. It allows for the intelligence services to access source and equipment location data retained by telecommunication providers for the purposes of ensuring national defence, internal security and prevention of acts of sabotage, espionage, terrorism, proliferation of weapons of mass destruction and highly organised criminality. Such measures cannot exceed the duration of three months and can be deployed exclusively in relation to a concrete operation, involving specific targets. The law explicitly bans real-time network traffic surveillance.[109]

4.3. Member States reform legislation on general surveillance of communications

The 2015 FRA report showed that five Member States – France, Germany, the Netherlands, Sweden and the United Kingdom – detail the conditions that permit the use of both targeted and untargeted surveillance.[110] This report focuses on these same five Member States when discussing detailed legislation on general surveillance of communications. FRA's selection is based on the fact that this type of collection is prescribed, in detail, in the law. The list of five Member States is in no way exhaustive, in the sense that other Member States' laws might allow for general surveillance of communications – but they do not regulate it in detail.

In Italy, for example, a Decree-Law of 2015 gives AISE authority to perform its tasks also by electronic means (*assetti di ricerca elettronica*). The law does not provide more details about these surveillance means; it only states that it should be exclusively directed abroad.[111]

In some cases, a lack of clarity on a provision's scope can prompt courts to deem it unconstitutional. The French constitutional court reached this conclusion when assessing a clause on surveillance and control of radio transmissions (Article L. 811-5 of the Interior Security Code).[112] A June 2017 bill tries to address this issue, clarifying the scope of the surveillance technique and its oversight.[113]

Other Member States do not explicitly permit civil intelligence services to engage in general surveillance of communications. For example, in Belgium, the law grants no general surveillance of communications' powers to the civil intelligence service (State Security – *Sûreté de l'Etat*). Only the military intelligence service (General Intelligence and Security Service – *Service Général du Renseignement et de la Sécurité*) – not covered by this report – has these powers.[114]

In the United Kingdom, the Investigatory Powers Act (IPA) received royal assent in November 2016, and its various provisions have started entering into force since 30 December 2016. At the time of writing, not all provisions of the IPA were fully in force; these will be brought into force in due course by means of regulations implemented by the Secretary of State. The IPA largely – but not entirely – replaces the Regulation of Investigatory Powers Act 2000 (RIPA). Therefore,

106 United Kingdom, Investigatory Powers Act 2016, s. 17 (2).
107 Anderson, D. (2016), p. 21.
108 United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', 23 February 2017, para. 5.13.
109 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Art. 2-5.
110 FRA (2015a), p. 20 and following.
111 Italy, Legislative Decree No. 7 of 18 February 2015 converted, with amendments by law of 17 April 2015, No. 43, Art. 8. See also Italy, COPASIR (2017), p. 11 and 18. For Poland, see Poland, Act on Internal Security Agency and Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*), 24 May 2002, Art. 5.1 which mentions "electronic surveillance" (prowadzenie wywiadu elektronicznego) as a task of the Internal Security Agency. This task is not further regulated in the law, making it difficult to describe the nature of such type of surveillance. The same law prescribes that "the Agency is competent to access metadata (telecommunication and internet data) in order to complete its tasks". Moreover, another task of the Internal Security Agency is to investigate, prevent and detect crimes "harming the economic foundations of the state". In 2014, the Constitutional Tribunal ruled that such task is not precise enough and violates the Constitution. See Poland, Constitutional Tribunal, case no. K 23/11, 30 July 2014.
112 France, Constitutional Court (*Conseil constitutionnel*), La Quadrature du Net and Others, Decision 2016-590 QPC, 21 October 2016. See also France, CNCTR (2016), p. 48 and following and France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 72 and following.
113 France, Bill reinforcing internal security and the fight against terrorism (*Projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme*), 22 June 2017.
114 Belgium, Organic law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), Arts. 44 and 44/1 to 44/5.

two pieces of legislation on surveillance powers are currently in force.[115]

> *"RIPA, 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."* Anderson, D. (2015), para. 35

A legislative reform proposal in its very early stages in Finland aims to introduce a detailed legal framework on general surveillance of communications, which would make it the sixth Member State with such legislation if the proposal is adopted. In its current form, the proposal grants powers to the Finnish intelligence services to conduct 'electronic surveillance of network communications' both in Finland and abroad. Such collection of intelligence can only be carried out to counter certain outlined activities that threaten national security and by using specific search criteria, subject to judicial authorisation. The proposal also creates a new independent and autonomous authority, the Intelligence Ombudsman. The Intelligence Ombudsman would be responsible for overseeing the legality of the use of intelligence collection methods and the observance of fundamental rights in surveillance activities. The Intelligence Ombudsman would have an extensive right to access information and necessary documents as well as to conduct inspections on the premises of the intelligence services. The Intelligence Ombudsman would also have the competence to order the suspension or termination of the use of a certain surveillance technique due to illegality. In such a situation, the court that authorised the initiation of the surveillance measure would issue the final decision on whether the measure could be continued.[116]

FRA's analysis further shows that general surveillance of communications of suspects can take place both within and outside the Member State. The safeguards established in the legislation differ for domestic- and foreign-focused surveillance measures. When intelligence services conduct surveillance domestically, the applicable legal safeguards are enhanced comparing to those in place for foreign surveillance.

Enhanced safeguards in place for domestic surveillance

An analysis of the detailed legal frameworks allowing for domestic general surveillance of communications reveals that legislators have decided to adopt enhanced safeguards for this type of surveillance. Among the five Member States having detailed legislation on general surveillance of communications, three allow for domestic surveillance: France, Germany and the United Kingdom. Restrictions on the permitted techniques for domestic surveillance differ among the countries based on citizenship criteria (Germany) or territorial criteria (United Kingdom and France). Additionally, the intelligence services must obtain warrants approved by the judiciary or expert bodies.

In Germany, the Basic Law (*Grundgesetz*) permits, in select circumstances, restrictions of the inviolability of the privacy of correspondence, post and telecommunications: "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."[117]

The 'strategic restrictions' prescribed by the *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* (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. 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).[118] 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.[119] In 2015, for example, the BND established a list of 1,762 selectors in the context of international terrorism to be applied on 1,132 telecommunication channels (email, voice recognition (*Spracherfassung*), data sets of metadata (*Verkehrsdatensätze*), and SMS); of these, only 41 turned out to be useful from an intelligence point of view.[120] The selectors should not contain any distinguishing features leading to a targeted telecommunication connection nor affect the core area of the private sphere. Different restrictions apply to communications outside Germany, unless they involve German citizens.[121] The list of selectors and the overall request for surveillance is controlled *ex ante* by

115 United Kingdom, Investigatory Powers Act 2016, Explanatory memorandum.
116 Finland, Ministry of Interior (2017), pp. 301-303.
117 Germany, Basic Law (*Grundgezetz*), Art. 10 (2).
118 See Huber, B. (2013), p. 2573.
119 Germany, G 10 Act, s. 10 (4).
120 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 8.
121 Germany, G 10 Act, S. 5 (2). See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1236 and following. 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.

the G 10 Commission, which decides whether the measures are permissible and necessary.[122] The surveillance order is valid for a renewable three-month period.

In 2015, the G 10 Act was further amended to increase the surveillance powers of the intelligence services: surveillance may now also be launched against individuals suspected of having planned or committed cybercrimes. The same amendment also provides that the BND may monitor international telecommunication to and from Germany to detect and respond to international cybercrime.[123]

In the United Kingdom, the Investigatory Powers Act 2016 provides an updated framework for the use of 'bulk' investigatory powers to obtain communications and communications data by the intelligence and security services.

Promising practice

Requesting independent reviewer to scrutinise surveillance powers

In the United Kingdom, while the Investigatory Powers Act was debated in parliament, the Home Office requested the Independent Reviewer of Terrorism Legislation, then David Anderson QC, to review the operational case for bulk powers. With a point of view independent from government and the ability to access secret national security information, the Independent Reviewer explained how bulk powers are currently used by the intelligence services; their importance to national security; the safeguards in place; potential changes the Investigatory Powers Bill brings; and recommendations for better adaptation of the intelligence collection techniques to the new threats and technologies.

For further information, see Anderson, D. (2016)

The powers that can be used domestically cover the retention and acquisition of electronic communications data,[124] and the retention and examination of bulk personal datasets.[125] For the purposes of this research, obtaining communications should be understood as 'obtaining the content of the communications' whereas obtaining of communications data should be understood as 'obtaining metadata' within the meaning of the definition included in the proposal for an e-Privacy Regulation (see box on EU legal terminology).

Note on terminology: EU law

'Electronic communications metadata'

"'[E]lectronic communications metadata' means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication."

'Electronic communications content'

"'[E]lectronic communications content' means the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound."

European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), *COM (2017) 10 final, Brussels, 10 January 2017, Art 4 (3) (c) and Art. 4 (3) (b).*

'Bulk acquisition' refers to the power of the intelligence services to require a telecommunications operator to retain communications data and disclose these to the intelligence services, as well as to select for examination the acquired communications data, as specified in the warrant.[126] Essentially, the telecommunications providers transfer the "who", "where", "when", "how" and "with whom" of communications, but not what was written or said. It includes information such as the identity of a subscriber to a telephone service or a detailed telephone bill. The bulk acquisition technique can be applied domestically, but the intelligence services may only collect communications data and not the content of the communications.[127] The bulk acquisition power originally derives from section 94 of the Telecommunications Act 1984.[128] The NGO Privacy International challenged the bulk acquisition powers under this provision before the Investigatory Powers Tribunal (IPT) – the specialist court of the United Kingdom for surveillance matters. The IPT ruled that until 4 November 2015 – when stricter safeguards were introduced – the intelligence services were violating the

122 Germany, G 10 Act, s. 15 (5).
123 *Ibid.* s. 5 (8).
124 United Kingdom, Investigatory Powers Act 2016, ss 158 – 175. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
125 *Ibid.* ss. 199 – 226. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
126 *Ibid.* s. 158 (6). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
127 *Ibid.* s. 158(6). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
128 For a description and assessment of the original bulk acquisition powers, see United Kingdom, IOCCO (2016b). See also United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 8 September 2017, paras 14-17.

right to private life (Article 8 of the ECHR).[129] Anderson provides an example of the use of bulk acquisition powers by the Security Service MI5: a threat was made by telephone against an overseas embassy in London. The Security Service used bulk acquisition data to identify the user of the telephone as a known hoaxer.[130]

Bulk personal datasets are sets of "information that includes personal data relating to a number of individuals"[131] and "the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions".[132] In simple terms, bulk personal datasets are sets of information about a large number of individuals, the majority of whom will not be of any interest to the intelligence services. However, the intelligence services will only look at the data relating to the minority who are of intelligence interest.[133] The use of bulk personal datasets by the intelligence services was disclosed for the first time in a 2015 report by the Intelligence and Security Committee of Parliament.[134] Privacy International challenged them before the IPT and, as for the bulk acquisition powers, the IPT found that the intelligence services violated the right to private life until 12 March 2015, when stricter safeguards were introduced.[135] Anderson provides an example of the use of bulk personal datasets following the attacks in Paris and Brussels: the Secret Intelligence Service (SIS) worked in partnership with MI5 and the Government Communications Headquarters (GCHQ) to identify individuals in so-called Islamic State of Iraq and the Levant networks who posed a threat to the United Kingdom. SIS used bulk personal datasets to identify a number of such individuals.

The United Kingdom's intelligence services, before exercising one of the 'bulk' powers, must obtain a warrant authorised by the Secretary of State and approved by a Judicial Commissioner. The warrants must specify the operational purposes for which any communications data obtained under the warrant may be selected for examination. The acceptable purposes for a warrant to be obtained are: national security; prevention or detection of serious crime; and the economic well-being of the United Kingdom, provided that this is related to the interests of national security.[136]

Promising practice

Explaining surveillance laws in codes of practice and on intelligence services' websites

In the **United Kingdom**, the government presented publicly to Parliament plain language draft codes of practice to explain each of the different forms of investigatory powers. Following a consultation process, they will be published in final form. In addition, the Secret Intelligence Service (SIS), the Security Service MI5 and GCHQprovide an easy-to-read explanation of the intelligence techniques' legal framework on their respective websites. They provide simple definitions of bulk investigatory powers, allowing individuals to better understand the law. This effort aims to increase transparency on the work of the intelligence services.

For further information, see the websites of the SIS, MI5 and GCHQ

The 2015 FRA report presented the domestic general surveillance of communications technique introduced in 2015 in France.[137] The law envisaged a potential obligation on telecommunications providers to detect terrorist threats with the use of 'algorithms' on their customers' connection data.[138] The CNCTR adopted a detailed opinion specifying what should be understood by 'connection data'.[139] For the purposes of this research, it should be understood as 'metadata'. In July 2016, the CNCTR gave a classified opinion to the prime minister on the planned general architecture of the algorithm.[140] By March 2017, the intelligence services had yet to ask the CNCTR to give an opinion on their use of this surveillance technique, meaning this surveillance technique had not yet been used by that point.[141]

French law also provides for the use of 'IMSI catchers' by intelligence services. These are a type of technical equipment that allows data to be collected, potentially identifying users of mobile phones and the location of devices via their SIM card numbers. The maximum

129 United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 17 October 2016.
130 Anderson, D. (2016), p. 170.
131 United Kingdom, Investigatory Powers Act 2016, s 199 (1) (a). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
132 *Ibid.* s. 199 (1)(b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
133 *Ibid.* s. 212. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
134 United Kingdom, Intelligence and Security Committee of Parliament (2015), Chapter 7.
135 United Kingdom, Investigatory Powers Tribunal, [2016] UKIPTrib 15_110-CH, 17 October 2016.
136 United Kingdom, Investigatory Powers Act, Chapters 1 -3.
137 FRA (2015a), pp. 23-24.
138 France, Interior Security Code (*Code de la sécurité interieure*), Art. L. 851-3.
139 France, CNCTR (2016), p. 120 and following. See also France, Interior Security Code (*Code de la sécurité intérieure*), Art. R. 851-5.
140 France, CNCTR (2016), p. 40.
141 France, DPR & CNCTR (2017), p. 51.

number of IMSI catchers that can be used simultaneously is set by the prime minister, following an opinion on the matter by the CNCTR.[142]

Safeguards in case of foreign surveillance

In all five Member States that have detailed legislation on general surveillance of communications, their respective laws provide for lower safeguards for foreign-focused general surveillance of communications than for domestic surveillance. All five permit their intelligence services to perform foreign surveillance. As noted, for Germany, the citizenship criterion is crucial; however, the prior authorisation procedure applicable to foreign surveillance requires the intelligence services to disclose less information to the approving body than for domestic surveillance. In the United Kingdom and France, compared to domestic surveillance, there is no such safeguard banning the collection and access to communications content.

In Germany, since 2016, the law on the federal intelligence service (BNDG) regulates the federal intelligence service's (BND) surveillance of foreign-foreign telecommunication. The reform adapted the legal framework to take into account technological evolution. The relevant sections were incorporated into the BND Law to highlight that German constitutional protection (Article 10 of the Basic Law) does not extend to these type of data.[143] The data can be intercepted outside Germany, through cooperation with foreign services or at German communication hubs and via satellite interceptions.[144] However, the law imposes the safeguard that only a foreigner's telecommunications may be intercepted. In practice, the BND is authorised to collect and process any foreign telecommunication content data (as well as metadata) from telecommunication networks if such data are deemed necessary to detect and pre-empt, among others, "threats against internal or external security".[145] Section 6 (4) of the BNDG prohibits the BND from collecting and processing data on German citizens outside Germany. Communications of EU institutions, public institutions in the EU Member States, and EU citizens can be intercepted in the counter-terrorism and non-proliferation context or if they provide important information on third countries.[146]

The telecommunication networks to be targeted must be ordered by the Federal Chancellery in advance, with effect for no more than nine months, and approved by a newly established oversight body, the Independent Committee (*Unabhängiges Gremium*).[147] The selectors established by the head of the BND to search the flow of telecommunication data must be aligned with the interests of German foreign and security policy. The Federal Chancellery needs to be informed.[148]

In the United Kingdom, the 'bulk' powers that require a foreign-focus under the Investigatory Powers Act are bulk interception of telecommunications data[149] and bulk equipment interference.[150]

'Bulk interception' is the power of "interception of overseas-related communications"[151] and "obtaining secondary data from such communications".[152] Essentially, the intelligence services tap undersea fibre optic cables landing in the United Kingdom to intercept their traffic. Anderson provides the following example of the use of bulk interception powers: after the disruption of a United Kingdom-based terrorist cell, GCHQ and MI5 continued to investigate its potential overseas links. GCHQ had been analysing data obtained through bulk interception warrants to look for patterns of behaviour indicative of operational planning. They identified an email address that was in contact with a United Kingdom-based individual. Analysis of the communications data and content of these emails revealed more members of the United Kingdom network and details of the attack plot.[153]

'Bulk equipment interference' covers a range of techniques involving interference with electronic equipment. This includes computers, electronic storage devices and smartphones for the purpose of obtaining communications or other information. The bulk equipment interference techniques are colloquially referred to as "hacking or the implantation of software into endpoint devices or network infrastructure

142 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 851-6. See also France, CNCTR (2016), p. 41.
143 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1245 and following.
144 See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1236 and following, Wetzling, T. (2017), p. 2 and 16.
145 Germany, BNDG, S. 6.
146 *Ibid.* S. 6 (3) and (7).
147 *Ibid.* S. 9 (4).
148 *Ibid.* S. 9 (2).
149 United Kingdom, Investigatory Powers Act 2016, Part 6 Chapter 1. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
150 *Ibid.* Part 7. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
151 *Ibid.* s. 136 (2)(a). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
152 *Ibid.* s. 136 (2)(b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
153 Anderson, D. (2016), p. 159.

to retrieve intelligence, but may also include, for example, copying data directly from a computer".[154] Bulk equipment interference requires a foreign focus.[155] MI5 suggests that bulk equipment interference "can be sometimes the only method by which [they] can acquire the data" and "plays an important role in making up for the loss of intelligence that may no longer be obtained through other techniques, such as interception." Prior to the IPA's entry into force, the bulk powers interference technique was never used in the United Kingdom.[156]

The French parliament adopted the Law on international surveillance in November 2015.[157] The Constitutional Court reviewed the bill and confirmed its constitutionality.[158] The law entered into force on 2 December 2015, amending the Interior Security Code. International surveillance shall pursue the same aims as national surveillance, as defined in Article L. 811-3 of the Interior Security Code.

However, the procedure is different. Article L. 854-2 prescribes three scenarios.[159] First, the prime minister can authorise the surveillance of international communication networks, without time limitations. Second, based on a request by a minister, the prime minister can authorise the exploitation of untargeted metadata collected on international communication networks. According to Warusfel, this type of measure is similar to those done via algorithms at the national level and amounts to 'mass surveillance'.[160] Third, the prime minister can authorise the exploitation of targeted content data and metadata. The law provides for the prime minister to issue authorisations without a prior opinion by the CNCTR. The French oversight body only performs *ex post* controls over the implemented measures.[161] Interestingly though, since May 2016, pursuant to a request by the prime minister, the CNCTR agreed to deliver *ex ante* opinions on requests for the exploitation of collected data.[162] After a one-year trial phase, this informal temporary agreement was extended in March 2017.[163]

The French legal framework defines international communications as communications sent or received from abroad. They should transit on French soil.[164] As soon as a communication can be linked to a French identifier (such as a French telephone number), the data are immediately destroyed, unless the person is already under surveillance or represents a threat to the nation.[165] Furthermore, MPs, lawyers, judges and media professionals working in France cannot be placed under surveillance when travelling abroad.

In the Netherlands, the new Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) extends the powers of the intelligence services to intercept network traffic, email and phone communications. The new legislation permits the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst*, AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst,* MIVD) to use several surveillance techniques; however, this report does not deal with military intelligence services. Most importantly, the law enables the services to perform "investigation-mandated interception" of data.[166] For the purposes of this law, "interception" means tapping, receiving, recording and monitoring in a targeted manner any form of telecommunication or data transfer through automated means, irrespective of where this takes place.[167] This includes the power to undo the encryption of conversations, telecommunications or data transfers. An explanatory memorandum states that investigation-mandated interception of data targets certain geographical areas and certain data streams.[168] Essentially, the investigation-mandate interception of data is a form of general surveillance of communications to the extent that it does not provide any limits to the amount of data that can be intercepted or the size of the targeted geographical area. Within the power of the investigation-mandated interception of data, AIVD can demand telecommunications service providers to transfer their customers' data to AIVD.[169] The providers do not have any discretion. To exercise these powers,

154 *Ibid.* p. 34.
155 United Kingdom, Investigatory Powers Act 2016, s 176(1)(c). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
156 Anderson, D. (2016), p. 184.
157 France, Law No. 2015–1556 on international surveillance (Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales), 30 November 2015.
158 France, Constitutional Court (*Conseil constitutionnel*), No. 2015-722 DC, 26 November 2015.
159 France, DPR & CNCTR (2017), p. 53 and following.
160 See Warusfel, B., *in* Gohin, O. and Latour, X. (eds.) (2016), p. 353.
161 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-9.
162 *Ibid.* Art. L. 854-2 (III).
163 France, CNCTR (2016), p. 45 and 47. See also France, DPR & CNCTR (2017), p. 54.
164 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 71.
165 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 854-1.
166 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 48.
167 *Ibid.*
168 The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (*Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie*) (2016), Draft Act on the Intelligence and Security Services 20... (Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..), Explanatory Memorandum.
169 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 53.

the intelligence services need prior ministerial authorisation. The prior authorisation must also be examined by the Assessment Committee on the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden*).

The 2015 FRA report presented the foreign general surveillance of communications techniques available to the National Defence Radio Establishment (*Försvarets Radioanstalt*) in Sweden, which have not been subject to legislative reform since 2015.[170] The law provides for the interception of signals from cables crossing Swedish territory, at the request of specific public authorities, following judicial approval.

170 FRA (2015a), p. 23.

5 Legality in case of international intelligence cooperation

With the globalisation of conflicts and the common transnational feature of threats such as terrorism, the benefits of international cooperation are well established. To achieve their goals, intelligence services may need specialist resources or access they do not have nationally, such as to acquire data that neither their domestic nor foreign intelligence operations can provide. To this end, EU Member States may establish partnerships with each other and with non-EU intelligence services through international intelligence cooperation. International intelligence cooperation is a very sensitive, complex and secretive field, as it touches closely on states' sovereignty, and leaks or miscommunication can result in serious diplomatic crises. Very few countries disclose information on international cooperation, its processes, and existing safeguards intelligence services are expected to follow. However, recent scandals, growing media interest, academic and civil society publications as well as the explosion of the use of big data techniques have hastened a global trend of increased transparency in this area as well.[171] This section analyses the legality and transparency principles currently in force in EU Member States.

The necessity of international cooperation

"International cooperation between intelligence services is indispensable in view of the diverse global security policy challenges. If intelligence services' exchange of personal data were prohibited, intelligence services would be incapable of acting in many areas."

Germany, Federal Parliament (Deutscher Bundestag) *(2017b), p. 1236 [FRA translation]*

All EU Member States have established such arrangements to greater or lesser degree. A number of EU Member States belong to communication networks for purposes of intelligence cooperation, which link them among themselves or with non-European countries (such as, for instance, the SIGINT Seniors Europe, SSEUR).[172] International intelligence cooperation – be it bilateral or multilateral – is normally based on international and/or bilateral agreements delimiting the scope of the collaboration. These agreements may focus on a thematic aspect of the data and techniques on which the operational cooperation will take place, such as joint operations, technical support or exchange of classified information, coordinating the fight against terrorism, or cooperation on criminal matters.[173] An important addition in recent years is intelligence cooperation for the purpose of cyber security.[174] The following section details how, and to which extent, international intelligence cooperation is legally grounded in EU Member States' legal frameworks.

UN good practices on intelligence sharing laws

Practice 31. Intelligence-sharing between intelligence agencies of the same State or with the authorities of a foreign State is based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

171 See Kojm, C. in Goldman, Z. and Rascof, S. eds (2016), p. 118 and following.

172 The SSEUR is composed of the Five Eyes (the U.S., the United Kingdom, Australia, Canada and New Zealand), and France, Germany, Spain, Italy, Belgium, the Netherlands, Denmark, Norway and Sweden. See Germany, Federal Parliament (2017a), p. 197.

173 Born, H., Leigh, I. and Wills, A. (2015), pp. 29-30.

174 Omand, D. (2014), in Duyvesteyn, I., de Jong, B., van Reijn, J. eds, pp. 14 and following.

Almost all Member States (27 out of 28) have established international intelligence cooperation in their national legal frameworks, defining and thereby regulating competences of intelligence services – either by granting them the authority to establish international cooperation or instructing them to enter into international partnerships. Examples of Member States with laws imposing a duty on intelligence services to cooperate with foreign partners include Belgium,[175] Latvia,[176] Luxembourg,[177] the Netherlands[178] and Portugal.[179] It is not apparent from the Maltese legal framework whether international intelligence service cooperation is prescribed by law: international exchange of data is indirectly referred to as being 'sensitive information', in cases where disclosure has not been consented to by the foreign government and cannot, consequently, be disclosed to the Security Committee.[180]

Very few Member States have explicitly articulated the modalities for both establishing and implementing international cooperation within the enabling laws. For instance, Article 59 of the Act on the Security Intelligence System of the Republic of Croatia provides that "the National Security Council shall approve the establishment and termination of cooperation with individual foreign agencies, on the basis of a proposal from the heads of security and intelligence agencies, and after obtaining the opinion of the Council for Coordination of Security and Intelligence Agencies."[181]

Few Member States have detailed laws describing the procedure intelligence services must follow to implement international cooperation. Germany, for instance, does have such laws.[182] Several Member States – Belgium,[183] Denmark,[184] Germany,[185] Latvia,[186] Lithuania,[187] the Netherlands,[188] Portugal,[189] and the United Kingdom[190] – have provided for the establishment of internal rules to be followed when exchanging information internationally. These internal procedural documents are drafted either by the services (Belgium, the Netherlands and Portugal) or by the executive (Latvia, Lithuania, and Poland). None of these internal guidelines are publicly available.

However, in a few Member States, parts of these internal rules are publicly available. In the Netherlands, for instance, where internal guidelines are classified, the Dutch oversight body (CTIVD) published its first in-depth assessment of these procedures in 2009.[191] In 2016, an updated and revised version of this report also included a detailed presentation of the most recent internal guidelines adopted by the AIVD in 2013 and 2014.[192] In the United Kingdom, general guidelines are also classified, but specific guidelines – on international intelligence cooperation where there is a risk of torture, for instance – are publicly available.[193]

Internal guidance applied by intelligence services might take different forms. In Denmark and Latvia, exchanges of intelligence may take place under specific rules and regulations, drafted by the services in the case of Denmark[194] and the cabinet of ministers in

175 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 20 (1).
176 Latvia, Law on Constitution Protection Bureau (*Satversmes aizsardzības biroja likums*), 5 May 1994, Art. 5 para. 5(3).
177 Luxembourg, Act of 15 June 2004, Art. 3(1).
178 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 88.
179 Poland, Act on the Internal Security Agency and the Intelligence Agency (*Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*), 24 May 2002, Art. 8.
180 Malta, Security Service Act, Art. 14(3).
181 Croatia, Act on the Security Intelligence System of the Republic of Croatia, 30 June 2006, Art. 59.
182 Germany, BNDG, S. 13 and following and Germany, G10 Act, S. 7a. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1274 and following and See Siems, T. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1479 and following.
183 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 20.
184 Denmark, Danish Security and Intelligence Service (PET), Legal Matters – Legislation.
185 See description in Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 504 and p. 509 and following.
186 Latvia, Law on the State Secrets (*Par valsts noslēpumu*), 17 October 1997, Art. 9, para. 7.
187 Lithuania, the State Defence Council (*Valstybės gynimo taryba*), establishes guidelines for international cooperation of intelligence institutions with intelligence and security institutions of foreign states, international organisations and institutions, which are not publicly available.
188 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 88.
189 Portugal, Law 50/2014, 1st amendment to law 9/2007 of 19 February that lays down the Organic law of the Secretary-General of the Intelligence Services of the Portuguese Republic, the Strategic Defence Intelligence Service and the Security Intelligence Service, 13 August 2014.
190 United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 42.
191 The Netherlands, CTIVD (2009), pp. 78-80.
192 The Netherlands, CTIVD (2016a), pp. 14-17.
193 See Born, H., Leigh, I. and Wills, A. (2015), p. 127, and United Kingdom, Cabinet Office (2010), Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees, Cabinet Office, July 2010.
194 Denmark, Danish Security and Intelligence Service (PET), Legal Matters – Legislation.

Latvia.[195] Three Member States – Austria,[196] Bulgaria[197] and Hungary[198] – apply the rules of police international collaboration to the procedures for establishing intelligence international cooperation. But, interestingly, not all Member States in which intelligence services are part of law enforcement authorities use police cooperation procedures. In Finland and Ireland, intelligence services legislation does not specify the procedures to be followed.

The scope of the collaboration is also not clearly detailed in law. For most Member States, international cooperation explicitly refers to both the transfer and the receipt of data, and no distinction is drawn between the two in the laws. Few Member States make an exception to this rule. In the United Kingdom, in a landmark decision, the Investigatory Powers Tribunal held, among others, that the law must specify the conditions for the receipt of data: "any request for, or receipt of, intercept or communications data pursuant [to international intelligence sharing arrangements] is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly"[199] by the government. In Germany, reforms of the intelligence services acts in 2015 and 2016 introduced detailed conditions for Germany's participation in shared databases and the transmission of intelligence data to foreign partners.[200]

UN good practices on external review of international intelligence cooperation agreements

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Very few Member States allow expert bodies to assess international agreements and/or cooperation criteria establishing international intelligence collaboration, either *a priori* or *a posteriori*. Belgium,[201] Luxembourg[202] and the Netherlands do so.[203] In Germany, the Parliamentary Control Panel (PKGr) is informed about the declaration of intent (*Absichtserklärung*) drafted by the services before conducting international cooperation. This declaration of intent, which clearly identifies the objectives, scope, duration and specific guarantees of the cooperation, must be approved by the Federal Chancellery before the cooperation begins.[204] The DPA must also be heard before the establishment of any new databases that share intelligence data with foreign partners.[205]

"There is an accountability gap. You know that all oversight bodies are looking at their national services, no one is looking at how the cooperation of secret services as a whole works out. When our services send the information we look at the ways they apply the rules, we do not know what the other intelligence service will do with it, we always follow one end of the string and the other end is not known."

(Expert body)

Some interviewees critically noted the absence of regulation of international cooperation between intelligence services, both on national and international levels, and its impact on oversight. The exclusion of international cooperation from national legislation was also deemed an 'abnormal situation', an example of under-regulation, and as lacking a legal basis (e.g. 'the [national] framework is satisfactory but lacking an international dimension'). Respondents noted that it also prevents individuals from seeking remedies and reinforces an 'accountability gap' with regard to the use of collection techniques, purposes and use of data. Even when international cooperation is mentioned in national legislation, procedures governing international cooperation and the exchange of intelligence remains vague and unclear. Some respondents stated that international cooperation currently mostly involves bilateral agreements, and that such agreements are the most efficient option.

"It is not at all normal that international cooperation on intelligence is not included in the law. This cooperation not only exists but is desired by the executive. The law should therefore include this in order to enable political control and proportionality, including for reasons of national sovereignty, as this cooperation could lead to a transfer of sovereignty."

(Academia)

195 Latvia, Law on the State Secrets (*Par valsts noslēpumu*), 17 October 1997, Art. 9, para. 7.
196 Austria, International Police Cooperation Act (*Bundesgesetz über die internationale polizeiliche Kooperation, Polizeikooperationsgesetz - PolKG*), BGBl. I Nr. 104/1997, and, Austria, EU Police Cooperation Act (*Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), EU – Polizeikooperationsgesetz, EU-PolKG*), BGBl. I Nr. 132/2009.
197 Bulgaria, Special Intelligence Means Act (*Закон за специалните разузнавателни средства*), 21 October 1997, Art. 34м.
198 Hungary, Act LIV of 2002 on the international cooperation of law enforcement bodies (*2002. évi LIV. törvény a bűnöldöző szervek nemzetközi együttműködéséről*), 1 April 2003.
199 United Kingdom, IPT, *Liberty & Others vs. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, para 53.
200 Germany, BNDG, S. 26-30. See Kutschbach, G. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1415 and following.
201 Belgium, Standing Committee I (2015), p. 24.
202 Luxembourg, CNPD, *Rapport Annuel 2015, pp.* 36-37.
203 Netherlands, CTIVD (2016a).
204 Germany, BNDG, S. 13 (5) and Germany, G10 Act, S. 7a (1).
205 Germany, BNDG, S. 28.

Oversight bodies have in academic publications[206] and at international conferences and public events raised the question of how to regulate international cooperation. For example, a representative of the Dutch oversight body addressed the absence of an international legal framework for international cooperation.

Regulating international cooperation

"And also on a national level [international cooperation] tends to be underregulated. Cooperation criteria are often unclear and there is no independent body involved in authorizing e.g. the exchange of personal data. Yet possible consequences can be far-reaching. Once data is exchanged, it is out of your hands. Foreign partners use your data for purposes you disagree of, e.g. illegal detention or targeting. The last years, secret services have intensified their international cooperation. The exchange of personal data takes place not only in bilateral contacts but increasingly also within a multilateral network, leading to databases and operational platforms. [...] Hence it is very important to start by setting national standards. And to allow national oversight bodies to assess this cooperation. [...] [R]elations between national oversight bodies are very important. Not only to exchange experience and views, but also to identify cross border issues and discuss findings in similar investigations. All within the existing legal mandates."

Bos-Ollermann, H. (2016)

206 Born, H., Leigh, I. and Wills, A. (2015).

6

Surveillance for a legitimate aim: need for 'national security' definition(s)

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".

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 *Roman Zakharov v. Russia*, the legitimate aim test does not create a major issue in the court's case law.

ECtHR case law: a legitimate aim

"[T]he Court considers it clear that the surveillance measures permitted by Russian law pursue the legitimate aims of the protection of national security and public safety, the prevention of crime and the protection of the economic well-being of the country."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015, para. 237

Whether the measures at issue pursue a legitimate aim is rarely questioned by the ECtHR. According to the court, notions like national security – the protection of which is a primary aim of intelligence services – must therefore comply with the 'quality of law' requirements, in particular foreseeability/clarity of the law.

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 Council of Europe Member States, in its case law, the court assigns to the notion of national security various concepts that need to have a factual basis.

It is clear from the examples listed in the box on ECtHR case law on national security that the latter goes beyond the protection of the territorial integrity of a state and protection of its democratic institutions – extending to major threats to public safety and including cyber-attacks on critical infrastructures. In some EU secondary legislation, 'national security' is explained as state security – for instance, in Article 15(1)

ECtHR case law: national security

Throughout its jurisprudence, the ECtHR has accepted, among others, as threats to national security:

- espionage (*Roman Zakharov v. Russia*, *Klass v. Germany*)
- terrorism (*Klass v. Germany*, *Weber v. Saravia*)
- incitement to/approval of terrorism (*Zana v. Turkey*)
- subversion of parliamentary democracy (*Leander v. Sweden*)
- separatist extremist organisations that threaten the unity or security of a state by violent or undemocratic means (*United Communist Party of Turkey v. Turkey*)
- inciting disaffection of military personnel (*Arrowsmith v. United Kingdom*)

Source: Born H. and Leigh I. (2005), p. 30; ECtHR (2013); updated by FRA, 2017

of the *e-Privacy Directive* 2002/58/EC. In other EU secondary legislation – for example, in Article 6(1)(d) of the *Admission of Third-Country Nationals for the Purposes of Studies Directive*[207] – 'national security' is referred to as 'public security'. The CJEU in *Fahimian v. Germany* stated that the concept of 'public security' covers both the internal security of a Member State and its external security.[208] Moreover, in *ZZ v. Secretary for the Home Department*, the CJEU 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 national law.[209]

The 2015 FRA report noted that the concept of national security is not used harmoniously across EU Member States.[210] In Luxembourg, the notion of 'national security' was inserted into the law reforming the intelligence services in 2016, to clarify the difference in the scope of missions of the police and intelligence services.[211]

"National security: all topics of fundamental interest for the stability of the country, unity of the country and safety of its citizens." (Parliamentary committee)

"It is not only military and political security, it is also increasingly infrastructure and economic and financial security. Threats can have a plurality of aspects. […] It includes security of technological infrastructures, cybercrime." (Parliamentary committee)

"The services do not have a monopoly on national security. Other services such as police, customs, etc., also have an essential role to play." (Expert body)

Respondents were asked how national security is defined in their respective legal framework or how it is understood in the context of intelligence. The responses reflected the legal terminology in each Member State and mainly referred to very broad concepts, as examples provided in the cited quotes show. Links were also made to international terrorism, organised crime and anti-democracy groups. Several respondents from expert bodies referred to their mandate as 'seeking the balance between national security and fundamental rights, privacy in particular'. Some of the respondents maintained that clearer definitions would help ('if not positive, at least negative'), including at EU level.

Defining national security: Luxembourg

"[W]e consider as activity which threatens or could threaten the national security or the above-mentioned interests, every activity, individual or collective, deployed domestically or from abroad,

a) which can be related to espionage, interference, terrorism, violent propensity extremism, proliferation of arms of mass destruction or of products linked to defence and technology related to defence, organised crime or cyber-threat to the extent that the latter two are linked to previously-mentioned activities, and

b) which is likely to endanger the independence and sovereignty of the State, the security and functioning of institutions, fundamental rights and civil liberties, the security of individuals and goods, the scientific and technical potential or the economic interests of the Grand Duchy of Luxembourg."

Luxembourg, Law of 5 July 2016, Art. 3(2) [FRA translation]

207 Council Directive 2004/114/EC of 13 December 2004 on the conditions of admission of third-country nationals for the purposes of studies, pupil exchange, unremunerated training or voluntary service, OJ 2004 L 375.

208 CJEU, C-544/15, *Sahar Fahimian v. Bundesrepublik Deutschland*, 4 April 2017, para. 39, C-145/09 *Tsakouridis*, 23 November 2010, paras. 43 and following and *C-601/15, N*, 15 February 2016, para. 66.

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

210 FRA (2015a), p. 24 and following. See also *ECtHR, Regner v. The Czech Republic [GC], No. 35289/11, 19 September 2017*, para. 67.

211 Luxembourg, Law of 5 July 2016 1. reorganising the State Intelligence Service; 2. modifying the Code of Criminal Procedure, the Law of 15 June 2004 regarding the classification of documents and security clearances and the Law of 25 March 2015 setting the regime for the compensation and the conditions for promotion of the State civil servants (Loi du 5 juillet 2016 1. portant réorganisation du Service de renseignement de l'État; 2. modifiant le Code d'instruction criminelle, la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité, et- la loi du 25 mars 2015 fixant le régime des traitements et les conditions d'avancement des fonctionnaires de l'État), Art. 3.

PART II: ACCOUNTABILITY

KEY FINDINGS

A diverse oversight framework

- Oversight bodies have diverse roles, including overseeing the legality of the intelligence services' functioning, their efficiency, policies, and their finances.
- Oversight of surveillance measures is normally undertaken either by the judiciary or an expert body. In 16 Member States, expert bodies are involved in the oversight system, and in 17 Member States, judicial bodies are involved in oversight, generally at the stage of authorising targeted surveillance measures.
- Fieldwork interviews suggest that oversight by expert bodies contributes to the development and improvement of internal safeguards in intelligence services.
- In most Member States, parliaments are to some extent involved in all of these roles. In 21 Member States, one or two specialised parliamentary committees are involved in overseeing the intelligence services.
- In seven Member States, DPAs have the same powers over intelligence services as over all other data controllers. In 11 Member States, DPAs have no powers over intelligence services. In 10 Member States, their powers are limited.

Independence, sufficient resources and powers and public scrutiny

- **Independence:** all 28 Member States include at least one independent body in the oversight of intelligence services. Almost all respondents from oversight bodies confirmed that their institutions are independent, impartial, and resistant to any external influence, including by politicians and the intelligence services. However, some interviewees from civil society and academia questioned the oversight bodies' actual independence.
- **Resources and powers:** oversight bodies in all Member States that have detailed legal provisions on general surveillance of communications can initiate controls on their own initiative. All Member States also provide at least one of their oversight bodies with full access to all relevant data and information. The interviewed experts believe that full access to intelligence information is key to empowering oversight bodies and ensuring effective oversight. However, of the five Member States that have detailed provisions on general surveillance of communications, oversight bodies have some form of binding powers in only three. Representatives of different oversight bodies stated that lack of technical expertise remains one of the biggest challenges in oversight. In all seven Member States covered by FRA's fieldwork, oversight bodies may either include technical experts or can engage them on an ad hoc basis. The fieldwork findings show that the latter is rarely done in practice.
- **Public scrutiny:** in all the five Member States that have detailed provisions on general surveillance of communications, the oversight bodies issue annual reports. Interviewed experts indicated that enhanced transparency is vital.
- The respondents view public scrutiny and transparency as being closely linked with the accountability of oversight bodies. Civil society and academia representatives called for more transparency, deeming the content of issued reports uninformative.
- Respondents emphasised the importance of cooperation among the different national actors and across the different purposes of oversight, regardless of its nature (e.g. prescribed by law or informal exchanges). According to the interviewees, cooperation is vital for effective oversight; it strengthens its transparency and helps overcome possible fragmentation of oversight by contributing to its continuity. The respondents also expressed a great need for both national and international cooperation among oversight bodies.

Whistleblower protection

- Provisions on whistleblower protection are prescribed in the legislation of four of the seven Member States covered by FRA's fieldwork. Interviewees tended to agree that efficient whistleblower protection within the intelligence services requires a specific regime, different than those designed for other governmental institutions.

Continuous oversight

- Twenty-two Member States include an independent authority – judicial or expert – in the authorisation of the use of at least one type of targeted surveillance measure. In six Member States, all types of targeted surveillance measures may be implemented without ex ante oversight by an independent body.
- In the five Member States that have detailed provisions on general surveillance of communications, only three provide for the binding involvement of an independent body in the authorisation of these measures. In the two Member States that do not do so, the oversight bodies also do not have the power to make binding interventions.
- In all five Member States that have detailed provisions on general surveillance of communications, an independent body is tasked with providing for ongoing oversight (oversight of the implementation) of these measures.

Oversight of international intelligence cooperation

- A majority of Member States – 17 out of 28 – do not prescribe oversight of international cooperation among intelligence services. Of the 11 EU Member States that do provide for oversight of such international cooperation in law, three have excluded information originating from foreign services from the scope of oversight; four do not differentiate between the oversight regime for international sharing of data and for domestic sharing of data; and four have limited the scope of the control over information obtained through such cooperation.
- The specific characteristics of international intelligence sharing require Member States to establish safeguards tailored thereto, notably:
  - prior approval of any agreement by the executive (currently in force in 27 Member States),
  - complementary approval by either the executive or the head of the services before the exchange may take place (currently in force in 4 Member States),
  - an assessment of fundamental rights anchorage (currently required in the laws of 3 Member States) or of the existence of equivalent data protection legislation (currently conducted in 2 Member States), and
  - data reliability assessments and the obligation to keep records (currently mandatory in 4 Member States).
- The dominant principle in international cooperation – the 'third party rule' – states that a foreign agency to which intelligence has been transmitted can neither share this information with a third party nor use the data for an objective different from the one for which the exchange was established in the first place. When considered to be third parties, expert bodies are not authorised to access – and therefore, oversee – intelligence data obtained via international cooperation. In some Member States, oversight bodies are increasingly not considered to be 'third parties'.

7 An imperative: control from within

Control v. Oversight

"Oversight should be distinguished from control because the latter term (like management) implies the power to direct an organization's policies and activities. Thus, control is typically associated with the executive branch of government and specifically with the senior management of intelligence services. An example of control, as opposed to oversight, would be the issuance of an executive order requiring an intelligence service to adopt a new priority in international intelligence cooperation, such as counterterrorism."

Born, H., Leigh, I. and Wills, A. (2015), pp. 6-7

The following section describes how controls within the services and by the executive contribute to the services' accountability.

7.1. Control by the services

UN good practices on intelligence services management of personal data

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 (2010), Report of the Special Rapporteur Martin Scheinin

As the UN Special Rapporteur on the right to privacy has highlighted, a mechanism enforcing accountability "needs to be embedded first and foremost within the authorities carrying out surveillance and it needs to be clear who is accountable for compliance".[212] Internal controls within the services may be undertaken by a designated officer or sector, who may be appointed by the services or the executive, and report to them as well. The 2015 FRA report described the situation in various Member States.[213]

In Germany, the NSA inquiry committee's report provides a detailed description of the powers of the data protection officer within the BND. The report highlights the impact of the Snowden revelations on her work. Interestingly, given the lack of awareness on data protection in the technical intelligence department of the BND, the data protection officer launched a project to raise awareness among the staff.[214] The 2016 amendments to the BND Law prescribe specific data protection rules on when collected foreign data need to be destroyed and how long they can be kept.[215] Similarly, in the United Kingdom, GCHQ's staff are continuously instructed and trained in the legal and other requirements of the surveillance legislation, with particular emphasis on human rights requirements. Additionally, there are computerised systems for checking and searching for potentially non-compliant uses of GCHQ's systems and premises.[216] For example, when an authorised person selects a particular communication for examination, this person must demonstrate that the selection is necessary and proportionate; this process is subject to internal audit.[217]

212 UN, Human Rights Council (2017), Report of the Special Rapporteur Joe Cannataci, para. 35.

213 See FRA (2015a), p. 30 and following.
214 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 526 and following.
215 Germany, BNDG, S. 10 and 12. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1271 and following.
216 United Kingdom, IOCCO (2016a), p. 26.
217 United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', February 2017, s. 6.14.

FRA was not able to interview any intelligence service representatives during its fieldwork.[218] However, other research participants – mostly representatives of oversight bodies, but also from the executive – discussed examples of control practices implemented by intelligence services. They mainly argued that expert body oversight contributes to the development or improvement of internal safeguards within the intelligence services to act lawfully. The relationships with the services were described as 'cooperative and not adversarial'. For example, intelligence services ask oversight bodies to be present in certain situations, such as to witness data destruction. The services also sometimes share material that might not be directly related to the specific oversight function but could still be relevant for the oversight bodies. Respondents also noted that oversight helps 'to ensure the greater legitimacy of the records held', and emphasised the importance of internal controls through 'a strong legal department within the services'. They viewed the abovementioned practices as contributing to the clarity and, thus, the legitimacy of the intelligence services.

"We also say how important it is for services to have a strong legal department within the services. It is not only for the outsider to be critical, but for inside." (Expert body)

"Also, 'behind the scene' we are doing a lot for fundamental rights, and 'behind the scene' we are helping the agencies to improve their practices, pointing to the issues that we consider disproportionate, unnecessary etc." (Expert body)

7.2. Control by the executive

Strictly speaking, control by the executive is not part of the oversight system because it is not independent. However, the nature of the involvement of the superintending governmental department concerned – whether Chancellery, Foreign, Interior or Defence Ministry – contributes greatly to the effectiveness of intelligence services' accountability systems. The intelligence services are part of the public administration and, as for every administration and public service, effective control stems from the government itself.

The relevant governmental departments can supervise 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; by authorising or approving specific surveillance measures; or by approving cooperation with other services. As a former director of the French intelligence service (DGSE) puts it: "political control is, first of all, [...] hierarchical control because the services do not work in vacuum but under the authority of the executive".[219]

In the United Kingdom, the intelligence agencies operate by law under the authority of the Secretary of State (for Foreign Affairs for the Secret Intelligence Service and GCHQ, and for Home Affairs for the Security Service), supported by dedicated teams of policy officials with full access to the work of the agencies. In the Cabinet Office, the National Security Secretariat coordinates policies – for example, towards overseas liaisons – and prepares and scrutinises budgets; the Joint Intelligence Committee provides strategic intelligence assessments and recommends intelligence priorities.

In France, a June 2017 reform changed intelligence coordination within the executive. The National Intelligence Council (*Conseil national du renseignement*) has the specific mandate of setting strategies and priorities for the services. It includes the president and the prime minister, ministers, the heads of specialised services if required by the agenda, and the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*). The coordinator is responsible for coordinating the actions of the intelligence services and ensuring efficient cooperation among them. The coordinator also transmits and checks the implementation of the president's instructions to the relevant ministers. Additionally, the coordinator coordinates and develops the initiatives taken by France concerning European and international cooperation in the fields of intelligence and the fight against terrorism. The coordinator proposes to the president the intelligence priorities in the fight against terrorism.[220]

In Germany, the reform of 2016 did not change the Federal Chancellery's supervising role over the work of the federal intelligence service (BND) or the coordinating role over the work of the federal intelligence services.[221] The NSA inquiry committee assessed the Federal Chancellery's capacities when controlling the BND. It supported the views of the PKGr calling for adjusting the Federal Chancellery's supervisory control to allow it to properly perform its controlling tasks.[222] In the meantime, the Federal Chancellery staff has significantly increased to take into account the request adjustments. Still the following quote by a Federal

218 The section on social fieldwork methodology in Annex 1 presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

219 France, DPR & CNCTR (2017), p. 14 [FRA translation].

220 France, Defence Code (*Code de la défense*), Art. R.* 1122-7, Art. R.* 1122-8 and Art R.* 1122-8-1.

221 See Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 536 and following.

222 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1243.

Chancellery staff member nicely illustrates the issues faced by all controllers.

The need to be selective when controlling

"We certainly often also became proactive. But we are, of course, as you rightly point out, as an entity that conducts legality reviews with relatively few employees at the Federal Chancellery trying to accompany a huge authority in terms of administrative and specialised control, not in a position to follow all processes in all departments down to the last detail. We always need and needed to concentrate on key areas."

Germany, Federal Parliament (Deutscher Bundestag) *(2017b), p. 1243 [FRA translation]*

In the Netherlands, the Minister of the Interior, the Minister of Defence and the Minister of General Affairs (the prime minister) are in charge of appointing the coordinator for the intelligence services. The prime minister instructs the coordinator, in agreement with the Minister of the Interior and the Minister of Defence.[223] The coordinator chairs a special committee on the intelligence services composed of representatives of relevant ministries.[224] The heads of the services are under obligation to cooperate with the coordinator.[225] The Minister of Interior reports to parliament annually regarding the work of the AIVD.[226]

In Belgium, the Minister of Justice appoints the head of the service, officers to certain posts, and the internal administrative control. The minister is also in charge of the expenses and discipline of the services.[227]

The 2015 FRA report highlighted the executive's crucial role in authorising/approving surveillance measures in most Member States.[228] In the United Kingdom, officials in the Home Office and Foreign Office scrutinise applications for warrants from their agencies and obtain their own legal advice before submitting advice on the applications to their Secretary of State. In France, members of the executive other than the president of the republic or prime minister may also exercise control over the intelligence services. Furthermore, a 2017 decree specifies that the heads of the intelligence services communicate to the national intelligence and fight against terrorism coordinator the intelligence to be brought to the attention of the prime minister and the president of the republic.[229] The prime minister may hold the services accountable via the Inspectorate of Intelligence Services, whose members the prime minister may appoint from among the personnel of existing inspectorates. This body is in charge of monitoring, auditing, researching, consulting, and assessing the intelligence services, and reports back to the prime minister.[230] While the inspectorate's powers were extended recently, the French parliamentary oversight committee is calling for its further strengthening.[231]

FRA's fieldwork included interviews with representatives of executive control bodies in three Member States (France, Germany, and Sweden). The interviewees described their roles as involving 'internal control in the services' – for example, that procedures and provisions are implemented properly; supervisory functions; acting as advisory to the government; and coordinating the services – for example, facilitating sharing of information between agencies and between government and the services. The experts said that, alongside their main supervisory role, they performed audit or advisory functions. Some said that they supplemented the general oversight system. They noted that they addressed matters as directed by the government, but also exercised their power to take up specific matters on their own initiative.

"The strength of the [national] system is having an independent person who says what is doable and what is not, and the government which decides in fine." (Expert body)

While executive control plays an intrinsic role and should always be informed about the work of the services, it may not have a strong interest in revealing failures that occur due to the potential political costs.[232] Therefore, for accountability mechanisms to provide public reassurance, they must include independent oversight, as well. Control led by the executive is in fact a pre-condition for setting up efficient oversight frameworks – as described in the following section.

223 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) Art. 4.
224 *Ibid.* Art. 5.
225 *Ibid.* Art. 7.
226 *Ibid.* Art. 12
227 Belgium, Organic Law on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, Arts. 4 and 5.
228 FRA (2015a), p. 32.
229 France, Defence Code (*Code de la défense*), Article R.* 1122-8-1.
230 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. See also France, DPR & CNCTR (2017), p. 24.
231 See also France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 24.
232 Born, H. and Wills, A. (eds.) (2012), p. 10.

8 Oversight framework of intelligence services

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.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

To fulfil their mandate, intelligence services need to act in secret and often to use methods that will involve access to personal data and intrude upon personal privacy. In democratic states, this also means the protection of an *open society* through the use of *secret tools*. "It is because of this paradox [...], that the security and intelligence services should be the object of democratic accountability and civilian control".[233] Oversight of intelligence services is one of the conditions of the services' legitimacy.[234]

The oversight on intelligence services is organised in extremely diverse ways in EU Member States. A single model would be an impossible objective because national oversight frameworks have to directly link to the political institutions and administrative and judicial organisation of each Member State.[235] Table 1 is based on a model developed by Cousseran and Hayez and adapted by FRA for comparative analysis purposes. It highlights that effective oversight requires a multiplicity of actors assessing a variety of aspects. However, the essential requirement of an effective oversight framework is that it is comprehensive. Comprehensive oversight requires the oversight of all aspects of the services' work, of which surveillance operations are but one element.

233 Born, H. and Leigh, I. (2005), p. 16. See also France, DPR & CNCTR (2017), p. 2.
234 Cousseran, J.-C. and Hayez, P. (2015), p. 288.
235 See Cousseran, J.-C. and Hayez, P. (2015), p. 291.

Table 1: Oversight framework: main actors and scope of control

Who?/What?	Efficiency	Legality	Policy / specific threats	Fundamental rights protection	Financial integrity and rigour
Parliament	Oversight committee	Oversight committee	Oversight committee & Inquiry commission	Inquiry commission	Financial Commission
Judge	-	Yes	-	Yes	Supreme Court of Auditors
Independent bodies	Expert bodies and State Secrets control body	Expert bodies	Expert bodies	Expert bodies, DPA, ombuds institutions	Special bodies
Watchdogs	Yes		Yes	Yes	Yes

Notes: *The red line indicates the focus of FRA's research.*

Source: *Cousseran, J.-C. and Hayez, P. (2015), p. 292; adapted by FRA, 2017*

8.1. Diversity of oversight mandates

Table 1 shows that the different oversight bodies within an oversight framework have varying purposes, with individual actors focusing on different aspects of the services' functioning. Actors with specifically limited mandates, such as supreme audit institutions, focus on a single task. Others' mandate requires them to undertake broader oversight and assess different aspects. Coordination is therefore needed.

FRA's research focused on two main aspects: legality – a core task of expert bodies – and fundamental rights protection. The review of intelligence policies is indirectly covered, as well. This report does not address the supervision of intelligence services' efficiency, given that this is only indirectly related to fundamental rights safeguards and would require data on surveillance techniques that are confidential. Similarly, this report does not analyse the role of supreme audit institutions, although these are very important for ensuring the financial integrity of, and rigour regarding, public money expenditures.[236]

Scrutinising intelligence services' finances

The Swedish National Audit Office (*Riksrevisionen*), mandated by parliament to audit all state finances, issued a report in 2015 on 'the control of the defence intelligence operations'. The 64-page document addresses four overarching questions: 1) has the government created preconditions for effective control?; 2) is the control conducted effectively?; 3) are the findings of the control reported to the controlled entities and the government?; and 4) are issues raised by the controlling authorities acted upon?

While the assessment is generally positive, it also calls for some improvements. For instance, the report states that the State Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) should be more explicit in its communications with controlled agencies on needed changes and also better document its control methodologies.

Swedish National Audit Office (2015), 'The control of the defence intelligence operations'

In terms of financial supervision over intelligence services, for example, in Germany and France, parliaments adopted original solutions to supervise the services' expenditures in addition to the specialised budget commissions and the Federal Court of Auditors (*Bundesrechnungshof*) and the French Court of Auditors (*Cour des comptes*), respectively.

236 For more information on SAIs, see, for example: Born, H. and Wills, A. (eds.) (2012), pp. 166-175.

The vast majority of specialised parliamentary committees have an ex post say on the effectiveness of budget allocations. Germany, exceptionally, has a separate parliamentary committee in charge of the budget – the Trust Panel (*Vertrauensgremium*), which decides intelligence services' budget and on investment in surveillance technologies. Three Trust Panel members participate in the meetings of the PKGr and three of the members of the PKGr participate in the deliberations of the Trust Panel.[237] The French parliamentary oversight body DPR oversees the expenses of the intelligence services through an annual report prepared by the national intelligence and fight against terrorism coordinator (*coordonnateur national du renseignement et de la lutte contre le terrorisme*)[238] and through the annual report by the Audit Commission on special funds (*Commission de vérification des fonds spéciaux*), which is composed of four members of the DPR.[239]

8.2. Diversity of actors

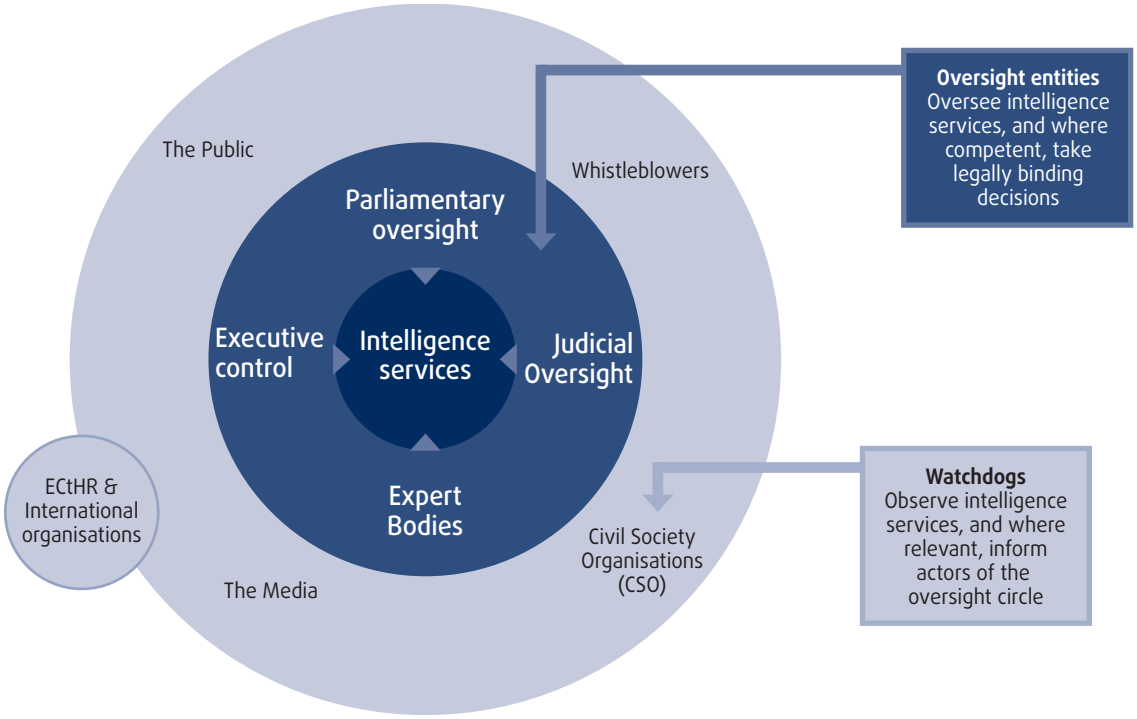
UN standards for oversight bodies

"(E)stablish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."

UN, GA (2016a), Resolutions on the right to privacy in the digital age, *21 November 2016, para. 5(d)*

The following sections introduce the main actors who contribute to the oversight of intelligence services and their accountability (Figure 5): parliaments; expert bodies; and several actors that perform important watchdog functions in democratic societies: media, ombuds institutions, national human rights institutions, civil society organisations and whistleblowers. (Data protection authorities, which are treated as a type of expert body for purposes of this report, are discussed in Section 9.2.)

Figure 5: Intelligence services' accountability scheme



Source: *FRA, 2017*

237 Germany, Federal Budget Order (Bundeshaushaltsordnung), 19 August 1969, as amended, s. 10 (a); and Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, s. 9. See also de With, H. and Kathmann, E., Policy Department C: Citizens' Rights and Constitutional Affairs (2011), p. 225.

238 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 22.

239 *Ibid.* p. 83.

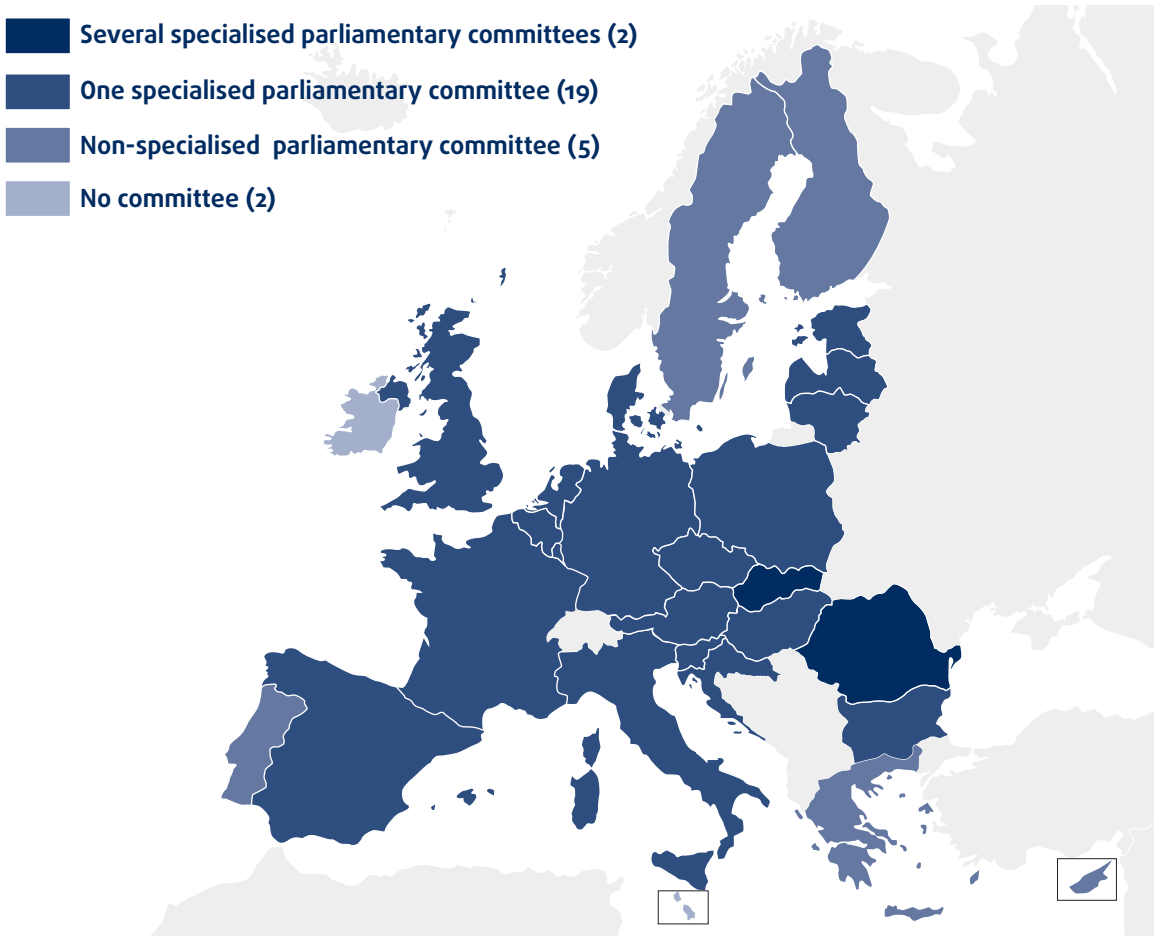
8.3. Parliaments

Parliament has the "supreme responsibility to hold the government accountable".[240] As lawmaker, it is responsible for enacting clear, accessible legislation and establishing the intelligence services and their organisation, special powers and limitations. It also approves the intelligence services' budget and plays a strong role in scrutinising whether their operations are in line with the laws they set out.

As illustrated in Figure 6, 26 EU Member States – all except for Ireland and Malta – provide for parliamentary oversight.[241] In 21 of these, special parliamentary committees oversee the intelligence services. The Venice Commission recommends setting up one parliamentary committee to deal with the various security and intelligence services, since this allows the committee to carry out more far-reaching oversight and to "cross agency boundaries".[242]

In Germany, on 7 December 2016, the Act on the Further Development of Parliamentary Oversight of the Federal Intelligence Services (*Gesetz zur weiteren Fortentwicklung der parlamentarischen Kontrolle der Nachrichtendienste des Bundes*) came into force, amending the Parliamentary Control Panel Act (*Kontrollgremiumgesetz,* PKGrG). It established the office of the Permanent Representative (*Ständiger Bevollmächtigter*), with the task of supporting the regular work and specific investigations of the Control Panel and the Trust Panel.[243] The Permanent

Figure 6: Parliamentary oversight of intelligence services in EU Member States



Source: FRA, 2017

240 Born, H. (2003), p. 36.

241 In Malta, the law establishes a Security Committee, which consists of the Prime Minister, the Minister, the Minister responsible for Foreign Affairs and the leader of the opposition. While introducing a parliamentary aspect, this body seems closer to an executive body. See Malta, Security Service Act 1996, Art. 14 and Schedule 2.

242 Venice Commission (2007), p. 33.

243 Germany, PKGrG, S. 5a. See Bartodziej, P. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1583 and following.

Representative participates in all meetings of the Control Panel, Trust Panel and G10 Commission. These provide the office with a source of information that the member of these bodies do not have. The Permanent Representative supervises the staff working for the Control Panel and the G10 Commission.

"Oversight is not lack of trust, but willingness to clarify."

(Parliamentary committee)

Sweden 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 government must present annual reports to the parliament on the protection of individual persons' integrity in relation to defence signals intelligence activities. These annual reports are reviewed by the Parliamentary Committee of Defence *(Försvarsutskottet)* before it is accepted by parliament.[244] The Committee on the Constitution is also relevant in this context as it is responsible for the areas of fundamental rights, data protection and privacy.[245]

8.4. Expert bodies

Table 2 lists the various expert oversight bodies established in the Member States. It does not include DPAs, but only the bodies specialised in intelligence matters. Across the EU, 16 Member States have set up one or more expert bodies exclusively dedicated to intelligence service oversight.

All five Member States with detailed laws on general surveillance of communications have established one or more expert bodies to oversee this capacity of the intelligence services. However, their mandates are not always comparable. The 2015 FRA report describes their powers.[246] The following paragraph focuses on changes since 2015.

In the Netherlands, the 2017 reform splits the existing CTIVD into two sub-committees: one performing general oversight by conducting investigations and another handling complaints lodged by individuals. The general oversight sub-committee consists of three members, including the chair (also chair of the entire CTIVD), nominated by the responsible ministers for 6 years with once-renewable mandate. The complaints-handling sub-committee consists of a chair and two additional members. At least two of the members of CTIVD the general sub-committee and all members of the complaints sub-committee of the must hold a master's or doctoral degree in law.[247] Currently, the CTIVD is assisted in its work by a staff of 12 persons: the secretary to the Committee, eight review officers, one IT expert and two secretaries,[248] but the Committee will receive an increased budget to be able to implement the new legislation.[249]

In the United Kingdom, the Investigatory Powers Commissioner and the Judicial Commissioners must hold or have held a high judicial office.[250] The number of staff provided to the Judicial Commissioners is subject to the approval of the Treasury, and is provided by the Secretary of State.[251] The Investigatory Powers Commissioner's Office will consist of around 70 staff. This will be made up of around 15 Judicial Commissioners, current and recently retired High Court, Court of Appeal and Supreme Court Judges; a Technical Advisory Panel, of scientific experts; and almost 50 official staff, including inspectors, lawyers and communications experts.[252]

The Investigatory Powers Commissioner has already secured access to in-house legal advice and identified independent standing counsel to facilitate performing his functions, in line with an agreement made with the UK government when the body was set up. The commissioner will have the flexibility to 'buy in' whatever advice he needs at any given time.[253]

In Germany, the G10 Commission carries out expert oversight for matters relating to targeted surveillance and strategic surveillance under the G10 Law. The G10 Commission is supported by the same secretariat (13 persons in 2016) that works for the Parliamentary Control Panel. With the reform of the PKGrG in 2016, the secretariat, under the management of the Permanent Representative, will be strengthened.[254] The reform of the BND Law on foreign-foreign surveillance established a new body in charge of approving such surveillance measures: the Independent Committee (*Unabhängiges Gremium*).[255] At the time of writing, the Independent Committee was not yet operational, although its members have been appointed, five supporting staff

244 Sweden, Parliamentary communication (Riksdagsskrivelse 2007/08:266) on the Government Bill "Adaptation of Defence Intelligence Activities" (Proposition 2006/07:63, En anpassad försvarsunderrättelseverkamhet), 8 March 2007.
245 Sweden, Parliament, The 15 parliamentary committees.
246 FRA (2015a), p. 41 and following.
247 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97-99.
248 The Netherlands, CTIVD (2017), p. 35, and CTIVD, webpage on members and staff.
249 The Netherlands, General States (*Staten-Generaal*) (2017), Parliamentary Document 34588, Nr. 67, 2 May 2017.
250 United Kingdom, Investigatory Powers Act, s. 227 (2).
251 *Ibid.* s. 238 (2).
252 United Kingdom, IPCO website.
253 United Kingdom, House of Lords (2016), Transcripts of debate on Investigatory Powers Bill, 17 October 2016, Volume 774, Column 2170.
254 Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), p. 1319.
255 Germany, BNDG, S. 16.

Table 2: Expert bodies (excluding DPAs) overseeing intelligence services in the EU

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	Three-Member Committee (*Τριμελής Επιτροπή*) [Not yet in place]
CZ	N.A.
DE	G 10 Commission (*G 10-Kommission*) Independent Committee (*Unabhängiges Gremium*)
DK	The Danish Intelligence Oversight Board (*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*) Council of State special formation
HR	Council for Civilian Oversight of Security and Intelligence Services *(Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*)
HU	N.A.
IE	Complaints Referee
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	The 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	Swedish Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten*) Commission on Security and Integrity Protection *(Säkerhets- och integritetsskyddsnämnden*) Defence Intelligence Court (*Försvarsunderrättelsedomstolen*)
SI	N.A.
SK	N.A.
UK *	Investigatory Powers Commissioner

Notes: *N.A. = not applicable (no expert body exists)*

** On September 1 2017, the Investigatory Powers Commissioner took over from the former Intelligence Service Commissioner and Interceptions of Communications Commissioner..*

Source: *FRA, 2017*

members have been hired and trained for the secretariat, rules of procedure prepared and secure facilities set up.[256]

For the purpose of this report, DPAs are considered to be oversight expert bodies. They are specialised bodies that have been specifically tasked with safeguarding privacy and data protection in EU Member States. The Court of Justice of the European Union (CJEU) has held in a series of judgments that supervision by DPAs is an essential

256 Lorenz, P. (2017), 'BND-Kontrolle am BHG: Unabhängiges Gremium nimmt Arbeit auf', *Legal Tribune Online*, 9 March 2017; and Dreusicke, L. (2017), 'Präsidentin des BGH in Osnabrück: Wer das Ausspähen des BND kontrollieren soll', *Osnabrücker Zeitung*, 27 April 2017.

component of the right to personal data protection.[257] Their powers and competences are analysed in Section 9.2.

8.5. Watchdogs

Other actors also substantially contribute to ensuring the effectiveness of existing safeguards. These include national human rights institutions, civil society actors – including the media, academia[258] and NGOs – and whistleblowers.

NGOs have launched lawsuits in various EU Member States, promoted reforms,[259] developed international principles applicable to oversight of intelligence services,[260] and have acted as watchdogs of legislative processes.[261] Consequently, it is important to support and respect their roles so that they can contribute to improving the oversight of intelligence matters. The same is true about national human rights institutions (NHRIs).[262] In France, for example, the French NHRI in 2015 contributed to the legislative reform regarding surveillance measures and their oversight by providing parliament with various opinions on different laws relating to intelligence and counter-terrorism.[263] The German NHRI submitted written opinions on relevant issues for parliamentary hearings, including the one on the BND reform in 2016.[264] However, NHRIs' opinions are not sought systematically in this area.[265]

Protecting fundamental rights via strategic litigation

In **France**, in 2017, the NGOs *La Quadrature du Net*, French Data Network and *Fédération des fournisseurs d'accès à internet associatifs* filed a 'priority preliminary ruling on constitutionality' (*Question Prioritaire de Constitutionalité,* QPC) with the Council of State related to the access of intelligence services to metadata retained by telecommunication providers. The Council of State referred the case to the Constitutional Court. The Constitutional Court decided on 4 August 2017 that the four-month authorisation the intelligence services can obtain to access metadata of a targeted suspect complies with the constitution. However, the Constitutional Court declared unconstitutional the extension of the same authorisation to access metadata of the suspect's entourage.

France, Constitutional Court, Decision n. 2017-648 QPC, 4 August 2017

In **France**, in 2016, four associations – *La Quadrature du Net*, *FDN*, *Fédération des fournisseurs d'accès à Internet associatifs* and *igwan.net* – filed a QPC with the Council of State, on the grounds that radio surveillance was not subject to any procedural safeguards. The Council of State referred the matter to the Constitutional Court, which held – in October 2016 – that the legal provision allowing for radio surveillance was contrary to the French constitution. As a result, Article L.811-5 of the Internal Security Code was repealed; this will take effect on 31 December 2017.

France, Constitutional Court, Decision n. 2016-590 QPC, 21 October 2016

In 2015, **United Kingdom**-based Privacy International started a legal challenge in the Investigatory Powers Tribunal (IPT), about whether the acquisition, use, retention, disclosure, storage and deletion of Bulk Personal Datasets (BPD) and Bulk Communications Data (BCD) is in accordance with the law or necessary and proportionate. In 2016, the IPT ruled that obtaining BPD and BCD, before doing so was publicly acknowledged, violated the right to private life, by virtue of the lack of foreseeability to the public and the lack of adequate oversight. However, the IPT accepted that, following public acknowledgment of the use of these powers, the changes made to oversight powers and the publication of the relevant procedures, the powers were compatible with the right to private life. The case was referred to the CJEU for matters relating to EU law.

United Kingdom, Investigatory Powers Tribunal, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, *IPT/15/110/CH, 17 October 2016 and 8 September 2017*

In 2014, Privacy International brought an action before the IPT, challenging the compliance of GCHQ's Computer Network Exploitation (CNE) – colloquially, 'hacking' – with domestic law and the right to private life (Article 8 of the ECHR) and freedom of expression (Article 10 of the ECHR). In 2016, the IPT ruled that CNE activities can in principle be lawful. The tribunal considered and gave guidance on how a warrant allowing for CNE activity would have to describe the potentially intercepted equipment. The IPT concluded that warrants compliant with such guidance would be lawful both under domestic law and the ECHR.

United Kingdom, Investigatory Powers Tribunal, Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, *IPT/14/85/CH 14/120-126/CH, 12 February 2016*

257 See in particular 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. See also Working Group on Data Protection in Telecommunications (2017).
258 University of Amsterdam (2015), *Ten standards for oversight and transparency of national intelligence services*, IViR (Institute for Information Law, University of Amsterdam). See also the various projects funded by the European Union under the FP7 and now the Horizon 2020 programme.
259 See, for example, Löning, M. (2015); Brown, I. *et al.* (2015). See also the strategic litigation, advocacy, capacity building and reporting undertaken by Privacy International.
260 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).
261 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); Bits of Freedom, a NGO, a digital rights organisation in the Netherlands closely follows the legal reforms.
262 Council of Europe, Commissioner for Human Rights (2016).
263 See France, Commission Nationale Consultative des Droits de l'Homme (2015); France, Commission Nationale Consultative des Droits de l'Homme (2016); France, Commission Nationale Consultative des Droits de l'Homme (2017a); France, Commission Nationale Consultative des Droits de l'Homme (2017b). See also France, Défenseur des Droits (2017).
264 Germany, Deutsches Institut für Menschenrechte (2016)
265 France, Le Monde (2017).

In 2013, the **German** branch of Reporters without Borders (RWB) brought an action against BND's strategic surveillance of international communications. RWB argued that both the interception of communications itself and the collection, storage and analysis of metadata violated their privacy. In 2016, the Federal Administrative Court decided that there was no privacy violation because, even if the NGO's communications had been under surveillance, BND deleted them immediately and such act could not be traced. In 2017, the case was brought before the Federal Constitutional Court challenging, among others, the lack of remedies in case of strategic surveillance.

Germany, Federal Administrative Court (Bundesverwaltungsgericht), *BVerwG 6 A 7.14, 15 June 2016*

During fieldwork interviews, all respondents were asked to describe cooperation efforts between their institutions and the other main actors in their country, including civil society organisations. The findings show that cooperation is least developed with civil society organisations (in comparison with other institutional bodies) and mainly takes the form of ad hoc exchanges or consultations. Few entities within the Member States researched have established contacts with civil society organisations or take advantage of certain networks operating domestically – such as the Belgian Human Rights Platform, established in January 2015, which brings together all institutions with human rights protection mandates, including the Standing Committee I. In Croatia, civil society participates in the Council for Civilian Oversight of Security and Intelligence Services, which exercises part of the oversight of the operations of intelligence services and their legality.[266] However, in the remaining Member States, many respondents suggested there was room for future developments and closer cooperation. The work of civil society is most appreciated by national human rights institutions, ombuds institutions, lawyers and academics for their professionalism, strategic litigation, provision of amicus curiae briefs, opinions on draft laws, participation in public consultations and provision of legal advice for individuals who seek remedies in case of violations.

The media unquestionably play a substantial role in generating or steering public debate during legal reforms. They also played a crucial role in publishing some of the US National Security Agency material exposed by Edward Snowden, informing the broader public about the existence and some of the functioning programmes of general surveillance of communications. Interviewed oversight body representatives in Italy, the Netherlands and Sweden noted that some of their investigations were triggered by media attention to certain issues. At the same time, in relation to trust-based cooperation, expert body representatives tended to cite reports or leaks of information, e.g. to the media, as undermining their relationship with the intelligence services.

As further analysed in Section 10.3, media professionals might be less willing to conduct in-depth investigative reporting on intelligence services if the confidentiality of their sources is not assured by enhanced safeguards against surveillance.

ECtHR case law: whistleblowers

"[A] civil servant, in the course of his work, may become aware of in-house information, including secret information, whose divulgation or publication corresponds to a strong public interest. The Court thus considers that the signalling by a civil servant or an employee in the public sector of illegal conduct or wrongdoing in the workplace should, in certain circumstances, enjoy protection. [...] In the light of the duty of discretion referred to above, disclosure should be made in the first place to the person's superior or other competent authority or body. It is only where this is clearly impracticable that the information could, as a last resort, be disclosed to the public [...]."

ECtHR, Guja v. Moldova [GC], No. 14277/04, 12 February 2008, paras. 72-73

The 2015 FRA report highlighted the importance of whistleblowers.[267] Staff within intelligence services may want to raise concerns about the legality of activities witnessed within their agency. This can be achieved by means of internal controls such as ethics commissioners or staff counsellors, to whom staff can turn in confidence if they have anxieties relating to the work of their service; and through whistleblower provisions, which allow staff to feel secure when reporting wrongdoing. Ethics counsellors, journalists and whistleblowers thus can also play an essential 'intermediary' role in alerting executive and oversight bodies to issues that require investigation. The Snowden revelations provide a good example of this since they led to both national and international litigation.[268]

266 Croatia, Act on the Security Intelligence System of the Republic of Croatia 2006 (*Zakon o Sigurnosno-Obavještajnom Sustavu Republike Hrvatske 2006*), Art. 110.

267 FRA (2015a), pp. 33 and 68.

268 See also the concept of 'insider' complaints in Forcese, C. (2012), p. 182. See also PACE, Committee on Legal Affairs and Human Rights (2015a).

Protecting whistleblowers

"Whistle-blowers should be strongly protected and whistleblowing mechanisms should be strongly encouraged. Reports on internal and external whistleblowing should be sent to an independent supervisory body. The press and their sources should be protected in their reporting on the activities of the intelligence and law enforcement agencies."

Korff, D. et al. *(2017), p. 12*

"The law should require public authorities to establish internal procedures and designate persons to receive protected disclosures.

States should also establish or identify independent bodies to receive and investigate protected disclosures. Such bodies should be institutionally and operationally independent from the security sector and other authorities from which disclosures may be made, including the executive branch."

Tshwane Principle 39 A and B(i)

The ECtHR addressed matters relating to whistleblowing by civil servants in *Guja v. Moldova*[269] and *Bucur and Toma v. Romania*.[270] The latter relates specifically to whistleblowing by a member of an intelligence service regarding the unlawful interception of communications. In deciding whether a sanction against a whistleblower is a justified interference with their freedom of expression, the ECtHR considers the following matters:

- whether the whistleblower had alternative channels for the disclosure,
- the public interest in the disclosed information,
- the authenticity of the disclosed information,
- the detriment to the affected institution,
- whether the whistleblower acted in good faith, and
- the severity of the sanction.

The French law on intelligence protects whistleblowers. If confronted with suspected wrongdoing, a staff member of the intelligence service can contact the CNCTR, which can then bring the case before the Council of State and inform the prime minister.[271] As of March 2017, the procedure has not yet been used.[272] In Germany, a whistleblower mechanism provides for the possibility for intelligence service staff to approach the Parliamentary Control Panel.[273] In the Netherlands, the new Act on the Intelligence and Security Services 2017 assigns the competence to investigate reported wrongdoing to the CTIVD.[274] In Belgium, when dealing with denunciations made by whistleblowers wishing to complain about their own administration, the Standing Committee I handles the individual complaint but focuses on the improvement of the efficiency of the intelligence services. Upon receiving a denunciation, it launches an investigation. The results of the investigation are shared with the whistleblower in general terms. They are also reported to the head of the relevant service, the competent minister and parliament. Finally, the general findings are made public.[275]

FRA asked different actors about possible provisions regarding whistleblower protection within the intelligence services. Provisions for such protection are prescribed in the legislation of four of the seven Member States researched. The respondents generally did not express specific or clear opinions regarding whistleblower protection provisions, and indicated that they lacked knowledge about the respective national context.

The interviewees did tend to agree on one aspect: that efficient whistleblower protection in the intelligence services requires a specific regime, different from those for other governmental institutions. In some Member States, recent legislative reform efforts included discussions of this issue, but they are not necessarily reflected in the enacted legislation. Otherwise, however, opinions on the issue of whistleblower protection generally varied, and also differed among respondents from the same Member State.

"It is not regarded as being very effective. For this reason, the political demand has been made time and time again that comprehensive protection for whistleblowers is needed." (Expert body)

"Well, we have no whistleblower protection. In general, there is no such protection and this is a real problem."

(Data protection authority)

"There are always calls for a whistleblower law in [country]. I do not consider this to be necessary. We do not need such a law." (Academia)

269 ECtHR, *Guja v. Moldova* [GC], No. 14277/04, 12 February 2008, paras. 70-78.
270 ECtHR, *Bucur v. Romania*, No. 40238/02, 8 January 2013, paras. 94-119.
271 France, Interior Security Code, Art. L. 861–3. See also Foegle, J.-P. (2015).
272 France, DPR &CNCTR (2017).
273 Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), 29 July 2009, s. 8 (1).
274 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97 and Arts. 125-131.
275 In total, the Standing Committee I received 22 complaints or denunciations, see Belgium, Standing Committee I (2016), p. 7.

In one Member State, for example, the opinions of the different actors ranged from a strong call to make whistleblower protection effective and a call for its implementation to questioning the need for such safeguards, even though the national legislation provides such a mechanism. The excerpted quotes illustrate the diverging opinions. These findings suggest that broader discussions are needed to encourage actors to fully consider their approaches to the issue.

9 Features of oversight bodies

ECtHR case law

Qualities required for supervisory control

"It is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...] supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 275

Public scrutiny

"The Court must also examine whether the supervisory body's activities are open to public scrutiny (see, for example, *L. v. Norway*, cited above, where the supervision was performed by the Control Committee, which reported annually to the Government and whose reports were published and discussed by Parliament; *Kennedy*, cited above, § 166, where the supervision of interceptions was performed by the Interception of Communications Commissioner, who reported annually to the Prime Minister, his report being a public document laid before Parliament; and, by contrast, *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 88, where the Court found fault with the system where neither the Minister of Internal Affairs nor any other official was required to report regularly to an independent body or to the general public on the overall operation of the system or on the measures applied in individual cases)."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para 283

The ECtHR favours oversight settings involving judges. The 2015 FRA report highlighted that a majority of EU Member States provide for such oversight.[276]

However, 'non-judicial bodies' – which this report refers to as oversight bodies in an encompassing manner or as expert bodies in a narrower sense – can be ECHR compliant. They should however have two essential qualities: be independent and have enough powers and competence to carry out continuous control that is subject to public scrutiny.

The interviewed oversight body experts were asked to identify what they consider to be the main features of effective oversight. Effective oversight was associated with the following five interrelated features: (1) cooperation among key actors in the area; (2) full access to intelligence information; (3) sufficient resources; (4) transparency (specifically through reporting), and (5) independence. These elements are listed based on the frequency with which they were mentioned during the interviews; however, this varied among respondents.

The respondents' views regarding what the most important elements of effective oversight are largely overlap with the main features of effective oversight identified in European case law. This is directly reflected with regard to independence, and partly with regard to public scrutiny, which is mainly considered through the issue of transparency. In this regard, reporting – mainly via reports produced, preferably published on a regular basis – plays an important role. The issues raised while discussing resources of oversight bodies, full access to intelligence information, and cooperation among key actors fall under the label of powers and competences. Table 3 presents the overlap between interviewed experts' views regarding features that make for effective oversight and the main features identified in ECtHR case law.

276 FRA (2015a), p. 51 and following.

Table 3: Effective oversight: legal standards and views of key actors

ECtHR standards	FRA fieldwork findings
Independence	Independence
Powers and competence	Full access
	Sufficient resources and expertise
	Cooperation of key actors
Public scrutiny	Transparency

Source: FRA, 2017

The following sections describe oversight bodies' features in detail, as formulated by the ECtHR and discussed in relevant fieldwork findings.

9.1. Independence

Basic requirements for independence

"In determining whether a body can be considered to be 'independent' – notably of the executive and of the parties to the case [...], the Court has had regard to the manner of appointment of its members and the duration of their term of office [...], the existence of guarantees against outside pressures [...] and the question whether the body presents an appearance of independence."

ECtHR, Campbell and Fell v. the United Kingdom, No. 7819/77 and 7878/77, 28 June 1984, para. 78

The ECtHR has confirmed that an institution's legal obligation to act independently and impartially is not sufficient to meet the minimum standard of independence; independence from the executive must be ensured both in functioning and institutionally.[277] The ECtHR requirement of independence entails organisational, operational and aspects relating to the members of the institution. Key questions in addressing the independence of an oversight body thus relate to its appointing authority; the body's composition and who chairs the body; rules on conflicts of interest; whether the law foresees its independent functioning and whether the body (in fact) operates without hindrance. Finally, independence is also a matter of perception: the body also needs to appear independent; the way it functions needs to be perceived as independent. In this context, the location of the body's offices may be relevant, for example – such as when an expert body is located within a ministry or in the intelligence service building. This is a particularly problematic matter given the data to which the oversight body has access. The need to be perceived as independent has to be balanced against practical security concerns.

Determining the optimal distance between the controlled and the controllers is a complex exercise, since providing up-to-date expertise requires oversight bodies to work side-by-side with the intelligence services. 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 poorly informed.

"The oversight body must be able to work independently, full-time, it must be able to specialise and choose its own staff." (Expert body)

Oversight body representatives were asked about safeguards for their institutions to carry out tasks independently and the measures implemented to sustain their independence. Almost all respondents stated that their institutions were independent, impartial, and resistant to any external influence, including by politicians or the intelligence services. Independence is said to be guaranteed by institutional and operational procedures. The institutional procedures mentioned by the respondents include statutory recruitment procedures, methods of appointment (or the standing of the members), fixed terms of office, seniority of staff, and allocated budgets (independent budgets). The operational procedures that ensure independence in oversight actions were related to security clearance requirements, the staff's duty of absolute secrecy, access to data/information of the intelligence services, and their power to initiate investigations. In addition, some interviewees noted that their independence improved while moving their offices outside the premises of, for example, executive or other governmental bodies. Still, some interviewees pointed to a lack of independence due to being integrated into the hierarchies and structures of the institutions they were meant to monitor.

The oversight representatives attributed less importance to oversight bodies' independence than to other aspects when discussing their effectiveness. This might be related to their view that they currently exercise their functions in full independence.

As with other issues, representatives from civil society organisations and academia were more critical regarding oversight bodies' independence. They emphasised the importance of independent oversight, voicing the opinion that such bodies are currently 'only independent because they call themselves independent'. They noted that staff of oversight bodies lack knowledge on independence. In addition, some operational features make it difficult to sustain

277 ECtHR, *Campbell and Fell v. the United Kingdom*, No. 7819/77 and 7878/77, 28 June 1984, para. 77.

their independence – such as not being able to issue binding decisions, or having overlapping functions (e.g. being independent from the executive while, at the same time, participating in functions closely linked to the executive). They also highlighted the lack of transparency in nomination procedures and budgets being part of general ministerial budgets. These factors were also described as feeding into oversight bodies' lack of transparency and accountability.

ECtHR case law: requirements for independence

"As to the independence requirement, in previous cases the Court has taken into account the manner of appointment and the legal status of the members of the supervisory body. In particular, it found sufficiently independent the bodies composed of members of parliament of both the majority and the opposition, or of persons qualified to hold judicial office, appointed either by parliament or by the prime minister [...]. In contrast, a Minister of Internal Affairs – who not only was a political appointee and a member of the executive, but was directly involved in the commissioning of special means of surveillance – was found to be insufficiently independent [...]. In contrast to the supervisory bodies cited above, in Russia prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities [...].This fact may raise doubts as to their independence from the executive. Furthermore, it is essential that any role prosecutors have in the general protection of human rights does not give rise to any conflict of interest [...]. The Court observes that prosecutor's offices do not specialise in supervision of interceptions [...]. Such supervision is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. In the framework of their prosecuting functions, prosecutors give their approval to all interception requests lodged by investigators in the framework of criminal proceedings [...]. This blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 278*

Regarding parliament, the 2015 FRA report emphasised that the question of independence should be understood in terms of pluralism, which many Member States ensure by including mandatory proportional representation rules on membership.[278] By contrast, the executive appoints the members of some expert bodies. This is the case, for instance, in Sweden and the United Kingdom. In the United Kingdom, the Investigatory Powers Commissioner and the Judicial Commissioners are appointed for three years, by the prime minister, upon joint recommendation by the Lord Chancellor, the Lord Chief Justice of England & Wales, the Lord President of the Court of Session and the Lord Chief Justice of Northern Ireland.[279] In the case of the Judicial Commissioners, recommendation by the Investigatory Powers Commissioner is also necessary.

While some aspects of independence need to be enshrined in law, others can be re-affirmed in codes of ethics at institutional level. The French law on intelligence integrated specific ethical rules into the legal framework, 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.[280]

The CJEU has emphasised that DPAs shall act in full independence, particularly from government.[281] The same requirement is prescribed by the *General Data Protection Regulation*.[282]

9.2. Powers and competence

The ECtHR's requirements for an oversight body to have 'sufficient powers and competence' to exercise its control continuously is linked not only to a strong mandate but also to the means put at its disposal to perform its oversight role.

UN good practices on sufficient resources

Practice 7. Oversight institutions have the [...] resources and expertise to initiate and conduct their own investigations.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

Oversight bodies may wield a variety of powers, a diverse combination of which may allow for adequate oversight of intelligence activity, including surveillance measures. These powers relate, on the one hand, to the appropriate review of the measures and, on the other, to the oversight bodies' ability to ensure that effective action is taken in case they find irregularities. What may be considered sufficient powers depends on a specific oversight body's function.

278 FRA (2015a), p. 41.

279 United Kingdom, Investigatory Powers Act, s. 227 (3)-(4).
280 France, Interior Security Code, Art. L. 832–1 and Art. L. 832–2.
281 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.
282 GDPR, Art. 52.

Securing sufficient powers and competence for the oversight system, however, may still fall short of securing an overall adequate oversight system, if the bodies involved do not have sufficient human, financial and technical resources to fulfil their functions appropriately.

Review of resources

"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."

Council of Europe Commissioner for Human Rights (2015), p. 14.

As the resource needs of oversight bodies may differ substantially according to their functions and their role within a state's oversight system, general standards for sufficient resources cannot be established. Therefore, they should be assessed on a case-by-case basis, taking into account the standard of sufficient powers. The oversight bodies contribute to the framing of the intelligence services' work as well as the specific control of the surveillance measures. DPAs can play an important but specific role in this area depending on their competences.

Parliamentary committees focus their review on the overall legality of the functioning of the services and the intelligence policy, and not of that of their specific operations. In the Netherlands, for example, the Parliamentary Commission for the Intelligence and Security Services (*Commissie voor de Inlichtingen- en Veiligheidsdiensten,* CIVD) is responsible for overseeing the services to the extent that matters remain classified and is regularly informed about the operational activities of the General Intelligence and Security Service.[283] The French parliamentary intelligence delegation (DPR) examines and assesses governmental policy on intelligence; it does not oversee the services directly. This is to preserve the separation of powers.[284] It may conduct hearings and request strategic intelligence reports from the executive.[285] The DPR does not carry out thematic investigations. In its 2017 report, the DPR suggested that two audits be conducted by the Inspectorate of Intelligence Services, one on recruiting intelligence service staff and one on intelligence files.[286]

The different parliamentary committees of Member States have various mandates and powers. These 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. The 2015 FRA report described the powers and competences of several specialised and non-specialised parliamentary committees in charge of the oversight of intelligence services.[287]

> *"The [United Kingdom's Parliamentary] Committee has been supported in its work by a team of seven core staff and seven Detainee Inquiry staff. These staff have an immensely difficult job to do. They act independently in support of the Committee and this is not always easy or popular with those who do not understand the importance of robust independent oversight."*
>
> *Statement by Chairman of the Intelligence and Security Committee (2017)*

Ad-hoc inquiry commissions or other general commissions can also play an important role in overseeing the services' work. In Belgium, the temporary 'Fight against Terrorism' Commission was established after the Paris attacks of November 2015. Its task was to examine the bills implementing certain measures put forward by the government following the terrorist attacks in Paris.[288] A Parliamentary Investigative Commission was also set up to examine the circumstances that led to the March 2016 attacks in Brussels.[289]

283 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*) (2016), 'Verslag van de commissie voor de Inlichtingen- en Veiligheidsdiensten over haar werkzaamheden in 2015', available at: https://zoek.officielebekendmakingen.nl/kst-34505-1.html

284 France, DPR & CNCTR (2017), p. 9

285 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 12.

286 *Ibid.* p. 57 and following.

287 FRA (2015a), pp. 34 and following.

288 Belgium, House of Representatives (2016), 'Magazine La chambre', *LaChambre.be*, p. 3; House of Representatives, Text adopted by the temporary 'Fight against Terrorism' Commission – Bill concerning complementary measures related to the fight against terrorism (*Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme/Wetsontwerp inzake aanvullende maatregelen ter bestrijding van terrorisme*), 14 April 2016.

289 Belgium, Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, 11 April 2016.

The German federal parliament's NSA inquiry committee

Following the Snowden revelations, the federal parliament established, on 20 March 2014, an inquiry committee (*1. Untersuchungsausschuss „NSA"*). The scope of its work was to investigate among others, these revelations, the operation of the Five Eyes (USA, UK, Canada, New Zealand, Australia) in Germany and the cooperation between the BND and the NSA. The committee published its 1,822 page-report on 23 June 2017, after 134 sessions and more than 90 witnesses (a total of 581 hours and 21 minutes of work). It is by far the most encompassing report published in the EU following the Snowden revelations.

Faced with a lack of cooperation from the services belonging to the Five Eyes, the inquiry committee focused its attention on, among others, the German legal framework, the work of the BND and other services, their surveillance powers, various intelligence programmes carried out by the BND, cooperation between the BND and the NSA, and the oversight system in Germany. The inquiry committee report contributes greatly to a better understanding of the work of the services in Germany, its oversight and international cooperation. In reaction to the Snowden revelations, the inquiry committee highlighted shortcomings, which led to an important reform of the German legal framework at the end of 2016.

The NSA inquiry committee members were not able to reach a consensus on the final report and so a separate opinion drafted by the opposition was added to the report. In particular, while the parties of the ruling coalition stated that no mass surveillance programme was carried out by the NSA and the BND (p. 1243), the opposition parties came to the opposite conclusion in their – partly redacted – separate opinion (p. 1323).

The NSA inquiry committee did agree that past serious grievances and major flaws could be attributed to the BND, necessitating reform.

*Germany, Federal Parliament (*Deutscher Bundestag*) (2017b)*

Members of parliamentary oversight committees tend to have access to classified information.[290] However, the law always qualifies the right of access, and few parliamentary committees have unrestricted access.[291] 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. In the United Kingdom, the ISC may request the chiefs of any of the three main intelligence and security services to disclose information, and they must make it available or inform the ISC that disclosure was vetoed by the secretary of state.[292] The French parliamentary committee (DPR) does not have access to information on ongoing operations carried out by the services, governmental instructions given to them, or surveillance methods or exchanges with foreign services.[293] The DPR gets its information through hearings, on-site visits and strategic documents, as well as opinions and reports by the oversight body.[294] The Dutch CIVD has access to the confidential part of the annual report of the General Intelligence and Security Service. The German Parliamentary Control Panel's access to files and information may be limited by the "direct executive responsibility" of the federal government. As underlined in FRA's 2015 report, the flipside of powers to access information also relates to security clearance.[295] In Belgium, the parliamentary committee decided on its own motion not to obtain clearance and thus cannot access confidential information, but it can turn to the Standing Committee I to conduct investigations.[296]

Oversight bodies' contributions to legislative reform vary greatly across Member States. Some contributions, in the form of official mandatory opinions, are prescribed by law – as is the case, for example, with the French expert body CNCTR. [297] The French parliamentary oversight body makes recommendations to the executive based on the analysis of intelligence policy and the functioning of the services. These recommendations are presented in a classified report addressed to the president, the prime minister and the speakers of both houses of parliament.[298] Once officially presented to the president, a non-classified report is also published with the recommendations. In the United Kingdom, the ISC published its views on the draft Investigatory Powers Bill.[299] In other legislative settings, the contribution can be published on a voluntary basis – see, for example, *The CTIVD's Views on the ISS Act 2017*[300] *in the Netherlands, or Interception of Communication Commissioners Office (IOCCO) Points to consider on the Investigatory Powers Bill* in the United Kingdom.[301] Participation in hearings and written evidence can also contribute to the legislative process and enhance transparency.

290 Wills, A. *et al.* (2011), p. 142.
291 See *Ibid.* p. 117; and Council of Europe Commissioner for Human Rights (2015), p. 44.
292 United Kingdom, Justice and Security Act 2013, Schedule 1, S.4. See, United Kingdom, House of Commons (2017), p. 7.
293 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.
294 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 12 and following.
295 FRA (2015a), p. 42.
296 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union 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, Arts. 32, 33 and 35 (2).
297 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 811-4 and L. 833-11.
298 France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 7 and 91.
299 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2016).
300 The Netherlands, CTIVD (2016b).
301 United Kingdom, IOCCO (2016b).

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 are provided for the breach of these requirements by members of oversight institutions.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

One of the most important powers of oversight bodies is their ability to initiate investigations on their own. The Belgian Standing Committee I can start investigations on its own initiative, on the request of the Chamber of Representatives or the competent minister or authority,[302] or on the request of a citizen or a civil servant who lodges a complaint or files a denunciation.[303] 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.[304] 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.[305] 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.[306] Belgium has a second expert body referred to as the Administrative Commission. It 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.[307]

In Germany, the Independent Committee (*Unabhängiges Gremium*) is an expert body, at the Federal Court of Justice, consisting of two judges and a prosecutor.[308] Its task is to review the legality and necessity of the BND's strategic foreign-foreign communications data surveillance. It is involved in the *ex ante* approval of strategic surveillance measures when they relate to EU institutions and Member States' authorities. The Independent Committee is also granted ex post review powers when the surveillance measures are deployed on EU or other foreign citizens. The investigative powers available to the Independent Committee are not specified in the law.[309]

ECtHR case law: binding interventions of oversight institutions

"The supervisory body's powers with respect to any breaches detected are also an important element for the assessment of the effectiveness of its supervision (see, for example, *Klass and Others*, cited above, § 53, where the intercepting agency was required to terminate the interception immediately if the G10 Commission found it illegal or unnecessary; and *Kennedy*, cited above, § 168, where any intercept material was to be destroyed as soon as the Interception of Communications Commissioner discovered that the interception was unlawful)."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015,* para. 282

Give an external oversight body the power to quash surveillance warrants and discontinue surveillance measures undertaken without the need for a warrant when such activities are deemed to have been unlawful, as well as the power to require the deletion of any information obtained from the use of such measures.

Council of Europe, Commissioner for Human Rights (2015), Democratic and effective oversight of national security services, *p. 13*

Whether an oversight body has the power to quash warrants, stop surveillance measures and require the rectification or erasure of collected data is also an important factor in assessing the effectiveness of the oversight system. To do so, it is granted continuous access to the gathered intelligence and is informed about any modifications. In France, if the CNCTR considers 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 on.[310] If the recommendation is not followed appropriately, the CNCTR can bring the case before the Council of State.[311] In the United Kingdom, the Judicial Commissioner, once established, will be able to reject warrants or quash those in operation.

302 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union 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.
303 *Ibid.* Art. 34.
304 Belgium, Organic Law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 43/2, as amended.
305 *Ibid.* Arts. 18/4 to 18/8 and 18/9 to 18/17, as amended.
306 Belgium, Organic Law on the control of police and intelligence services and the Coordination Union 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. 33.
307 Belgium, Organic Law on intelligence and security services (*Loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 43/1, as amended.
308 Germany, BNDG, S. 16.
309 Wetzling, T. (2017), p. 8.
310 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-6.
311 *Ibid.,* Art. L. 833-8.

In Sweden, the expert body SIUN, is tasked with ensuring that the state's signals intelligence is carried out lawfully.[312] 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 Defence Intelligence Court. It has the power to stop on-going signals intelligence and subsequently order the destruction of collected data.

ECtHR case law: access to relevant documents

"Turning now to the prosecutors' powers and competences, the Court notes that it is essential that the supervisory body has access to all relevant documents, including closed materials and that all those involved in interception activities have a duty to disclose to it any material it required."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 281

UN good practices on access to information

Practice 7. Oversight institutions 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 (2010), Report of the Special Rapporteur Martin Scheinin

Another key power of oversight bodies is access to information, IT systems, documents and data – including not only that relating to specific operations, but also to internal policies and guidance. While access need not be complete, it should cover everything that may be relevant for the oversight bodies. In addition, access should be autonomous: oversight bodies should not be required to rely on the services to provide them what they deem relevant.

In the United Kingdom, the Investigatory Powers Commissioner (IPC) must keep under review the majority of the targeted and bulk surveillance powers available to the intelligence services, such as the interception of communications, the acquisition or retention of communications data and equipment interference.[313]The primary aim of the IPC's oversight is to keep under review the operation of safeguards to protect privacy,[314] excluding cases already being considered by the courts.[315] The Investigatory Powers Act grants extensive powers to the IPC. The intelligence services must disclose or provide all the necessary documents and information for the purposes of IPC's functions.[316] In addition, if the IPC requires assistance in accessing apparatuses, systems or other facilities of the intelligence services when exercising oversight functions, this must be provided by the intelligence services.[317]

In the Netherlands, the new legislation stipulates that one of the two sub-committees of the CTIVD performs general oversight. It reviews on a regular basis the activities of both intelligence services by investigating whether their operations or actions are in accordance with the existing legal surveillance framework. The CTIVD may request information and the minister's cooperation, and can give the minister unsolicited advice. In addition, through in-depth investigations and its complaints-handling[318] role, the CTIVD ensures that the intelligence services perform their duties lawfully. To do so, it has unlimited and independent access to AIVD data.[319]

In France, the CNCTR enjoys permanent, complete and direct access to the implementation reports and registries of surveillance techniques, to the collected intelligence, as well as to the transcriptions and extractions carried out by the intelligence services. Moreover, the CNCTR has unlimited access to the premises where collected data are stored, in addition to the devices used to trace the collected data.[320]

312 Sweden, Signals Intelligence Act (*Lag [2008:717] om signalspaning I försvarsunderrättelseverksamhet)*, ss. 10 and 10a, 10 December 2009; and Sweden, Regulation with instructions for the Swedish Foreign Intelligence Inspectorate (*Förordning [2009:969] med instruktion för Statens inspektion för försvarsunderrättelseverksamheten*), 15 October 2009.

313 United Kingdom, Investigatory Powers Act 2016, s. 229 (1).
314 *Ibid.* s. 229 (5).
315 *Ibid.* s. 229 (4).
316 *Ibid.* s. 235 (2).
317 *Ibid.* s. 235 (3) and (4).
318 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 97.
319 *Ibid.,* Articles 107-111.
320 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-2.

In Italy, the DPA is responsible for providing ongoing and ex post oversight on the services. It has the right to initiate inspections and to access classified materials.[321]

Most of the interviewed expert oversight bodies indicated that they have full, unrestricted, relevant access to intelligence data. According to the interviewees, they have 'access to (very) confidential and secret information', 'unlimited access', 'the full access', 'access to all documents', 'can get every information we want', 'can get classified information', 'can request anything from the intelligence services'.

Oversight body representatives noted that accessing intelligence services' documents and systems is a usual practice of the oversight system and is regularly exercised to the extent possible, regardless of the scope of activities. A limited number of staff (directly involved) in data protection authorities, ombudsperson or national human rights institutions enjoy different levels of security clearance with regard to direct access to the intelligence services' files.

"The important thing is for the inspector to be able to inspect the records of the organisation itself directly. We are not dependent on the organisation to say "we are going to show you only these 10 files", to provide us material. They should and do volunteer matters which are within the scope of the inspection; however, this is insufficient. We should be able to inspect their computer records." (Expert body)

"The primary concern of the oversight is to have access to all the material available to the services. […] The oversight body needs to have access to the algorithms and to the strategies behind those algorithms." (Expert body)

Although full access to intelligence information is crucial for effective oversight, so is the ability to fully benefit from such access. Some respondents questioned oversight bodies' ability to do so, particularly due to limited technical capabilities. This was indicated both by way of critical self-assessment of the competences within the oversight bodies, and via criticisms from other bodies or organisations in the field. Representatives of civil society, academia and lawyers questioned the bodies' 'abilities to check the things properly', including their general understanding of the digital environment – for example, the digital (technical) skills of members of parliamentary committees.

"While the surveillance community, the secret service and the police are now immersed in big data and the advanced information society, the oversight bodies should not use coaches drawn by horses. But this is the situation today because intelligence organisations, services and police are hesitant to accept the use of [certain] software by control bodies, oversight bodies." (Data protection authority)

For effective compliance control, the *General Data Protection Regulation* grants 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.[322] 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 mentioned in the explanatory report to the protocol.[323]

DPAs' competences vis-à-vis intelligence services vary in the Member States, and depend on national legislation. DPAs may have no powers, limited powers or the same powers over the intelligence services as any other data controller.[324] FRA's findings show that, in most Member States, DPAs have either no competences over national intelligence services (in 11 EU Member States), or their powers are limited (in 10 Member States).

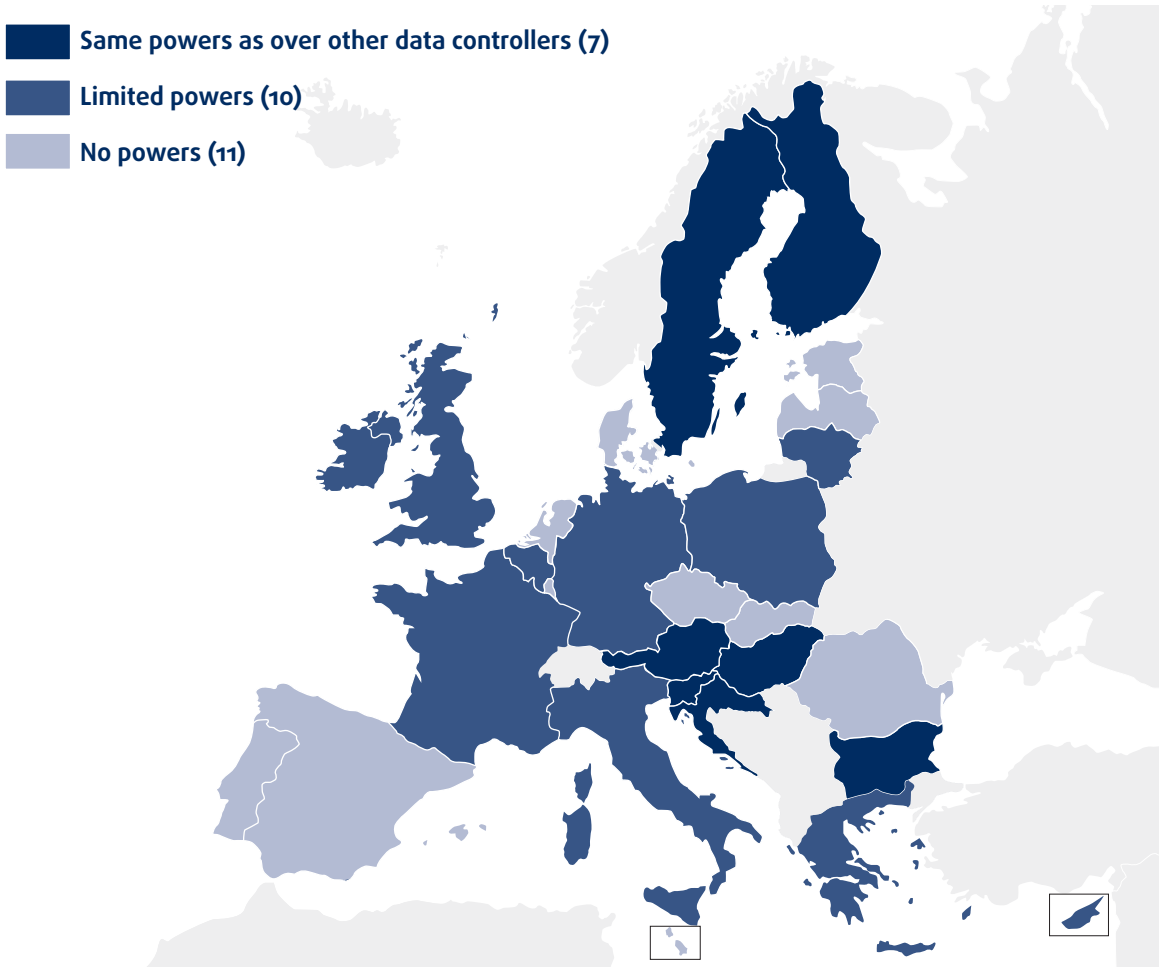
321 Italy, Data Protection Code, Art. 160 (4).

322 GDPR, Art 57.

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

324 See FRA (2015a), pp. 46-51, for a detailed overview of DPAs' competences over intelligence services.

Figure 7: DPAs' powers over national intelligence services, by Member State



Source: *FRA, 2017*

As Figure 8 illustrates, the extent of oversight coverage among Member States is very diverse. In four Member States – Austria, Bulgaria, Hungary and Sweden – both the expert bodies and the DPA are competent to assess the legality of surveillance techniques conducted by intelligence services. By contrast, in six EU Member States, no expert body has been set up to supervise surveillance techniques, and the intelligence services are exempt from DPAs' scope of competences. The 2015 FRA report raised questions regarding possible overlapping supervision powers for Member States with both types of oversight bodies, and questioned the effectiveness of oversight in the EU Member States that have not established any expert bodies and have exempted their DPAs from overseeing intelligence services.[325]

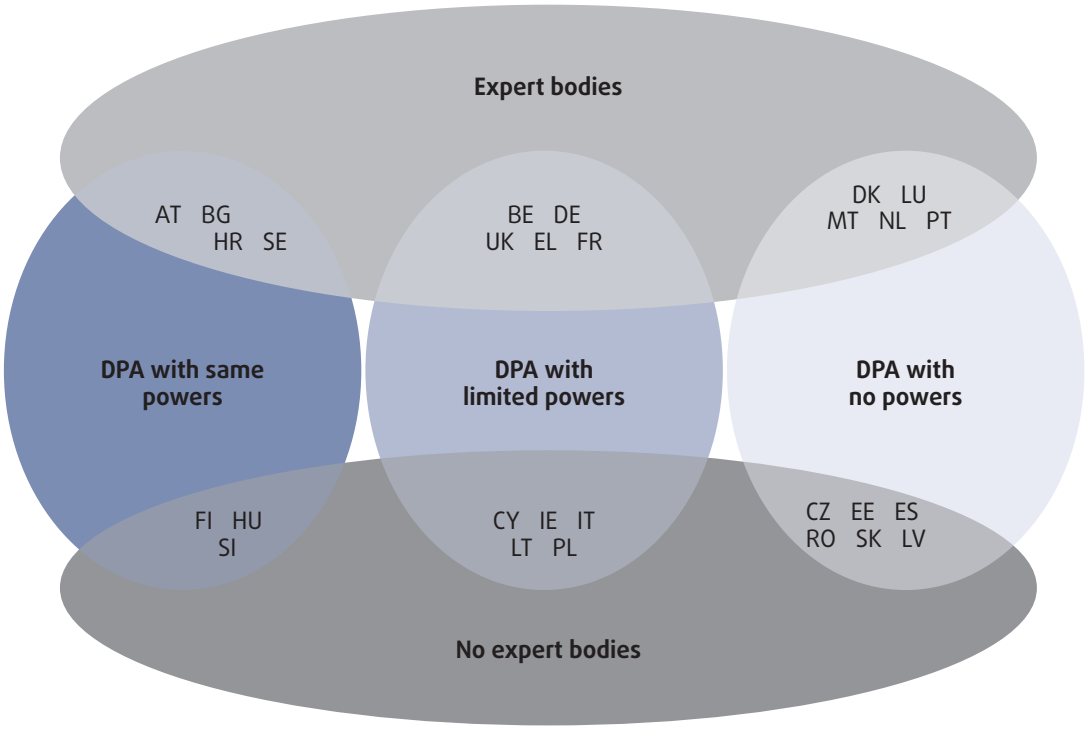
DPAs with limited powers act as regulators of the treatment of data used for intelligence purposes. They may have an advisory role, providing opinions on proposed laws that have an impact on personal data protection, including the setting up of new databases in the field of national security. DPAs treat intelligence services as data controllers and their oversight is limited to supervising the intelligence services' compliance with obligations linked to the processing of data. DPAs with limited powers do not look at the content of intercepted communications. For example, the DPAs could check through inspections whether the intelligence services respect the permissible period of retention of the collected data. However, the law may limit their access to databases containing data that were collected through certain intelligence techniques.

DPAs' powers are limited in 10 Member States. For instance, in the United Kingdom, the national intelligence services may rely upon the exemption for national security cases, which is provided in the data protection law.[326] The Information Commissioner Officer (ICO) must audit compliance with requirements or restrictions imposed by the retention of communications data in

325 FRA (2015a), p. 53.

326 United Kingdom, Data Protection Act 1998, s. 28 (1).

Figure 8: DPAs' and expert bodies' powers over intelligence techniques, by EU Member State



Notes: *'No powers' refers to DPAs that have no competence to supervise intelligence services.*
'Same powers' refers to DPAs that have the exact same powers over intelligence services as over any other data controller.
'Limited powers' refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers).

Source: *FRA, 2017*

relation to the integrity, security or destruction of data retained by the services. In other words, the ICO does have competence in reviewing *how* the data is retained, even if they have no access to *what* is retained. In practice the ICO liaises closely with the expert bodies and advises on data protection standards.

In Germany, the new federal data protection legislation only grants the Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) the power to file non-binding complaints (*Beanstandungen*) against intelligence services when data breaches are detected.[327] Additionally, depending on how the law is interpreted, it may provide the commissioner the power to request, upon suspecting individual intelligence service staff members of committing specific data breaches, the court to impose individual sentences of up to three years on such staff members.[328] However, the legal provisions on sentencing are ambiguous regarding intelligence services staff, because intelligence activities are potentially excluded from the scope of application.[329] In 2016, the commissioner filed a formal complaint against the Federal Office for the Protection of the Constitution (BfV) for illegal practices in transferring data originating from domestic general surveillance of communications to a counter-terrorism database. The commissioner's latest annual report notes that this complaint was the result of a joint inspection with staff from the secretariat of the G10 Commission.[330]

In Member States where expert bodies exist and DPAs have the competence to oversee intelligence services, their interaction is sometimes organised by law, and sometimes in practice takes place without legal requirements. In Member States in which DPAs and other expert oversight bodies share competence, a lack of cooperation between these may leave gaps in the

327 Germany, Federal Data Protection Act (*Bundesdatenschutzgesetz*), s. 16 (2), in force on 25 May 2018.
328 *Ibid.* s. 84 in conjunction with s. 42, in force on 25 May 2018.
329 *Ibid.* s. 45, in force on 25 May 2018.
330 Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2017), pp. 134-135. See also, Germany, Federal Parliament (2017a), p. 642 and following and on the challenges to control: Germany, Federal Parliament (2017a), p. 811 and following

overall oversight of the services. 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 (for example, in the Netherlands). 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 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.[331] Regrettably, the MoU's content is classified and not publicly available.

"The Memorandum [of Understanding] is an example of how to extend the law in favour of citizens' protection."

(Data protection authority)

Similarly, a 2016 report by a committee appointed by the Swedish executive considered possible supervisory overlaps and suggested moving some control functions from other agencies to the DPA.[332]

In the six Member States where no expert bodies have been set up to supervise surveillance techniques, and intelligence services are exempt from DPAs' scope of competences, the legal frameworks allow only for targeted surveillance and all foresee judicial involvement in the authorisation of such measures.

Two of these – Estonia and Slovakia – have empowered other authorities with controlling competences. In Estonia, the oversight of the services is since January 2016 exercised by the ombuds institution, the Chancellor of Justice, who may undertake ex post review both on its own initiative and further to a complaint. It can recommend changes to the legal framework and can initiate judicial review of the same by the Constitutional Court.[333] In Slovakia, the oversight of intelligence services is divided among five different oversight bodies: one specialises in reviewing decisions taken by the National Security Authority, three in reviewing the performance of the intelligence services (one per service), and a recent special commission was set up to supervise the use of information technology tools. This commission must include two independent experts, chosen by the parliament, who have at least ten years of professional experience as either police officers, prosecutors, judges or members of an intelligence service.[334]

The representatives of the oversight bodies (expert bodies, parliament committees and data protection authorities) were asked to assess their body's mandate in terms of its ability to conduct effective oversight over intelligence gathering. Powers to investigate, the scope of investigations, the implementation of their propositions, control limitations, and related matters were addressed. Most respondents described their current mandates as 'sufficient', 'robust', 'solid', 'clear', and as having 'broad powers', and claimed that these encompass important powers. Among the powers supporting the robustness of their mandate, respondents most often mentioned the following features along with defined powers (e.g. ex post oversight): (a) full access to intelligence information, including on-site visits to premises and direct contact with staff; (b) independent investigations and the ability to choose the subjects of investigations and which data collection techniques to investigate; (c) opinions, recommendations provided (e.g. on legislation).

Even where respondents considered the mandate of their oversight body to encompass sufficient powers, they mentioned the non-binding nature of their decisions (examples provided in France, Italy and the Netherlands) or limited competence as limitations (e.g., dealing only with a specific issue or stage of oversight or only with exceptional situations). A few respondents stated that the current powers are insufficient – and the impact of oversight low – and need to be expanded.

While discussing the role of DPAs in intelligence oversight, respondents highlighted that other actors in the field recognise their powers and expertise. In the past few years, an 'important level of listening' has been reached. The interviewees provided examples of regular consultation on relevant issues, including draft legislation (particularly in France, Italy and the United Kingdom). They maintained that they do see their contributions making an impact in terms of changes to legal frameworks. They also stated that DPAs' contributions – through cooperation with other institutions; by submitting opinions on relevant issues, annual reports, and special reports to the parliament; and by providing evidence during parliamentary

331 Italy, Italian Government (2013). See also COPASIR (2014), p. 19.

332 Sweden, State Official Reports (*Statens Offentliga Utredningar*) (2016), pp. 169 *et seq.*

333 Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), 1 May 2016, Article 1 para 9.

334 Slovakia, Act No. 404/2015 Coll. amending and supplementing Act N. 166/2003 Coll. on the protection of privacy against unauthorised use of information-technological tools and on amendment of certain laws (Act on protection against eavesdropping) (*Zákon, ktorým sa mení a dopĺňa zákon č. 166/2003 Z. z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane predodpočúvaním) v znení neskorších predpisov*), 19 December 2015, art. 8(a).

hearings or discussions, etc. – enhance the transparency of the intelligence oversight process. The interviewees believe that DPAs serve as 'a constant reminder to the balance of rights', raising public awareness on possible rights violations.

"In the past year, the consulting activity that is requested by [intelligence services] increased considerably. We were consulted three times, [...] opinions were requested. The DPA activities are perceived as important." (Data protection authority)

However, despite their recognised expertise in the area, DPAs feel they are operating in a 'fragmented system' ('fragmented nature of the regimes'). They noted that they have limited powers in the intelligence oversight process – for example, by focusing solely on data processing and not the techniques used; having oversight only of a specific step/stage in the process, such as ex ante; limiting their review to compliance with data retention rules; or having only indirect access to data. These give DPAs a sense of lacking power – as being unable to follow 'the file as a whole'. Interviewees also mentioned that they sometimes do not fully understand the competences of all the other actors in the field.

"[It is important] to make sure each body with powers in this area has an understanding about what one could do... But I think the concern is really around the fragmentation, complexity, lack of transparency." (Data protection authority)

"The other bodies are very important because the DPA cannot go as far in its review." (Data protection authority)

DPAs repeatedly emphasised the importance of institutional cooperation with different national and international authorities, the coordination of activities, and the complementarity of different actors' activities in the field. They acknowledged that they interact with few other national authorities, but noted that they have been developing beneficial cooperation with intelligence services (e.g. 'from suspicion to increasingly seen as a partner'; '[a] bond of trust is being established'). The interviewees noted that some of the cooperation is not formalised, and that it remains fragmented, selective and occasional. The Article 29 Working Party was referred to as the main forum for international cooperation, although differences between DPAs' competences in intelligence oversight hinder further cooperation.

"[Some] DPAs feel uncomfortable because they have no expertise in the field in question, and therefore stop themselves from even thinking about it."

(Data protection authority)

Providing oversight bodies with sufficient financial resources is key to ensuring that their oversight is effective.[335] Human resources also play a key part. A certain parity between the powers of the overseer and the mandate and powers of the intelligence services also contributes to the effectiveness of the oversight structure. Especially in view of the trend of intelligence services increasing their technological capacities, financial resources and their reliance on complex systems, "recourse to independent technical expertise has become indispensable for effective oversight".[336] Therefore, highly specialised legal and technical knowledge constitute particularly important resources for oversight systems.

The 2015 FRA report emphasised the need for oversight bodies to be technically competent.[337] Several expert bodies have tackled this issue by recruiting external technicians, either on an ad hoc or more permanent basis. In December 2014, the Dutch CTIVD established a 'knowledge network' of scientific experts (in the fields of security, intelligence, and information law) to regularly advise the Review Committee on specific reports relating to technological, legislative and social developments.[338] Indeed, with the increased sophistication of surveillance techniques, often automatised, the CTIVD recognised the need for ICT expertise and invested additional financial resources in technology for carrying out oversight. The CNCTR is provided with the human, technical and budgetary means needed to accomplish its missions.[339] A secretary general and 14 staff members assist its work.[340] It can also consult and answer the questions of the Electronic Communications and Posts Regulatory Authority (*Autorité de régulation des communications électroniques et des postes*, ARCEP).[341] In the United Kingdom, the Investigatory Powers Act requires the IPC to establish a Technology Advisory Panel, mandated to provide advice on "the impact of changing technology on the exercise of investigatory powers and the availability and development of techniques to use such powers while minimising interference with privacy".[342] Although not yet fully functional, IPC has already started identifying experts to fill this new panel.

While discussing the skills available in their institutions, the respondents – representing a variety of oversight bodies – confirmed that oversight of intelligence collection is dominated by legal expertise. Most interviewed staff working on relevant issues at expert oversight bodies, data protection authorities, ombuds or national human rights institutions have legal

335 Council of Europe, Commissioner for Human Rights (2015), p.9.
336 *Ibid.* p.10.
337 FRA (2015a), pp. 43, 60 and 73.
338 The Netherlands, CTIVD (2015), p. 10.
339 France, Interior Security Code (*Code de la Sécurité Intérieure*), Art. L. 832-4, first sentence.
340 France, CNCTR (2016), p. 60.
341 France, Interior Security Code (*Code de la Sécurité Intérieure)*, Art. L. 833-11.
342 United Kingdom, Investigatory Powers Act, s. 246 (1).

backgrounds. In some Member States, the legislation envisages a legal background for the staff and/or members of the committees. In a few Member States, information about the staff's background and possible needs was not made available for FRA's research.

"In principle, we are a committee of legal experts. […] As far as the secretariat is concerned, the staffing plan determines which qualifications are required." (Expert body)

Civil society organisations active in this field mainly engage lawyers. In some cases, their legal capacity is supported by technical experts, or certain knowledge is developed through involvement in the field. Many organisations have been involved in litigation on a variety of issues relating to data protection or privacy, including cases alleging unlawful data processing by intelligence agencies.

"We need more computer people." (Expert body)

"One area where we need to get some more expertise is in the technical field, maybe someone who knows more about data analysis, algorithms, that need is increasing."

(Expert body)

"You need someone who has the necessary expertise to understand specific technical processes. In my view, none of the members of the [expert body] are so well-versed in technical matters that they are able to assess complex situations – in particular situations concerning the [services] - on the basis of their own knowledge." (Expert body)

A few oversight body representatives said they have legal and technical expertise, and emphasised the importance of having both. In some cases, this combination was noted as a recent development. A few respondents believed that their technical capacity was sufficient, and no specific changes were needed. An absolute majority of the interviewees identified a great, increasing need for technical expertise, which is currently missing. Representatives of expert oversight bodies, parliamentary committees and executive control institutions expressed a clear demand for technical expertise, which is perceived as highly advantageous and beneficial for their authority. The respondents indicated that they believe a lack of technical expertise will remain one of the biggest challenges in the oversight field in the coming years.

"Regarding the intelligence services: it is working well for the moment but the growing technical complexity means that the DPA will have to increase its technical staff of IT experts who will be able to provide real technical expertise, particularly on the protection of data banks."

(Data protection authority)

The major need for technical expertise was acknowledged by oversight bodies and other experts in the field. During interviews, respondents representing civil society organisations, practicing lawyers and academia criticised the oversight bodies' limited technical capacity in terms of staff with technical background. As one respondent put it, 'with all my respect, they are not young IT types that you should have in an organisation as such'. Technical competence (capacity) was often mentioned by the respondents as one of the main features of effective oversight.

In terms of having sufficient resources, approximately two out of three respondents from oversight bodies expressed satisfaction with currently available human resources. Comments included that these 'are adequate', 'as things currently stand, it is remarkable', 'at the moment meet the needs', 'staff numbers are reasonably stable', 'there is no need to be expanded', 'it is effective because it is not too big', 'enough resources', and 'we have what we want'. Examples of these kinds of assessments were provided in most Member States.

Assessments of the size of the staff differed across the institutions. For example, some respondents said oversight can be effective in a small (limited) circle; others referred to limited resources, an increasing workload and the complexity of the work ('the work has become more complicated and [numbers of] investigators are no longer adequate'); and some indicated that they were in the unsatisfactory situation of being understaffed and said there was a clear lack of human resources.

"In the past, cases were simple; now they are more complex. The use of specific methods and appeals have increased, in technicality and volume." (Expert body)

"Even though we have not always been fully staffed, public confidence in our body has significantly increased due to the greater transparency of our procedures and the decisions we have made." (Expert body)

With regard to technical capacities, the respondents quite often noted difficulties in recruiting technical staff (ICT specialists) because the public sector is not able to compete with the private sector in terms of salaries. According to respondents, the same applies both to the intelligence services and their oversight.

Among the requirements for staff of oversight bodies, many respondents mentioned security clearance – the highest level of confidentiality in most cases – as the main criteria. Some said that the clearance procedure does not hinder recruitment and is not a restricting factor (e.g., 'an accelerated clearance procedures can be applied during the recruitment process'). Others said that it takes time and prolongs recruitment and might

be unattractive to possible candidates ('it is very tough procedure', 'it takes 4-5 months').

Among other difficulties faced by oversight bodies regarding resources, respondents mentioned the following issues: staff turnover, which can affect credibility and might risk leaked information; part-time staff (e.g. judges) with competing private practices; and a lack of control over outsourced staff.

Regarding budgets, opinions varied – ranging from being positive about sufficient budgets, recent increases or adequate funding to references to a lack of financial resources.

Respondents were also asked if they could hire or recruit additional external staff in case of need. There are no common opinions and experiences in this regard as situations differ quite extensively. In some Member States, oversight bodies have no possibility to hire external expertise; in other Member States, oversight bodies have never used this opportunity although it is provided for in the relevant legislation. In some Member States, expert bodies receive external support, including from academia, when needed. Still, the outsourcing of expertise is rare. Most institutions rely on available internal resources.

"The oversight process is becoming an extremely technical and massive task." (Expert body)

Some interviewees referred to computerised/automated oversight tools, including those built into the software used by intelligence services, as providing possibilities for furthering technological development and strengthening oversight. These include "automated checking", "the ability to carry out a technical verification at regular intervals", and "updates of the data banks", including "computerised clean-up techniques" or "automated data destruction". Other respondents refer to these as providing an important opportunity to identify possible violations at an early stage, and encourage application of, for example, data protection oversight by design. They are also considered a positive feature for the intelligence services, bringing more balanced oversight and a possible solution for oversight bodies' need for technical expertise. In some Member States, strategies for implementing such tools have recently been developed or implementation has just started. The oversight experts noted the importance of following closely ICT developments in the agencies themselves, and progress in understanding the digital world among the various stakeholders.

"At minimum, there must be very close cooperation governed by law, and not just dependent on the will and the intention of the acting persons." (Data protection authority)

Finally, in connection with resources, interviewees repeatedly pointed out that not only the resources themselves matter, but the way institutions work and communicate with each other does, as well. The interviewed experts generally raised the importance of cooperation in its different constellations – including with intelligence services, executive control; between oversight bodies; with civil society – and natures (e.g. prescribed by law by different functions, formalised through a MoU, informal exchanges) when discussing different topics, such as effective oversight, measures to uphold fundamental rights, and the transparency of the activities of both intelligence services and oversight bodies.

According to the interviewees, cooperation through 'constant dialogue' and 'continuous sharing of information' contributes to having a systematic approach to oversight and helps overcome possible fragmentation of the oversight system. Likewise, sharing good practices helps build trust, and sufficient levels of trust allow actors to cooperate. The respondents also expressed a great need for both national and international cooperation, and exchanges of information and best practices in the area. The *General Data Protection Regulation* gives advisory powers to DPAs when Member States draw up legislative or administrative measures. Therefore, DPAs can contribute by pointing out potential threats to data protection when Member States plan to modify surveillance powers granted to intelligence services.

Swedish government preparatory study recommends stronger role for DPA

In 2016, the national government appointed an expert committee to examine how a higher degree of integrity protection can function within a single governmental department, allowing thus the supervision of collection of personal data to be also attributed to a single authority. The expert committee issued a 222-page report which provides an overview of the role of the committee and previous work in the area, then scrutinises the current system of supervision and how it could be improved.

While the general assessment is positive, it does, for instance, call for some simplifications or clarifications in relation to the mandate of control functions. In particular, the committee recommends giving the DPA a more central role, mainly in relation to provisions in sector-specific legislation that are of a more general nature (such as related to cookies), and states that other monitoring bodies should consult the DPA or even hand issues over to it to resolve them.

Sweden, Government preparatory study (2016), 'Joint responsibility over personal integrity'

9.3. Openness to public scrutiny

The ECtHR puts great emphasis on the liability for the executive but also the oversight body to give account on their respective work in the area of intelligence services oversight.

ECtHR case law: executive and oversight bodies subject to public scrutiny

"The Court notes at this juncture the liability of the executive to give account, in general terms rather than concerning any individual cases, of such operations to a parliamentary committee. However, it cannot identify any provisions in Hungarian legislation permitting a remedy granted by this procedure during the application of measures of secret surveillance to those who are subjected to secret surveillance but, by necessity, are kept unaware thereof. The Minister is under an obligation to present a general report, at least twice a year, to the responsible parliamentary committee about the functioning of national security services, which report, however, does not seem to be available to the public and by this appears to fall short of securing adequate safeguards in terms of public scrutiny [...]. The committee is entitled, of its own motion, to request information from the Minister and the directors of the services about the activities of the national security services. However, the Court is not persuaded that this scrutiny is able to provide redress to any individual grievances caused by secret surveillance or to control effectively, that is, in a manner with a bearing on the operations themselves, the daily functioning of the surveillance organs, especially since it does not appear that the committee has access in detail to relevant documents. The scope of their supervision is therefore limited [...]."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 82

Oversight bodies need to be transparent and provide adequate information to the public about their activities and those of intelligence services. This is because oversight systems serve the ultimate goal of protecting the public against abuse in the implementation of surveillance measures. Due to their independent status, the various bodies of oversight systems are ideally placed to provide credible and reliable information to educate the public about the activities and role of intelligence services.[343]

Member States and oversight bodies take very divergent approaches when it comes to the regulations and/or practices aiming to provide for the transparent functioning of the oversight system. Considering the secret nature of the techniques and operations, it is beyond dispute that full transparency of oversight is neither possible nor desirable. However, as high a degree of transparency as possible is indispensable for ensuring that citizens can understand and thus trust the functioning of the oversight system and, consequently, that of the secret services.

In the United Kingdom, for example, the Investigatory Powers Commissioner must report "as soon as reasonably practicable after the end of each calendar year"[344] or at any time requested by the prime minister[345] or where the commissioner considers it appropriate.[346] With respect to the commissioner's annual reports, the prime minister has an obligation to publish them, and lay a copy thereof before parliament together with a statement on any matter that has been excluded.[347] Therefore, the prime minister has the power to exclude matters from the published report but may do so only after consultation with the commissioner.[348] The grounds on which some matters can be excluded are laid down in law.[349]

Representatives of oversight bodies were asked how their institutions contribute to the implementation of transparency in oversight. Issues relating to transparency were raised by the respondents while addressing accountability and the effectiveness of oversight, too.

In general, according to the interviewees, transparency is a relatively recent topic in the area of intelligence collection and its oversight. The Snowden revelations have significantly contributed to transparency – for example, several oversight bodies indicated that, 'in reaction to the Snowden leaks afterwards many governments all of the sudden published information *that beforehand was considered secret.*' The effects are reflected in publications, increased efforts to improve general communications, information exchanges and institutional cooperation. To a certain extent, the issues relating to transparency were mentioned in the context of upholding fundamental rights during the collection of intelligence and its oversight.

343 Council of Europe Commissioner for Human Rights (2015), p. 65.

344 United Kingdom, Investigatory Powers Act, s. 234 (1).
345 *Ibid.* s. 234 (3).
346 *Ibid.* s. 234 (4).
347 *Ibid.* s. 234 (6).
348 *Ibid.* s. 234 (7).
349 *Ibid.*

"It is rather difficult to talk about transparency in relation to services whose effectiveness depends upon secrecy."

(Parliamentary committee)

"The issue of transparency is discussed in connection with an area of activity the very principle of which is a lack of transparency, since classification of information as secret puts a limit on transparency." (Expert body)

"There is a lack of transparency on this issue, due in particular to its degree of technical complexity, which is itself heightened by the difficulty in accessing information, since the intelligence services are not very communicative."

(Civil society organisation)

While discussing transparency issues, many oversight body representatives mentioned existing limitations for transparency in the oversight of intelligence collection. Some respondents believe the general culture of secrecy around intelligence services interferes with transparency, and that the lack of transparency is inevitable. The limitations or lack of transparency are related to a great variety of issues, such as technical complexity, classification of information, level of secrecy ('the trade-off between transparency and secrecy'), and restrictions and limitations defined by legislation, which have to be respected. Some respondents said that secrecy constraints serve as a tool to keep the procedures implemented properly, e.g. observing classification levels. Some interviewees believe that transparency can nonetheless be maintained through cooperation or communication between the different institutions and public authorities that operate in the area.

According to Born and Wills, useful elements for achieving maximum transparency include availability of information about the conduct of the oversight bodies, regular reporting to a relevant authority and occasional publication of special reports.[350] Regarding these key aspects, it is relevant whether the oversight bodies have open sessions, whether their members are allowed to comment on their findings, and whether the body issues comprehensive, regular and largely informative reports. At the same time, the effectiveness of providing transparency will inevitably depend on the powers of the oversight bodies, as that will, among others, define the quality and quantity of information they have access to in the first place. As emphasised in FRA's 2015 report, expert bodies' ability to publish public versions of periodic and investigation reports is essential.[351]

The meetings of the Dutch CIVD are strictly confidential. It publishes an annual report, addressed to the House of Representatives, with information about the number of meetings and the agenda items.[352] The report of the Intelligence and Security Committee of the United Kingdom, whether annual or *ad hoc*, usually contains redactions on security grounds suggested by the services – but these must be justified, and the committee has the final say.[353] In a case of major disagreement, the prime minister may exceptionally insist on a redaction before a report is sent to parliament (the redaction is reported).[354] The ISC may also choose to report privately to the prime minister if a national security matter is exceptionally sensitive[355] – an example might be the handling of an ongoing espionage case. Though members of the German Parliamentary Control Panel 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.[356] It reports to the parliament twice during the legislature.[357]

FRA analysed some of the key features of the publicly accessible reports prepared by expert bodies[358] (Annex 3) and parliamentary oversight committees (Annex 4) in several Member States. A report's length can indicate the level of detail provided therein and thus how transparency is observed. For example, in 2016, the Belgian Standing Committee I produced an annual report of 131 pages. By contrast, the German G10 Commission published a 10-page report. However, some expert bodies publish separate reports on specific investigations conducted and exclude this information from their annual reports. It is also not uncommon for parliamentary committees to prepare *ad hoc* thematic reports, as is the case in the United Kingdom[359] and Italy.[360]

350 Born, H. and Wills, A. (2012), p. 80.
351 FRA (2015a), p. 41.

352 The Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*) (2016), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page.
353 United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), p. iv (foreword).
354 United Kingdom, Justice and Security Act 2013, ss. 2 (3) and 2 (4) of Part 1.
355 United Kingdom, House of Commons Library (2017), p. 6.
356 Germany, PKGrG, S. 10 (1). See Bartodziej, P. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1556 and following.
357 See Germany, Federal Parliament (*Deutscher Bundestag*) (2016), the latest report covering November 2013 to November 2015. See also de With, H. and Kathmann, E. (2011), Policy Department C: Citizens' Rights and Constitutional Affairs, p. 218; Heumann, S. and Wetzling, T., Stiftung neue Verantwortung (2014).
358 Excluding data protection authorities.
359 For example, see United Kingdom, Intelligence and Security Committee of Parliament (2015).
360 For example, see Italy, COPASIR (2015), 'Report on so-called "Butterfly" and "Return" operations and on the affair "Flamia"' ('Relazione sulle cosiddette operazioni "Farfalla" e "Rientro" e sulla vicenda "Flamia"'), Rome, 12 March 2015.

In general, expert bodies' reports describe the surveillance legislation in the Member State concerned and outline the particular expert body's mandate, powers and internal functioning. Depending on these powers, the expert bodies present statistics on authorisations of surveillance measures and the ex post controls and investigations they conducted. In exceptional cases – for instance, in France and Germany – the number of individuals that were under surveillance during the reporting period is stated, as well as the purpose pursued by the surveillance. In France, the CNCTR has the possibility to publish the total number of people under surveillance because it controls all surveillance techniques in France. Between 3 October 2015 and 2 October 2016, 20,282 persons were subjected to a surveillance technique.[361] In Germany, the Parliamentary Control Panel publishes information on the number of individuals under targeted surveillance (pursuant to Section 3 of the G 10 Law). In 2015, there were 336 primary targeted persons (*Hauptbetroffene*) during the first semester and 322 in the second half of the year; and 249 indirectly targeted persons (*Nebenbetroffene*) during the first semester and 224 during the second. This means that 1,502 telecommunication connections (*Telekommunikationsanschlüsse*) were tapped during the first semester, and 1,336 during the second half of 2015.[362]

The Belgian Standing Committee I also publishes very detailed numerical information on surveillance authorisation issued to the services. These are separated according to each service and each surveillance method (specific and exceptional).[363] Where applicable, most annual reports contain statistics on the outcomes of complaints by individuals. Some expert bodies also report on their interactions with other domestic institutions and foreign expert bodies. Given that the expert bodies in parallel have an advisory role, some of them provide, in their annual reports, recommendations to governments concerning good practices and legislative improvements.

The Dutch CTIVD has criticised the ban on the publication of the number of wire taps performed by the intelligence services. It has noted that publishing mere tapping statistics does not reveal the factors affecting the number of interceptions, or the techniques used for such purposes. In addition, it does not influence the priorities or reveal sensitive information on the technical capacity of the intelligence services. Therefore, it has claimed that national security is not endangered.[364] Based on the CTIVD's opinion, the Dutch Council of State in 2016 annulled a decision of the Minister of Interior not to make tapping statistics available to the NGO Bits of Freedom following a Freedom of Information request.[365]

Parliamentary reports focus on the number of hearings conducted and the list of witnesses heard. Annual reports rarely provide details about the content of the hearings. However, this is done, for example, in Italy and the United Kingdom. In the United Kingdom, reporting on the hearings is not limited to a brief summary of the proceedings. An extensive degree of transparency is achieved by providing links to the full transcripts of the proceedings. Parliamentary committees tend to report on the budget of the intelligence services as well as the threats the intelligence services focused on during the reporting period. Parliamentary committees also provide explanations of the oversight methods used to gather information from the intelligence services and, when applicable, present statistics on the investigations conducted and the outcome of complaints received by individuals.

Overall, an analysis of the reports of expert bodies and parliamentary committees in several Member States shows that particularly in Belgium, France and United Kingdom, expert bodies or parliamentary committees have substantially taken into account transparency requirements. Their reports are accessible and provide detailed overviews of the concerned oversight systems and the results these produce, depending on their competence (e.g. extensive statistics on use of surveillance techniques, authorisations, *ex post* controls and complaints-handling). They also make use of their advisory role towards the government and outline recommendations regarding current practices and legislative reforms, while informing the public about the inter-institutional dialogue they conducted during the reporting period.

361 France, CNCTR (2016), p. 73.
362 Germany, Federal Parliament (2017), p. 5.
363 Belgium, Standing Committee I (2016), p. 49 and following.
364 The Netherlands, CTIVD (2012), pp. 26-28.
365 The Netherlands, Administrative Jurisdiction Division of the Council of State (*Afdeling Bestuursrechtspraak van de Raad van State*) (2016), *Case no. 201505432/1/A3*, 4 May 2016.

Promising practice

Promoting transparency in oversight

Regularly issuing detailed reports

The Italian COPASIR, the French DPR, the German PKGr and the United Kingdom's ISC are legally obliged to regularly publish reports. This promotes transparency by regularly informing parliament and the public about the parliamentary oversight committees' work.

Italy, COPASIR (2017); France, DPR (2017); Germany, PKGr (2016); and United Kingdom, ISC (2016)

Reporting on number of parliamentary committee sessions

In Italy, France, Germany and the United Kingdom, parliamentary oversight committees report on the number of sessions held during the reporting period. This allows the public to be informed about the amount of time invested in overseeing the work of intelligence services.

Italy, COPASIR (2017); France, DPR (2017); Germany, PKGr (2016); and United Kingdom, ISC (2016)

Reporting on content of parliamentary committee hearings

The United Kingdom's ISC provides in its annual report a link to the transcripts of the hearings held during the reporting period, hosted on its website, thereby providing a significant level of information about its work

United Kingdom, ISC (2016)

Reporting on number of staff of intelligence services

The United Kingdom's ISC and the French DPR specify the number of staff working for each of the intelligence services. This means the public is informed about the size of intelligence services.

United Kingdom, ISC (2016); and France, DPR (2017)

Availability of expert bodies' annual reports in English

The Belgian Standing Committee I, the Dutch CTIVD, the French DPR, the Danish TET and the Greek ADAE publish their respective annual reports in both the original language and in English. This promotes cooperation and a better understanding of the oversight bodies' work beyond national borders.

Belgium, Standing Committee I (2016); Netherlands, CTIVD (2016); France, DPR (2017); Denmark, TET (2017); and Greece, ADAE (2016)

Reports on safeguard breaches by intelligence services

The United Kingdom's IOCCO reports on interception errors by the intelligence services. IOCCO lists the safeguards provided by the surveillance legislation and presents statistics on the breaches per safeguard by the intelligence services.

United Kingdom, IOCCO (2016)

Reports on number of individuals under surveillance

The French CNCTR and the German G10 Commission's annual reports provide statistics on the number of individuals that were under surveillance during the reporting period. The data come from the exercise of the oversight powers granted to these expert bodies.

France, CNCTR (2016); Germany, Federal Parliament (2017)

Report on intelligence services cooperation

The Belgian Standing Committee I's annual report published in 2016 presents the committee's endorsement of international cooperation of intelligence services regarding foreign terrorist fighters. In the report, the committee also outlines a number of principles that should govern international cooperation among intelligence services as well as its oversight.

Belgium, Standing Committee I (2016)

When discussing transparency requirements, representatives of oversight bodies most often referred to their reports or other publications. The reports include annual reports, activity reports, investigation reports and other specific (occasional, thematic) reports, in addition to mandatory reports. In most cases, there are two versions of the reports prepared by oversight bodies: classified and declassified, or secret/redacted and public versions. Similarly, reports may include a confidential annex.

Representatives of oversight bodies described the reports as substantive, detailed and lengthy. They stated that discussions with the executive control and intelligence services on what is to be declassified in their reports are sometimes quite intense. The oversight body representatives also indicated that, with nearly every report or publication, they attempt to provide 'more transparency', 'to push the limit', to be able to report as much as possible, and to explain and substantiate why certain information is kept secret and cannot be published. This is viewed as contributing to the changing nature of the 'secret culture'. Other actors who engage in democratic control – mostly civil society representatives – have observed such changes, too.

Question: *"Do you have lots of discussions whilst the report is being drawn up?"*

Answer: *"Yes. This was particularly the case with the first report, in connection with which there was a real desire to educate and explain matters properly."*

(Parliamentary committee)

"Have we actually got more in our report? The answer is we do and I think that, following Mr. Snowden, there was undoubtedly greater pressure to put more in and this new legislation is a good example, where much more openness is being encouraged and I think we will go on pressing..."

(Expert body)

Many oversight body representatives said that it is important for the general public to know that some information is classified/secret/redacted, rather than publishing a report and implying that it is complete. They noted that the arguments for excluding certain information from reports are important and should be communicated.

"I think people need to realise how much of what we do is secret and it is such a small amount, and it really is only when there are real national security issues." (Expert body)

Respondents also talked about opinions, recommendations and proposals, and studies on specific issues that respond to specific requests or are initiated by the oversight bodies themselves.

The interviewees considered any other information to the general public or specific interest groups (e.g. journalists) to add to transparency – for example, information on the website, communications to encourage individuals to appeal to the review body, the ability to initiate 'contact' through the website, press releases, provision of information to media 'on request', and making decisions (judgements) available on the website. Participation in conferences and other events was mentioned by several respondents as ways to hold discussions within a wider international framework, as well as with civil society and the media.

Representatives of civil society organisations, academia, lawyers and some national human rights institutions tended to be critical of the content of oversight body reports and their transparency in general, and indicated they expected more. The main criticism was that there is very limited information on actual activities and little explanation of how the oversight or review is carried out, while the main focus is on describing the relevant legal basis.

"I think one third of the report is what they regularly say every two years... 'this is our legal basis...', and I say 'this is not what I want to know'. I want to know a bit more about their work." (National human rights institution)

"It sets out what it does, on what legal basis... blah, blah, blah. And there's nothing else in there. Absolutely nothing."

(Academia)

"But when it comes to the substantive issues, let's say: what have we learned from the [expert body]? How many interceptions have there been? Not just how many times did we meet, but what was the substance of that discussion. Were there any novel decisions? Were there any novel technologies that came to our attention? I want to know about this." (Civil society organisation)

"What's actually going on? We always had a feeling or hints that what was revealed in the Snowden revelations was in one form or another happening. But no one really knew substantially. The reform just now, even many members of parliamentary oversight committees I have talked to, say they only learn about these things from the media - and not from the official channels they are supposed to learn them from..." (Media)

Respondents representing various institutions mentioned diverse ways to improve transparency and to make themselves more open. Some spoke of possible improvements with regard to reporting (e.g. 'The reports could also go a little further without impacting on confidentiality concerns'). Others noted that the bodies should themselves be able to decide on what to report. Some expected legal reforms to introduce mandatory reporting by oversight bodies. Several representatives of expert oversight bodies mentioned

hiring communications consultants to improve communications (regarding information to the public, by reviewing/editing the reports 'to help turn our language into something that is accessible to anybody and to try and make it more obvious'). The recent disclosure of the location of an office was mentioned as an example of positive change.

Respondents representing different institutions and organisations pointed to different recent examples that they believed showed changes in the predominant culture of secrecy. Such developments involve both the intelligence services and oversight bodies. With regard to the intelligence services, for example, civil society members from the Netherlands noted that the head of the intelligence service is publicly known, is willing to participate in different forums, and 'is approachable'. Intelligence service representatives attend conferences and other public events, including some organised by academia. Examples of comments about changes in the United Kingdom include: 'you go to conferences now and you find people engaged in a civilised discussion with people from security side about the issues'; a round table convened 'a quite high profile group of individuals both from the government side and the agencies, and the existing oversight bodies, but also from privacy campaign side and individuals who are bringing cases'. Meanwhile, in Germany, after the Snowden revelations, the parliamentary control panel for the first time published its rules of procedure on its website.[366]

Respondents indicated that intelligence actors' participation in, and presentations at, national parliamentary hearings make important contributions to transparency. Members of parliamentary committees referred to these hearings, some of which are public, as an important information channel for the public who can watch, e.g., the heads of the intelligence services being interviewed.

366 Germany, Federal Parliament (*Deutscher Bundestag*) *Parliamentarisches Kontrollgremium (*2016), Rules of Procedures (*Geschäftsordnung*).

10 Stages of intelligence service oversight

Effective oversight of surveillance operations requires potentially being present at every stage. The ECtHR refers to this as 'continuous control' in the *Roman Zakharov* case. Factors that have a bearing on the effectiveness of oversight include: the independence of the relevant body, the scope of measures requested (targeted or general surveillance of communications; content or metadata; domestic or foreign), its powers to access or request information, and its resources – in terms of staff, time and expertise, including with a view to the number of warrant requests received. For *ex ante* oversight, the level of required detail in a warrant and the time period for which the warrant is provided is also relevant, especially in cases where ongoing oversight is weak.

This report's discussion of the implementation of the standards gives particular attention to ongoing and ex post oversight. A more detailed treatment of such oversight is given below, because it is at the stage of implementation of surveillance measures that safeguards on general surveillance of communications operations are most relevant.

ECtHR case law: stages of oversight

"Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 233

10.1. *Ex ante* authorisation and oversight

ECtHR case law: *ex ante* authorisation

"The Court will take into account a number of factors in assessing whether the authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration. These factors include, in particular, the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation."

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 5 December 2015, para. 257

"The Court recalls that [...] it expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 77

UN good practice on intelligence collection and oversight

Practice 22. [...] 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 (2010), Report of the Special Rapporteur Martin Scheinin

Continuity of oversight of surveillance operations requires, among others, that independent oversight be present at the stage when the surveillance measures are first ordered. The overseers must therefore be informed at once of the issuance of warrants. 'Authorisation' entails the issuing of a warrant, while 'approval' refers

to the review of a signed warrant before it is put into effect. Ex ante authorisation or approval by independent overseers is not yet common in EU Member States, but can be seen as a promising practice both to ensure that surveillance operations are fully justified as necessary and not ordered arbitrarily, and to enable meaningful ex post review of the warranted operations. Ex ante oversight may either take the form of the independent body actually authorising the warrant or of conducting an approval process involving independent review of a signed warrant before it enters into force.

"The ideal situation would be to never have to say 'no'. This is what I would like to aim for in the future; an understanding of the intrinsic and legal limits [by the services]." (Judiciary)

Supervision by the judiciary or experts

"[T]he value of judicial control depends upon the expertise the judges in question have in assessing risks to national security and in balancing these risks against infringements in human rights."

Council of Europe, European Commission for Democracy through Law (Venice Commission) (2007), Report on the democratic oversight of security services, *para. 206*

In Belgium, the State Security, before using exceptional methods of surveillance, must submit a duly motivated, written request to the Administrative Commission.[367] The Administrative Commission gives its opinion on such requests within four days. If the decision is negative, the proposed measures may not be implemented.[368] In case of a positive decision, the Administrative Commission notifies the Standing Committee I, which can overrule the commission's decision.[369]

In the United Kingdom, the double-lock system was introduced in 2016. It will require, once in force, that warrants or notices for both targeted surveillance and using bulk powers be authorised by the Secretary of State[370] and subsequently approved by the Judicial Commissioner.[371] The Judicial Commissioner is required to review whether the warrant or notice is necessary on relevant grounds and whether the measures applied for are proportionate to their aim. The warrant or notice can take effect only after the Judicial Commissioner has approved it.[372] Warrants are valid for six months,[373] and retention notices can require the retention of data for 12 months.[374] In the case of bulk interception warrants, for example, the requested measure should relate to the interception of overseas-related communication (either content or metadata). This means that for the communication to be intercepted, it must be sent or received by someone outside British territory.[375] In authorising the measures, the Secretary of State must ascertain that they are necessary to prevent serious crime, and/or ensure the economic well-being or national security of the state.[376] The Judicial Commissioner then reviews whether the measures are necessary and proportionate and can quash a warrant if not satisfied.[377]

However, with regards to the effectiveness of ex ante reviews of bulk measures, it is noteworthy that the core requirement in the UK system regarding the contents of the warrant is that it must specify the operational purpose(s) of the requested measures "in a greater level of detail" than described above.[378] Thus, in turn, the actual strength of the *ex ante* review relating to the necessity and proportionality of the requested measures will, to a great extent, depend on the level of detail regarding the purposes. This is relatively straightforward for simple targeted warrants where the specified individuals or premises are known and can be specified. For warrants for surveillance involving bulk measures not only must the objective relate to a sufficiently high intelligence priority but the review will have to take into account what has been

367 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 18 (10).
368 *Ibid.* Art. 18 (10)(3).
369 *Ibid.* Art. 18 (10)(7).
370 United Kingdom, Investigatory Powers Act, s. 19 for interception and examination, s. 87 for retention of communications data, s. 102 for equipment interference. S. 19 and 102 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
371 *Ibid.* s. 23 for interception and examination; and s. 87 (1) (b) for retention notices, s. 102 (1) (d). ss. 23 and 102 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
372 *Ibid.* s. 23 (1) for interception and examination, s. 89 (1) for retention, s. 108 (1) for equipment interference. Ss. 23, 89 and 108 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
373 *Ibid.* s. 32 (2) (b) for interception and examination, s. 116 (2) (b) for equipment interference. Ss. 32 and 116 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
374 *Ibid.* s. 87 (3).
375 *Ibid.* s. 136 (2)-(3). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
376 *Ibid.* s. 138 (2). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
377 *Ibid.* s. 140. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
378 *Ibid.* s. 142. Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

previously established by the oversight body regarding the compatibility of the methods used (access, filtering and selection algorithms) to ensure the activity under the warrant will be compatible with privacy rights (Article 8 of the ECHR). In that way the overseer must, in the words of a UN Special Rapporteur, conduct the review such that "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."[379]

Authorisation and approval of targeted surveillance

A detailed comparison of authorisation and approval processes for targeted measures is difficult, as they may vary within Member States depending on the different types of surveillance measures involved, whether they relate to content or metadata, and whether they have a domestic or foreign focus. Table 4 shows the different bodies that have a binding/final decision in the authorisation or approval processes of different types of targeted surveillance measures relating to content data. The information provided for one Member State covers all potential actors with a binding decision-making power in allowing targeted surveillance measures. Six Member States have two or more approval bodies. In some cases (e.g. in the United Kingdom), one body is in charge of authorising and the other one of approving the measures. In others (e.g. in Hungary), the involvement of different bodies depends on the type of techniques used by the intelligence services.

Table 4: Binding authorisation/approval of targeted surveillance measures in the EU-28

	Judicial	Executive	Expert bodies	Services
AT			✓	
BE		✓	✓	
BG	✓			
CY		✓		
CZ	✓			
DE		✓	✓	
DK	✓			
EE	✓			
EL	✓			
ES	✓			
FI	✓			
FR		✓		
HR	✓			
HU	✓	✓		✓
IE		✓		
IT	✓			
LT	✓			
LU		✓		
LV	✓			
MT		✓		
NL*	✓	✓	✓	
PL		✓		✓
PT	✓			
RO	✓			
SE	✓			
SI	✓			✓
SK	✓			
UK**	✓	✓		

Note: * *Situation reflecting the requirements of the Intelligence and Security Services Act 2017, which will be applicable when the relevant sections enter into force.*

** *Situation reflecting the requirements of the Investigatory Powers Act, which will be applicable when the relevant sections enter into force.*

Source: *FRA, 2017*

379 UN, Human Rights Council (2014), Report of the Special Rapporteur Ben Emmerson, para. 7.

In general terms, as Table 4 illustrates, just over half of the Member States involve the judiciary (judges or prosecutors) in ex ante oversight, in relation to at least one type of targeted surveillance measure. In Portugal, the new law provides for access to metadata by intelligence services to be authorised by a judicial panel composed of the presidents of all criminal sections of the Supreme Court and a judge appointed by the Superior Council of Magistrates.[380] In Italy, requests for targeted interception measures need to be authorised by the Prosecutor General of Rome.[381] Three Member States – Austria, Belgium and Germany – involve expert bodies in all approval processes. At the same time, in six Member States – Cyprus, France, Ireland, Luxembourg, Malta and the Netherlands – all types of targeted surveillance measures may be implemented without ex ante oversight by an independent body with binding decision powers. In France, for example, requests for targeted surveillance measures are authorised by the prime minister after a non-binding opinion of the CNCTR, upon the receipt of a detailed request by the relevant minister, outlining the technique(s) to be used; the service for which it is presented; the purpose(s) pursued; the reason(s) for the measures; the period of validity of the authorisation; and the person(s), place or vehicles concerned.[382]

Ex ante oversight

There is growing support for extending external authorisation to:

- untargeted bulk collection of information;
- the use of key words or selectors to extract data from the information collected through bulk interception, particularly where they are related to identifiable individuals;
- the collection of and access to communications data (including when held by the private sector); and
- computer network exploitation.

Council of Europe Commissioner for Human Rights (2015), p. 62

Authorising general surveillance of communications

Unlike targeted surveillance, general surveillance of communications – at least during its initial stages – targets not an individual but rather large flows of data. As a consequence, such measures do not usually allow for an individualised proportionality analysis. *Ex ante* authorisation or approval has to focus on the seriousness of the objective of the operation as an intelligence requirement, the level of proportionality, and whether access, filtering and selection algorithms use discriminatory criteria. The analysis must establish whether the proposed operations are compatible with privacy rights. Table 5 presents the actors that have a binding/final say in the approval of general surveillance of communications measures in the five Member States that have detailed legislation on such surveillance measures.

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 Defence Intelligence Court, which can have four to nine members: two or three ordinary judges (the chair and vice chair; there can be a second vice chair), and two to six lay members.[383] The panel that hears a case and grants authorisations must be composed of at least the chair and two lay members (and not more than three lay members).[384] The government appoints all members. The chair and vice chair are appointed after an open recruitment process led by the Judges' Board (*Domarnämnden*).[385] Lay members of the court should have special knowledge in matters of importance to the court's activities.[386] The interests of individuals are represented by lawyers (*integritetsskyddsombud*) who are or have been members of the bar or served as judges, appointed for a four-year period.[387] The court may declare that its sessions are not public, and its decisions may not be appealed.[388]

In contrast, in France, when it comes to the use of the so-called 'algorithm', the prime minister authorises automatic processing based on selected parameters.[389]

380 Portugal, Organic Law No. 4/2017, of 25 August, approving and regulating the special procedure to grant the Security Intelligence Service (SIS) and the Defence Strategic Intelligence Service (SIED) access to communication and Internet data and proceeds to the amendment to the Law No. 62/2013 26 August (Law on the organisation of the Judicial System), Art. 7.

381 Italy, Code of criminal procedure (*Codice di procedura penale*), Art. 266 and following and Italy, Implementing norms (*norme di attuazione*), Art. 226.

382 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 821-2.

383 Sweden, Act on the Defence Intelligence Court (*Lag (2009:966) om Försvarsunderrättelsedomstol*), 15 October 2009, Art. 2.

384 *Ibid.* Art. 9.

385 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).

386 Sweden, Act on the Defence Intelligence Court, Art. 3.

387 *Ibid.* Arts. 5 and 6.

388 *Ibid.* ss. 3, 5, 6, 9, 14 and 16. Details are provided in Sweden, Regulation 2009:968 with instructions for the Defence Intelligence Court. The website of the court is available in Swedish only. The court was established in 2009, replacing a previously existing Signals Intelligence Board.

389 France, Interior Security Code, Art. L. 851–3.

Table 5: Approval/authorisation of general surveillance of communications in France, Germany, the Netherlands, Sweden and the United Kingdom

	Judicial	Parliamentary	Executive	Expert
DE		✓		✓
FR			✓	
NL*	✓		✓	✓
SE				✓
UK**	✓		✓	

Notes: * *Situation reflecting the requirements of the Intelligence and Security Services Act 2017, which will be applicable when the relevant sections enter into force.*

** *Situation reflecting the requirements of the Investigatory Powers Act, which will be applicable when the relevant sections enter into force.*

Source: *FRA, 2017*

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 renewal 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 again provides the prime minister with its opinion for authorising the identification of the person considered as threat. Since its creation in October 2015, no negative opinion from the CNCTR were overruled by the Prime Minister.[390]

As a general rule, when targeting communications' content data, prior oversight is required in most Member States for both targeted surveillance and the use of selectors in the context of general surveillance of communications. This changes, however, when intelligence services solely access metadata through rules governing access to retained data. In these cases, it is usually sufficient for the services' directors to authorise access.[391] This is problematic, because communications data reveal an individual's pertinent personal information in a similar way to content data.[392]

However, addressing any issue relating to prior oversight in isolation of the oversight system as a whole will not offer a complete picture of its effectiveness. Inevitably, national systems will strike different balances when designing their respective architecture of checks and balances. Consequently, apparent strengths or weaknesses of ex ante review may be undermined or remedied, respectively, in ongoing and ex post oversight.

10.2. Ongoing and *ex post* oversight

To meet the standard of continuity, oversight also needs to be present at the stage when the measures are being implemented – in other words, while the operations are ongoing – as well as at the time when they have already been concluded. In addition, oversight should cover all surveillance processes, from collection to the destruction of data.

The use of general surveillance of communications makes these functions of the oversight system particularly crucial safeguards, given that in such operations ex ante oversight will, by definition, have a limited scope of review. Ongoing and ex post oversight can also provide valuable insights in the form of feedback to the body authorising or approving general surveillance of communications. This section focuses on ongoing and ex post oversight of specific types of operations.

As Annex 5 illustrates, a number of Member States have expert bodies that undertake ongoing and ex post review, while only very few provide for judicial oversight during the implementation of surveillance measures. FRA's research shows that most Member States involve an independent oversight body either at the stage when surveillance measures are being implemented or after they have been concluded – or during both of these stages. Depending on the powers and competences of the oversight bodies at these stages, a combination of ongoing and ex post oversight may be the best approach.

390 France, CNCTR (2016), p. 66.

391 This is the case in the United Kingdom for targeted collection of metadata (Investigatory Powers Act, S. 61).

392 For the required safeguards in case of retention of data by telecommunications service providers, see CJEU, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Postoch telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson and Others*, 21 December 2016, and the analysis of the case in the Introduction.

10.3. Exceptional situations and special protection

Two circumstances need to be considered separately because they derogate from the general framework of ordering and overseeing surveillance operations. These involve urgent operations, and surveillance of specific professional groups that benefit from enhanced protection.

Exceptional situations

ECtHR case law: safeguards for the use of urgent procedures

"[W]here situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours [...]. For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a *post factum* review, which is required, as a rule, in cases where the surveillance was authorised ex ante by a non-judicial authority."

ECtHR, Szabo and Vissy v. Hungary, *No. 37138/14, 12 January 2016, para. 81*

"[T]he Russian 'urgent procedure' does not provide for sufficient safeguards to ensure that it is used sparingly and only in duly justified cases. [...] The domestic law does not limit the use of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-judicial urgent procedure, thereby creating possibilities for abusive recourse to it [...]. Furthermore, although Russian law requires that a judge be immediately informed of each instance of urgent interception, his or her power is limited to authorising the extension of the interception measure beyond forty-eight hours. He or she has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed [...]. Russian law does therefore not provide for an effective judicial review of the urgency procedure."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 266*

Member States' laws define cases of urgency as cases where undertaking the usual authorisation/approval procedures might irreversibly affect or undermine the purpose of the measures. This can occur because standard approval processes may take days. In urgent cases, safeguards are adapted to the extraordinary circumstances at issue, usually by way of a special ex ante approval procedure or via ex post approval. For example, Belgium provides for special ex ante approval in cases of "extreme urgency". In such cases, the head of the service may, with the approval of the Administrative Commission's president, authorise exceptional surveillance measures for up to 48 hours. The authorisation has to justify the use of the urgent procedure and has to be communicated to the members of the commission immediately.[393]

Examples of ex post approval can be found in France and the United Kingdom. In France, in case of "absolute emergency", the prime minister may authorise surveillance measures without the CNCTR's opinion. The prime minister is required to inform the CNCTR within 24 hours of giving the authorisation and justify the use of the urgent procedure.[394] Recourse to the urgent procedure was made only once between October 2015 and October 2016.[395] In the United Kingdom, in urgent cases, the Investigatory Powers Act foresees that a warrant can be issued for targeted interception and equipment interference as well as for bulk equipment interference and specific bulk personal datasets without the Judicial Commissioner's prior approval.[396] The Judicial Commissioner has to be notified and has three working days after the day the warrant was issued to decide whether or not they approve the warrant, and notify the authorising person. If the Judicial Commissioner refuses to approve then warrant, the implementing authority must, "so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible".[397] In addition, the Judicial Commissioner may decide to request the destruction of any material collected or impose conditions on its use or retention.[398]

Similarly, in Germany, a reform of the G 10 Law aligned the approval procedures in cases of emergency. While the competent federal ministry can provisionally approve

393 Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 18 (10)(4).

394 France, Interior Security Code, Art. L. 821-5. The urgent procedure cannot be used when the services wish to use the so-called algorithm: France, Interior Security Code, Art. L. 851-3 V.

395 France, CNCTR (2016), p. 56.

396 United Kingdom, Investigatory Powers Act 2016, ss. 24 and 109 for targeted interception and examination, and equipment interference warrants respectively. S. 180 for bulk equipment interference, s. 209 for bulk personal datasets. Ss. 24, 109, 180, and 209 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

397 *Ibid.* ss. 25 (2); 110 (2); 181 (2); 210 (2) respectively. Ss. 25, 110, 181 and 210 were not into force at the time of writing and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

398 *Ibid.* s. 25 (3). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

strategic surveillance, the chair of the Parliamentary Control Panel or the chair's proxy needs to give their provisional approval within three days, and full approval by the control panel has to be obtained within two weeks.[399] The surveillance measure can start before the G 10 Commission's approval but the data cannot be used. The approval request needs to take place with 24 hours.[400] In the context of foreign to foreign surveillance, the 2016 reform lists situations which qualify as emergency. The approval of the Independent Committee needs to be sought without delay. When a request is rejected, the data must be destroyed.[401]

Protected professions and privileged information

ECtHR case law: surveillance measures concerning media

"In the instant case, [...] the use of special powers would appear to have been authorised by the Minister of the Interior and Kingdom Relations, if not by the head of the AIVD or even a subordinate AIVD official, but in any case without prior review by an independent body with the power to prevent or terminate it [...]. Moreover, review post factum, cannot restore the confidentiality of journalistic sources once it is destroyed."

ECtHR, Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, No. 39315/06, 22 November 2012, paras. 100-101*

Special authorisation and approval procedures may also apply when the scope of the surveillance includes information protected by professional privilege. Member State laws often provide enhanced protection to certain professionals (e.g. media professionals, lawyers, judges). The Council of Bars and Law Societies of Europe (CCBE), for example, has adopted specific recommendations in this area.[402] In the Netherlands, several lawyers in 2015 filed a complaint in court, alleging that they had been under surveillance. The court decided that the procedure in place at the time for obtaining authorisation to intercept lawyers' communications was unlawful and violated the right to private life, in the absence of prior approval by an independent body.[403] At the end of 2015, this judgment as well as the ECtHR's decision in *Telegraaf Media Nederland Landelijke Media B.V. and Others* triggered a legislative amendment aiming to better protect journalists' sources. The Minister of the Interior and the Minister of Defence established an independent temporary commission to provide for the ex-ante oversight of surveillance operations in connection to the special powers included in the Intelligence and Security Services Act 2002, allowing for the tapping of lawyers and journalists. Since 1 January 2016, this commission, chaired by the chair of the CTIVD, gives binding advice to the ministers on the authorisation of measures that 1) may affect privileged lawyer-client communication or 2) are aimed at identifying journalists' sources.[404] The 2017 reform of the Dutch legislation transferred this authority to the Court of The Hague.[405]

In France, the law protects parliamentarians, lawyers, judges and journalists. Requests for surveillance measures in respect to these professionals must be considered by the CNCTR in a plenary session. The urgent procedure cannot be applied. Moreover, transcripts of the collected intelligence data must be transmitted to the CNCTR for a specific control of the necessity and proportionality of the risks entailed by targeting potentially privileged communication, assessed in terms of the need for enhanced safeguards.[406] The CNCTR outlined the scope of such enhanced protection, and provided definitions of the covered professional categories, in an opinion adopted in October 2015.[407]

CNCTR on enhanced protection for certain professions

"Any person, irrespective of nationality who, in France, his country of origin or internationally, exercises one of the professions cited in the law or holds a mandate of similar nature to that of French parliamentarians, shall enjoy the protection of the law."

France, CNCTR (2016), p. 102 [FRA translation]

Similarly, the United Kingdom provides for enhanced safeguards when interception or equipment interference would target parliamentarians or communications protected by legal privilege, would include confidential journalistic material, or where its purpose is to identify or confirm a source of journalistic information.[408]

399 Germany, G 10 Act, S. 14 (2).
400 *Ibid.* ss. 10 and 15 (6).
401 Germany, BNDG, S. 9 (4).
402 See CCBE (2016).
403 The Netherlands, District Court The Hague (*Rechtbank Den Haag*), Case No. C/09/487229/KG ZA 15-540, 1 July 2015.
404 Netherlands, Minister of the Interior and Kingdom Relations & Minister of Defence *(Minister van Binnenlandse Zaken en Koninkrijksrelaties & Minister van Defensie)* (2015). accessed on 12 February 2016.
405 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*) Arts. 27 and 30.
406 France, Interior Security Code, Art. L. 821-7.
407 France, CNCTR (2016), p. 102 and following. See also the pending case ECtHR, *Association confraternelle de la press judiciaire v. France*, No. 49526/15.
408 United Kingdom, Investigatory Powers Act 2016, for interception: ss. 26-29; for equipment interference: ss. 111-114. Ss. 26-29 and 111-114 are yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note). See also ECtHR, *10 Human Rights Organisations and Others v. the United Kingdom*, No. 24960/15, pending before the ECtHR.

In Sweden, the law specifies that all gathered intelligence concerning communications of persons bound by legislated professional secrecy, suspects or accused and their defence counsel, as well as statements given in confession to a priest must be immediately destroyed.[409]

Interestingly, in Belgium, aside from lawyers and journalists, the law includes doctors among professionals of whom surveillance is in principle prohibited.[410] Exceptionally and when strictly necessary, the law prescribes enhanced safeguards for the authorisation of interceptions of the protected professions' communications. One of the safeguards envisaged is that, depending on the profession, the President of the Order of French and German speaking Bar Associations, the President of the Order of Flemish Bar Associations, the President of the National Council of Doctors or the President of Professional Journalists Association must be notified by the Administrative Commission prior to the implementation of the surveillance measure. The Administrative Commission must provide all necessary information to the presidents of these professional associations.[411]

In Germany, federal law provides enhanced protection to various professionals bound by professional secrecy – such as members of parliament, faith leaders and lawyers – only in case of targeted surveillance.[412] Enhanced protection is not available in case of strategic or foreign-to-foreign surveillance.

409 Sweden, Signals Intelligence Act, Art. 7.
410 Belgium, Organic law on intelligence and security services (*loi organique des services de renseignement et de sécurité*), 30 November 1998, Art. 2 (2), as amended.
411 *Ibid.* Art. 18/2 (3), as amended.
412 Germany, G10 A, S. 3b in conjunction with Code of Criminal Procedure, S. 53. See Löffelmann, M. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1201, p. 1252 and following and p. 1268.

11

Oversight of international intelligence cooperation

The internationalisation of threats led to an increased need for joint operations and the intensification of international communication and data exchanges between intelligence services. This in turn means that intelligence activities have become more diverse and include a growing cross-border element.

11.1. Specific safeguards

UN good practice on authorisation process

Practice 32. National law outlines the process for authorizing both the agreements upon which intelligence-sharing is based and the ad hoc sharing of intelligence. Executive approval is needed for any intelligence-sharing agreements with foreign entities, as well as for the sharing of intelligence that may have significant implications for human rights.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

UN good practice on circumvention of national obligations through intelligence-sharing

Practice 35. Intelligence services are explicitly prohibited from employing the assistance of foreign intelligence services in any way that results in the circumvention of national legal standards and institutional controls on their own activities. If States request foreign intelligence services to undertake activities on their behalf, they require these services to comply with the same legal standards that would apply if the activities were undertaken by their own intelligence services.

UN, Human Rights Council (2010), Report of the Special Rapporteur Martin Scheinin

The specificities of international intelligence sharing require Member States to establish safeguards that are tailored to these processes. These include – but are not limited to – prior approval of any agreement or pattern of cooperation by the executive, the implementation of fundamental rights risk assessments, strong guarantees for protection of sources and personal information, data reliability assessments and the obligation to keep records.

As identified by Born, Leigh and Wills, "requirements of this kind have a number of benefits. They establish a clear framework for approval of cooperation activities. They can help to ensure that cooperation is aligned with the government's foreign policy, defence, security, and diplomatic objectives and does not unwittingly undermine or contradict these. They ensure that political overseers have an understanding of the arrangements that the state's services have with partners. They allow for scrutiny to take place of any risks of particular partnerships at an appropriate political and managerial level."[413] Prior approval may be required before the establishment of the agreement and/or before the exchange of data.

In almost all Member States, intelligence services must obtain the approval of the executive before concluding an international agreement. Only in Slovenia is international intelligence cooperation at the discretion of the head of the service.[414]

In the Netherlands, under normal circumstances, decisions to cooperate with foreign services lie with the head of the service. However, authorisation by the

413 Born, H., Leigh, I. and Wills, A. (2015), p. 93.
414 Slovenia, Slovene Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji, ZSOVA*), 7 April 1999, Art. 7.

relevant ministers is mandatory before collaborating with 'high-risk services'.[415] Cooperation criteria are not spelled out in the 2002 Act. Over the years, the Dutch oversight body carried out several investigations into this matter and issued recommendations to the relevant minister. These were partially incorporated into Articles 88 to 90 of the 2017 Law replacing the 2002 Act.[416] The law provides for a compulsory risk assessment before entering into a cooperation agreement. The assessment will serve not only to identify potential risks inherent in the cooperation, but also what type(s) of cooperation may be established by the intelligence services. Furthermore, the law requires ministerial approval, which can be delegated to the head of the service.[417] The CTIVD expressed some criticisms when the law was being debated in parliament and maintained that additional privacy- and data protection-related safeguards should be included.

In Sweden, the Ministry of Justice must only be briefed before the cooperation takes place.[418] Four Member States – Denmark, Germany, Hungary and Lithuania – require an additional form of approval before the actual exchange of data may take place. Such approval can be given either by the executive, the judiciary or by the head of the services. In Germany, strategic surveillance data exchange requires the agreement of the Federal Chancellery.[419] Foreign-foreign surveillance data can only be transferred to foreign intelligence services of EU, European Economic Area (EEA) and NATO Member States if such a transfer was approved by the Federal Chancellery. For any other country, additional approval by the Head of the Chancellery is needed.[420]

UN good practice on intelligence sharing

Practice 33: Before entering into an intelligence-sharing agreement or sharing intelligence on an ad hoc basis, intelligence services undertake an assessment of the counterpart's record on human rights and data protection, as well as the legal safeguards and institutional controls that govern the counterpart. Before handing over information, intelligence services make sure that any shared intelligence is relevant to the recipient's mandate, will be used in accordance with the conditions attached and will not be used for purposes that violate human rights.

UN, Human Rights Council, Report of the Special Rapporteur Martin Scheinin

Fundamental rights risk assessments in international cooperation

"Intelligence service managers should put in place risk assessment processes for international intelligence co-operation that set out the factors which must be considered before undertaking particular types of cooperation. [...] The executive should ensure that there is cross-government sharing of appropriate information on countries' human rights records as this assists services in undertaking risk assessments."

Born, H., Leigh, I. and Wills, A. (2015), pp. 109 and 112

In 2016, while encouraging nations to establish intelligence-sharing platforms to better combat terrorism, the UN General Assembly stressed that any counter-terrorism effort should not neglect the rule of law, human rights and fundamental freedoms.[421] As a general rule, democratic states are keen to share information with partner states where similar democratic structures are guaranteed. To ensure this, some Member States – such as Croatia, Germany and the Netherlands – conduct risk assessments, i.e., a global evaluation of several factors, such as the legal principles regulating the potential partners' activities, the international political context in which foreign states operate, existing bilateral or international agreements, and/or an assessment of respect for fundamental rights.[422]

Risk assessments are conducted based on guidelines that are not accessible to the public. However, the 2016 CTIVD review report on the implementation of cooperation criteria spells out the various cooperation criteria taken into account before entering into a cooperation agreement:

- respect for human rights and democratic anchorage,
- professionalism and reliability of the foreign intelligence service,
- advisability in the context of international commitments,
- whether cooperation would enhance the performance of tasks and
- reciprocity rule.[423]

The assessment of potential partners' 'human rights footprint' is crucial. Indeed, as highlighted by Born, Leigh and Wills, "concerns about the human rights "foot print" of incoming information go beyond the implications for reliability; they also include possible legal implications of using such information".[424]

415 The Netherlands, CTIVD (2016b), p. 5.
416 The Netherlands, Intelligence and Security Services Act 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*), Arts. 88-90.
417 The Netherlands, CTIVD (2016b), p. 8 and following.
418 Sweden, Regulation on Defence intelligence service *(Förordning [2000:131] om försvarsunderrättelseverksamhet),* 30 March 2000, pp. 3 and 4.
419 Germany, G10 Act, S. 7a.
420 Germany, BNDG, S. 13 (5).
421 UN, GA (2016b), pp. 6 and 8.
422 Born, H., Leigh, I. and Wills, A. (2015), pp. 108-110.
423 The Netherlands, CTIVD (2016b), p. 5 and following.
424 Born, H., Leigh, I. and Wills, A. (2015), pp. 112-113.

When assessing the general level of human rights compliance, some Member States focus their analysis on specific rights, such as data protection and the protection of sources. This is the case, for instance, in Denmark,[425] Germany[426] and Slovenia,[427] where ensuring that a data protection framework exists in the recipient state is a pre-condition for any information sharing and disclosure of personal data. In addition, some Member States, such as Luxembourg,[428] require specific protection of sources of information.

Reliability of data: caveats and reliability assessments

"Intelligence services should ensure that caveats are attached to information shared with foreign partners."

"Caveats should set out in unambiguous terms the use to which that information may be put and with whom it may be shared."

"Reliability assessments should be attached to intelligence shared with foreign partners, particularly where it relates to identifiable individuals."

Born, H., Leigh, I. and Wills, A. (2015), pp. 114 and 115

Reliability of the received data is, indeed, crucial – not only to ensure a correct implementation of intelligence strategies, but also for the protection of fundamental rights. To secure reliability of the data, Member States may attach a specific caveat[429] to the transfer of data and/or conduct data reliability assessments. Germany, for instance, includes "appropriations clauses" that specify that the data cannot be used for a different purpose than the one for which they were originally collected, and that the use must respect democratic principles.[430]

It is difficult for intelligence officers to know the source of the data collected by foreign organisations or the conditions under which they were collected. There is therefore a potential for misguided decisions, affecting the implementation of intelligence strategies and the protection of fundamental rights.

A well-known example of the reliability question crystallised around the source of information that led the US into the 2003 Iraq invasion. Crucial data collected by the German intelligence service (BND) through an Iraqi source known as the "Curveball" was handed over to the CIA, but the reliability of the source, and consequently of the data transmitted, was later questioned.[431] The BND highlighted that doubts about the reliability of such information were earlier communicated to their American partners through caveats. This example illustrates the difficulties faced by agents in assessing the data they receive, and the vital importance for all intelligence services, senders and receivers, to attach data reliability assessments and caveats to the data transferred.

Caveats may also ensure greater transparency on the use of the data received, and therefore, more accountability on the lawful purpose for exchanging data. As emphasised by experts,[432] one of the risks inherent in international sharing of data is the possibility for intelligence services to circumvent domestic obligations by getting partners to collect or process data in ways that would have been deemed unlawful under national law. Such a practice is explicitly prohibited in the United Kingdom.[433] In Germany, both the BNDG and the G10 Act provide that intelligence services must seek written agreements from their foreign counterparts that guarantee that the information received was not collected or processed through activities contrary to rule of law principles.[434]

This is important to ensure compliance of intelligence measures with fundamental rights. As pointed out by several civil society organisations, the increasing practice of intelligence-sharing has reinforced the risk of such arrangements being used to infringe fundamental rights principles. Several civil society organisations around the globe – including three from EU Member States, specifically Hungary, Ireland and the United Kingdom – have decided to challenge the secrecy governing international intelligence cooperation by requesting access to the agreements under freedom of information rules.[435]

425 Denmark, Act on the Danish Security and Intelligence Service, section 10(2) and (4), cf. section 7.
426 Germany, G10 Act, S. 7a (1).
427 Slovenia, Slovene Intelligence and Security Agency Act, Art. 12 (11).
428 Luxembourg, Act of 5 July 2016 on the reorganisation of the State Intelligence Service, Art. 11 (4).
429 Born, H., Leigh, I. and Wills, A. define 'caveat' as "conditions restricting the use of information shared with a partner intelligence service", Born, H., Leigh, I. and Wills, A. (2015), p. 97.
430 Germany, BNDG, S. 13 (3).
431 See Born, H., Leigh, I. and Wills, A. (2015), p. 39; see also Lefebvre N. (2015), p. 29.
432 See Born, H., Leigh, I. and Wills, A. (2015), pp. 48-50, and UN, Human Rights Council, Scheinin, M. (2010), p. 29.
433 United Kingdom, Investigatory Powers Act, s. 9 and s. 10.
434 Germany, BNDG, S. 13 (3) and Germany, G10 Act, S. 7a
435 See International Network of Civil Liberties Organisations (INCLO) (2017), *International Intelligence-Sharing Project,* and Privacy International v. National Security Agency, Office of the Director of National intelligence, Department of State, and National Archives and Records Administration (Five Eyes FOIA), 5 July 2017.

Recording and tracking obligation

"Legislation should include provisions on the duty of record keeping for international intelligence cooperation, in particular, concerning the exchange of information with foreign partners."

Born, H., Leigh, I. and Wills, A. (2015), p. 94

To ensure adequate accountability, it is essential that intelligence services track and keep records of all transactions with foreign partners. Some EU Member States – including Croatia, Estonia, Germany and Hungary – have included such obligations in their laws governing the functioning of such services.[436] Recording obligations may be hampered, though, by the so-called 'third party rule' – further discussed in Section 11.3. Indeed, some partner and allied services only provide intelligence on the understanding that the receiving service will seek permission before disclosing it outside the intelligence community, and that such permission may be denied. Such a rule, referred to as the 'control principle', is widely adhered to within intelligence communities to ensure trust among partners.

In Germany, transfers have to be documented. The exchange agreement must state that the data may only be used for the same purpose for which they were transferred, and that the German intelligence service from which the data originate reserves the right to ask how data are used.[437] Receiving parties have to sign up to purpose limitation, to keep tag on the data that indicates their origin from telecommunication surveillance, and to provide information about further use on request of the BND. Similarly, in Croatia, the submitted data must be documented, including a written disclaimer that the information provided can only be used for the purposes for which they were provided.[438] In both Germany and Croatia, intelligence services include in these caveats the right to seek feedback on how the submitted data are used. In Germany, such caveats must be clearly indicated before the cooperation starts: the intelligence services must include, in the intent of cooperation that is transmitted to the Federal Chancellery for approval, these two agreements with the foreign partner, on purpose limitation and *a posteriori* information of the use made of the data.[439]

436 Croatia, Act on the Security Intelligence System of the Republic of Croatia, Art. 60 (3), Estonia, Security Authorities Act, s. 34; Germany, BNDG, S. 15 (2) and Germany, G10 Act, S. 7a (3); Hungary, Act CXXV of 1995 on the National Security Services, s. 46.
437 Germany, BNDG, S. 13 (3) and Germany, G10 Act, S 7a (4).
438 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. 60.
439 Germany, BNDG, S. 13 (3) and Germany, G10 Act 7a (4).

Prior controls and authorisations must be complemented by ex post controls, which can be performed internally or externally. However, oversight of international arrangements requires access to information relating to activities and data transfers conducted under international cooperation. In 2016, the CTIVD expressed regret that the draft intelligence bill did not include a recording requirement. According to the Dutch Review Committee, to enable internal and external control, "personal data should be provided exclusively in writing".[440] This is the case, in particular, for exchange of large volume of data that did not go through any evaluation from the services before being exchanged.[441]

11.2. Limited but existing oversight

UN good practices on oversight of international cooperation

Practice 34. Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities.

UN, Human Rights Council, Report of the Special Rapporteur Martin Scheinin

ECtHR case law: external supervision of international cooperation

"The governments' more and more widespread practice of transferring and sharing among themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 78

Although essential for ensuring fundamental rights compliance and boosting trust among intelligence service partners, the laws of a majority of Member states – 17 out of 28 – do not enshrine a clear provision stating whether, and to which extent, oversight bodies have competence over international cooperation. The absence of such a legal basis obliges both intelligence services and oversight bodies to interpret the legal framework to define whether, and to what extent, oversight bodies may assess international exchanges of data. To be lawful, any measure that interferes with privacy must first and foremost be prescribed by law. In the United Kingdom, for example, the Interception of

440 Netherlands, CTIVD (2016a), p. 10.
441 The Netherlands, CTIVD (2016d), p. 27.

Communications Commissioner questioned the extent and exact scope of his remit in this area in his 2013 annual report.[442] Similarly, in Germany, a member of the G 10 Commission wondered to what extent the third party rule limits the commission's oversight over data transfers, when the G 10 Act does not refer to any limitation.[443] In some Member States, the absence of specific reference may be understood as a *de facto* application of the domestic oversight system to international cooperation.

> *"Legislation should include provisions that oblige the service and/or executive to inform the intelligence oversight body about international intelligence cooperation agreements."*
>
> *Born, H., Leigh, I. and Wills, A. (2015), p. 94*

> *"The legislative mandates of bodies that oversee the intelligence services [...] should make clear that their role and powers extend to relevant intelligence cooperation and activities of the services they oversee."*
>
> *Born, H., Leigh, I. and Wills, A., (2015), p. 190*

Eleven EU Members States have laws that specify the legal basis for oversight bodies to oversee international cooperation. Of these, three – France, Ireland and Spain – have excluded information originating from foreign services from the scope of oversight. Four – Denmark, Finland, the Netherlands and Romania – do not differentiate between the oversight regime for international sharing of data. Three – Luxembourg, Portugal and Sweden – have limited the scope of the control over such information. In Germany, the scope of competences of the oversight bodies depends on the type of surveillance conducted: it is limited for strategic surveillance, and similar to domestic oversight for foreign-to-foreign data transfers. The following paragraphs introduce some of the specificities of the legal frameworks prohibiting, allowing or limiting national oversight over international intelligence cooperation.

In the Netherlands, the CTIVD conducted several investigations into the legality of international cooperation.[444] In 2015, it conducted two investigations following requests from the House of Representatives, on the criteria for establishing cooperation and on the prior ministerial approval required before any exchange of data. 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.[445] The CTIVD added that "the potential of the General Intelligence and Security Service of the Netherlands (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.[446] Based on past review reports, the CTIVD also emphasised 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)."[447]

In Belgium, the Standing Committee I in 2013 launched an investigation regarding one of the missions of the Coordinating Unit for Threat Analysis (OCAM), which establishes and maintains contacts with foreign partners. This investigation, jointly conducted with the Standing Committee P, followed previous similar investigations in 2009 and 2011 on OCAM's international activities. Concluded in 2015, the investigation recalled that OCAM is not an intelligence service as such, and therefore the foreign counterparts with whom it may establish cooperation should be better defined.[448] The oversight body clarified, though, that a directive regulating OCAM's international cooperation was adopted by the national security council after the investigation concluded.[449]

In France, Spain and the United Kingdom, similar wording included in the respective acts regulating intelligence services exempt "information communicated by foreign services or international organisations" from the remit of parliamentary oversight commissions,[450] as well as, in the case of France, the independent expert oversight body (CNCTR).[451]

In Luxembourg, Portugal and Sweden, the oversight bodies are not expressly tasked with overseeing international data transfers and they generally cannot exercise their full competences over international intelligence cooperation. However, in these four Member States, the body charged with ensuring the control of domestic intelligence activities must be informed of data transfers. In Sweden, for instance, the intelligence services must inform the Swedish

442 United Kingdom, IOCCO (2013), p. 62.
443 Huber, B., *in*: Schenke, W. et al. (eds.) (2014), p. 1451 and following.
444 See The Netherlands, CTIVD (2009), (2016), (2016a), (2016b) and (2016c).
445 The Netherlands, CTIVD (2014), p. 37 and following. See also The Netherlands, CTIVD (2015), p. 28.
446 The Netherlands, CTIVD (2014), p. 5.
447 *Ibid.* p. 28.
448 Belgium, Standing Committee I (2016), p. 33-37.
449 *Ibid.* p. 34.
450 France, Ordinance no. 58-110 of 17 November 1958 related to the functioning of parliamentary assemblies (*Ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires*), Art. 6 nonnies; Spain, Law 11/2002 of 6 May, regulation of National Intelligence Centre (*Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia*), Art. 11 and the United Kingdom, Justice and Security Act 2013, schedule 1, para. 5 (c).
451 France, Interior Security Code (*Code de la sécurité intérieure*), Art. L. 833-2. - IV.

Foreign Intelligence Inspectorate (*Statens inspektion för försvarsunderrättelseverksamheten*) of the principles applied in their international cooperation and the countries and/or organisations they cooperate with.[452]

In Germany, the scope of oversight bodies' competences over international cooperation differs depending on the type of surveillance conducted. The Independent Committee may conduct controls at all time over foreign to foreign data transfers.[453] However, in cases of strategic surveillance, the oversight is limited, as data transfers only need to be reported to the G 10 Commission on a monthly basis and to the PKGr every six months.[454] The German government informs the PKGr about the international data exchanges.[455] In 2015, the German intelligence service (BND) transferred data to two foreign services.[456]

The effectiveness of oversight exercised by national bodies over international intelligence cooperation was questioned by several institutions, both at national and international level. In Poland, where no limitations are expressly mentioned by law, a judgment of the ECtHR highlighted the absence of effective oversight over activities conducted under international cooperation, and in particular, of the effectiveness of the investigation powers of the parliamentary commission in this field. In *Al Nashiri v. Poland*, the court noted that the "instant case (...) also points out in this context to a more general problem of democratic oversight of intelligence services. The protection of human rights guaranteed by the Convention, especially in Articles 2 and 3, requires not only an effective investigation of alleged human rights abuses but also appropriate safeguards – both in law and in practice – against intelligence services violating Convention rights, notably in the pursuit of their covert operations. The circumstances of the instant case may raise concerns as to whether the Polish legal order fulfils this requirement."[457]

The absence of any specific mention of oversight over international cooperation in a law may be differently interpreted from one Member State to another. In some, this absence might be understood as implicit permission for oversight bodies to conduct similar control regarding international cooperation as over domestic intelligence efforts. Others may couple this absence with the third party rule (see Section 11.3), and interpret it as a tacit prohibition on controlling international intelligence-sharing.

452 Sweden, Regulation on Defence Intelligence Service, Art. 6.
453 Germany, BNDG, S. 15 (3).
454 Germany, G10 Act, S. 7a.
455 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), pp. 10-11.
456 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 9.
457 ECtHR, *Al Nashiri v. Poland,* No. 28761/11, 16 February 2015, para. 498.

11.3. Limits to oversight: the third party rule

> *"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."* European Parliament, Committee on Civil Liberties, Justice and Home Affairs (2013b)

The dominant principle of international cooperation is the 'third party rule', also known as the 'originator control principle'. This rule specifies that a foreign agency to which intelligence has been transmitted can neither share this information with a third party, nor use the data for an objective different from the one for which the exchange was established in the first place. While the rule is a core element of trust in which the global intelligence cooperation is rooted, it is also used by intelligence services to prevent oversight bodies from accessing any information related to international cooperation.

Third party rule should not act as a foreign veto

"[Member States should] [e]nsure 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, Democratic and effective oversight of national security services, *2015, Recommendation 16, p. 13*

Some Member States explicitly refer to the third party rule either in their laws or in the bilateral agreements signed with foreign partners.

The majority of parliamentary committees do not have access to classified information received from foreign secret services. This is explicitly stated in the cases of Spain,[458] France[459] and the United Kingdom,[460] among others. In its activity report, the German Parliamentary Control Panel acknowledged this fact and called for

458 Spain, Law 11/2002 of 6 May, National Intelligence Centre Act, Art. 11(2).
459 France, Ordinance No. 58-1100 on the functioning of the parliamentary assemblies, Art. 6.
460 United Kingdom, Justice and Security Act 2013, s. 5(c) of Schedule 1.

amendment of the legislation to enhance parliamentary control of international exchanges between services.[461]

In some Member States, such as Belgium, the Netherlands and Sweden, the oversight body is not seen as a third party. This specific understanding of the nature of oversight bodies results from a parallel mechanism: oversight bodies acknowledge that the current form of the terrorist threat requires intelligence services to regularly exchange information, while overseers are granted full access to all information to effectively perform their tasks. In Belgium, for instance, following a request by the Defence Ministry, the Standing Committee I delivered a positive opinion on the international exchange of information relating to foreign terrorist fighters, but also clarified that the control over multilateral activities remains real.[462]

Promising practice

Enhancing international cooperation among oversight bodies

Equal access to information obtained via international cooperation could allow enhanced international cooperation among oversight bodies. In 2015, oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland launched joint project, whereby each body would conduct national investigation in relation to foreign terrorist fighters. A final report is due in 2017; intermediary assessments show the added-value of such coordinated efforts.

Belgium, Standing Committee I (2016), p. 80 and The Netherlands, CTIVD (2017), p. 33.

The third party rule has functional purposes: it ensures protection of sources, reinforces trust among intelligence partners and prevents intelligence data from being shared multiply, becoming thus their own reliability proof. The question of whether oversight bodies should be considered as third parties under the third party rule has crucial implications. As demonstrated above, oversight bodies play a very important part in achieving effective intelligence. Effective intelligence is, for foreign partners, a guarantee of valuable and trustworthy information and therefore ultimately increases and strengthens international cooperation. In that sense, the trend by some Member States to increasingly stop considering oversight bodies as third parties and grant them full access to information originating from international cooperation will ensure better cooperation among both overseers and intelligence services. A harmonised approach over oversight bodies' statutes in this regard (including parliamentarian committees) would foster exchange of best practices among Member States.

11.4. Powers and competences of oversight bodies over international cooperation

> *"Oversight bodies should receive copies of all such agreements at the time they are entered into or when they are revised. The oversight body should be obliged to review each agreement and, when possible, undertake random audits to measure compliance with the terms of the agreement. Such audits can help determine whether the agreement needs to be revised in light of past practice."*
>
> *Born H. and Leigh I., 2012, p. 144*

Very few Member States' legal frameworks provide for the possibility of an external review, either ex ante or ex post, of international agreements establishing international intelligence cooperation. Those that do include Belgium, Luxembourg and the Netherlands.

In Belgium, Hungary and the Netherlands, oversight bodies have access to internal guidelines governing exchanges of information. In Belgium, the Standing Committee I highlighted some weaknesses in the directives established by the National Security Council. Notably, the committee pointed out the absence of clear criteria clarifying when international cooperation can be established with foreign counterparts, and data transfers are allowed; delimiting the uses foreign counterparts may make of the data they receive; and reinforcing data protection safeguards when information is transferred to countries that do not offer the same level of data protection.[463] The Standing Committee I reiterated these concerns in its latest report.[464] The National Security Council eventually adopted a directive on this matter in 2016. In the Netherlands, the Dutch oversight body, CTIVD, has published detailed information, including recommendations, on the internal guidelines adopted by the General Intelligence and Security Service[465] and on the cooperation assessments (referred as "weighting notes") intelligence services must conduct before entering into international agreements.[466]

11.5. Bridging the gaps: peer constraints

The two restrictions mentioned above – the absence of a clear legal basis for the oversight of international

461 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), p. 14.
462 Belgium, Standing Committee I (2016), pp. 73-74.
463 Belgium, Standing Committee I (2015), p. 74.
464 Belgium, Standing Committee I (2016), p. 5.
465 The Netherlands, CTIVD (2009), pp. 6-12.
466 The Netherlands, CTIVD (2016c).

intelligence cooperation in some Member States and the limitations introduced in the legal frameworks of others – are not the only aspects hampering such oversight.

Accountability deficit

"Often, it is not possible for an oversight body to ascertain whether the data which the national service receives from abroad was collected lawfully. A national oversight body can only examine whether the national service provided or received information lawfully."

The Netherlands, CTIVD Annual Report 2014-2015, *p. 35*

The deficits described above by the Dutch oversight body prompted reflection on the possibility to create alternative oversight mechanisms that fit the specificities of international cooperation. An innovative way of performing oversight has emerged from these reflections: the "peer constraint" mechanism.

The third party rule restricts the majority of oversight bodies' ability to provide safeguards on the international exchange of data. However, the gaps are sometimes filled by other actors and in different ways, notably through peer-constraint mechanisms.[467] To receive intelligence, an intelligence service must be trustworthy in the eyes of its counterparts. Here, the pressure exercised by an intelligence service on its foreign counterpart replicates, to a certain extent, the constraint exercised by oversight bodies. In addition, the interest of any service in receiving intelligence magnifies this incentive. This is the case in Belgium where, since 2016, the intelligence services have a degree of control on international cooperation.

Of the 17 Member States where oversight of international cooperation is not provided for in law, guidance on the conditions for overseeing international intelligence cooperation might be included in classified internal guidelines drafted by the executive or the head of services. Generally, such guidance invites or imposes on the intelligence services the duty to exercise a priori and/or a posteriori control on data transfers taking place within international cooperation. In Belgium, this process was endorsed in January 2016, when the 1998 law on intelligence services was modified on the recommendation of the Parliament and the Standing Committee I to grant oversight competence to the Belgian intelligence services.[468]

Deeks describes 'peer constraints' as follows: "Through various mechanisms (formal and informal, public and private), one state's intelligence community can affect the way in which another intelligence community conducts [...] surveillance; the amount and type of intelligence the other intelligence community receives; and, less tangibly, how the other intelligence community views its own legal obligations".[469] Such constraint may be formally inserted as a caveat in the international agreement or may result from the tacit observation of one country's legal framework, including the extent of the oversight structure and the complaints and judicial decisions taken against the intelligence community.[470]

In the aftermath of the Snowden disclosures, peer constraints have become increasingly used among partners to ensure that international cooperation follows democratic principles. Approaches taken in to accessing, processing and controlling intelligence data are increasingly monitored by foreign partners to evaluate to which extent exchanged data will be lawfully processed, and to which extent they may access reliable data. Changes in legislation framing the access, use and control of intelligence may prompt either an intensification of or a decline in collaboration from foreign counterparts.

Peer-constraint mechanisms present certain added-value over classical oversight mechanisms. Firstly, they tackle the lack of expertise some overseers may have while assessing surveillance techniques and the implications of specific safeguards regarding the use of the data collected. Secondly, they give intelligence services a real interest in being deemed trustworthy by foreign counterparts. Third, they are completely independent from the executive of their foreign partner. However, peer-constraint mechanisms will only have (a limited) impact if they originate from a state with an effective oversight system.

467 Deeks, A. (2016), pp. 17-29.

468 Belgium, Organic Law concerning the intelligence and security services *(Loi organique des services de renseignement et de sécurité),* 30 November 1998, Art. 7 and 11.

469 Deeks, A., (2016), p. 4.

470 *Ibid.* pp. 17-22.

PART III: REMEDIES

KEY FINDINGS

Remedial avenues

- FRA's research shows that, in the context of surveillance, individuals' right to seek remedy is limited but not absent. A limited number of individuals seek remedies. On average, according to the experts interviewed, 10 to 20 complaints are filed a year.
- Non-judicial remedies are more accessible to individuals than judicial mechanisms. The procedural rules are less strict, and proceedings are faster and cheaper. Three EU Member States do not provide individuals with the possibility to lodge a complaint related to surveillance with non-judicial bodies. In ten of the 25 EU Member States that do provide that possibility, one single non-judicial body is entrusted with remedial powers, and in the remaining 15, individuals may lodge a complaint with two or more bodies with remedial powers.
- In 10 of the 16 Member States that have expert bodies, these bodies have the most powers to offer an effective remedy. They are also independent and enjoy full access to classified information and premises.
- Remedial bodies' effectiveness depends foremost on their binding decision making powers. In 18 Member States, remedial bodies can issue binding decisions. Most of them are expert bodies and data protection authorities.
- The effectiveness of remedies available to individuals has been questioned – predominantly by representatives from civil society organisations, lawyers and academia. Various factors hamper their effectiveness, including low levels of awareness about the existence of remedies and non-implementation of the right to access information and/or the notification obligation.

Limits to effective remedies

- FRA's findings show that EU Member States' laws limit individuals' rights to notification and access to information on various grounds linked to national security. Imposing limitations is in line with relevant ECtHR case law.
- In nine Member States, individuals may exercise the right to access their own data indirectly – through the DPAs who have competences in this area or through expert bodies.
- EU Member States address the judiciary's lack of expertise in secrecy and technical matters relating to intelligence services' work in various ways, including:
  - the development of alternative adversarial procedures to allow for the use of classified information;
  - cooperation mechanisms between remedial expert bodies to tackle the lack of expertise of judicial and non-judicial bodies; and
  - the establishment of quasi-judicial bodies.
- In four Member States, an expert body's decision or preliminary assessment can be appealed before a judge. Arrangements on access to sensitive information are then prescribed by law.

12 The remedial route

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 (2010), Report of the Special Rapporteur Martin Scheinin

The 2015 FRA report recalled that the right to an effective remedy is an essential component of access to justice, and allows individuals to seek redress for violations of their rights. For a remedy to be 'effective' in practice and in law, judicial or non-judicial bodies need to have a number of specific powers (both from institutional and procedural perspectives)[471] offering individuals proper redress. In *Roman Zakharov v. Russia*, the ECtHR outlined the elements of an effective remedy and noted the challenges posed specifically by secret surveillance.

ECtHR case law: effective remedy in cases of surveillance

"Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. 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, judicial control offering the best guarantees of independence, impartiality and a proper procedure [...] As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications. [...] [E]ffectiveness [of remedies] is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. "

ECtHR, Roman Zakharov v. Russia [GC], No. 47143/06, 4 December 2015, paras. 233, 234 and 298

471 Gajdošová, J., in Dietrich/Sule (eds), forthcoming.

The 2015 FRA report highlighted that non-judicial avenues 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. In the 28 EU Member States, non-judicial bodies such as DPAs, expert bodies, executive bodies, parliamentary committees, and ombuds institutions offer remedies.

Twenty-five Member States have empowered at least one of their oversight bodies or their ombuds institution with remedial power. In three Member States – the Czech Republic, Latvia and Poland – no non-judicial body is available, and individuals can lodge a complaint only with a judge. (As further discussed below, the United Kingdom's Investigatory Powers Tribunal is not a non-judicial body, but also does not qualify as an ordinary court.) Table 6 shows the types of non-judicial bodies with remedial powers in the Member States.

Table 6: Non-judicial bodies with remedial powers in the context of surveillance, by EU Member State

	Executive (ministry)	Expert body(ies)	DPA	Parliamentary committee(s)	Ombuds institution
AT		✓	✓		✓
BE		✓	✓		✓
BG			✓	✓	
CY			✓		
CZ					
DE		✓	✓	✓	*(acts as a filter: only reasonable complaints are sent to the PKGr)*
DK		✓			
EE					✓
EL			✓		
ES					✓
FI			✓		✓
FR		✓	✓		✓
HR		✓	✓	✓	✓
HU	✓		✓	✓	✓
IE		✓	✓		
IT			✓		
LT			✓	✓	✓
LU		✓			
LV					
MT		✓	✓		
NL*		✓			
PL					
PT		✓			✓
RO				✓	
SE		✓	✓		
SI			✓	✓	✓
SK				✓	
UK**					

Notes: * *Table reflects the situation under the Intelligence and Security Services Act 2017 and will be applicable when the relevant sections enter into force.*

** *The Investigatory Powers Tribunal, although not an ordinary court, cannot be classified as a non-judicial body.*

Source: *FRA, 2017*

The 2015 FRA report showed that the availability of various remedies does not necessarily help to ensure effectiveness.[472]

"The average citizen does not even know where to address a complaint." (Data protection authority)

The fieldwork interviews[473] addressed the availability of remedies in case of alleged unlawful data processing by intelligence services. Two dominating opinions emerged. Most respondents representing public authorities or institutions (such as expert oversight, executive control and judiciary) tended to list the avenues available and confirm their sufficiency, adequacy and satisfactory availability. Their existence appears to be seen as proof of their efficiency. Very few respondents from public authorities questioned the effectiveness of the remedies offered. These findings were also related to the generally low level of knowledge among the interviewees of practical implementation of the remedies in the Member States, the number of complaints, and little knowledge about their outcomes, unless the institution itself had a remedial function.

"Yes, the avenues available for individuals to complain are enough. Yes, I think the websites of the governments are quite good at this, they always have a page on this, send the letter to this address and online application for filing your complaints." (Expert body)

"[A] signed letter [is] enough to submit a request, with details on what is allegedly affected, such as a mobile number, bank account, or email account." (Expert body)

Representatives from civil society organisations, academia, and practicing lawyers acknowledged that it is positive that complaints against intelligence services do not need to be strongly substantiated for remedial bodies to consider them. However, they tended to be critical about available remedies and questioned their efficiency. Notably, a majority of the interviewed civil society representatives were lawyers who have been involved in lodging both judicial and non-judicial complaints, challenging the lawfulness of intelligence surveillance on behalf of individuals. Most respondents who were critical considered available remedies ineffective for safeguarding the right to privacy. Some respondents did not even consider them as remedies. Respondents indicated that several factors make the remedial process cumbersome or complicated. These include: low awareness among individuals about the possibility to seek remedies; that complaints are based on assumptions or suspicions when the notification requirement is not prescribed by law; and the types of responses given by remedial bodies. Respondents also mentioned poor capacities of remedial bodies in terms of staff and technical expertise. Moreover, they noted that, even though no costs are involved in seeking remedies through non-judicial avenues, the subject matter can be complex and complainants could benefit from legal advice – but legal aid is not available.

"There is already an existing complaints procedure. Even though it is not a formalised one, if you were to complain, these complaints would have to be taken seriously."

(Academia)

"A limited number of remedies is available for persons. For national surveillance measures, the procedure requires the person to file a complaint with the [expert body] before being granted recourse to the [judge], without any information required to be disclosed to the person on the existence of surveillance measures." (Civil society organisation)

"What will be the point of an individual lodging a complaint if he can base his arguments only on rumours? 'The direct and personal interest' of the law is difficult to demonstrate."

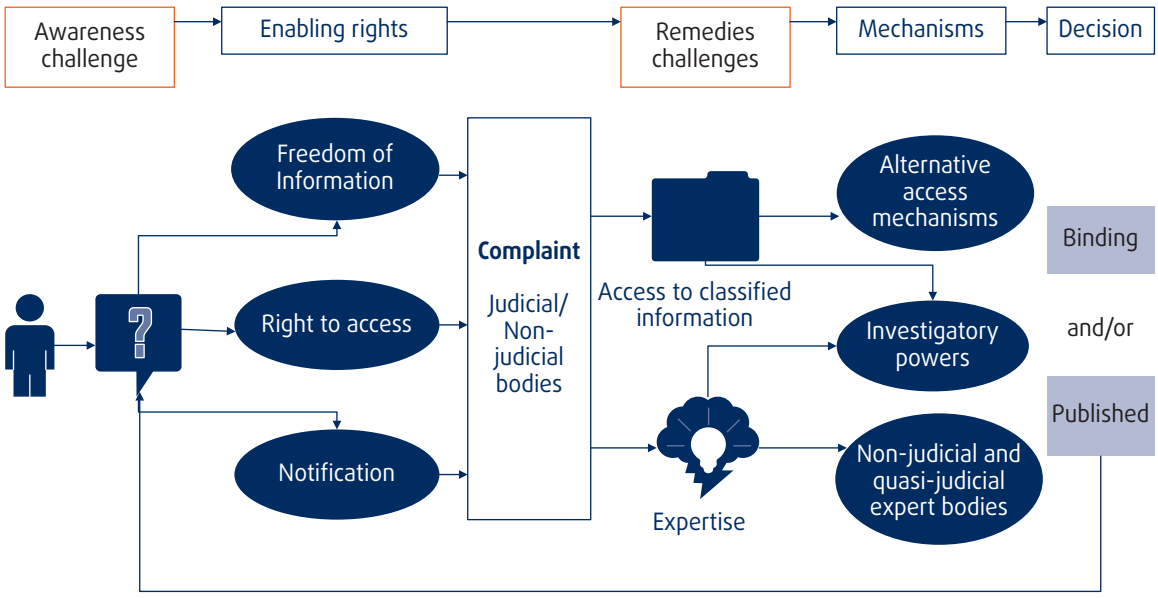
(National human rights institution)

Figure 9 illustrates the different challenges individuals and remedial bodies may confront when seeking, and seeking to provide, effective remedies. For individuals, the first issue is the lack of awareness of surveillance measures. Various tools can help enhance individuals' awareness: notification that they have been under surveillance or right to access to their own data serve as rights' enablers and open the way to a complaint. Remedial bodies are also confronted with several challenges. They can be denied access to classified information or they may lack the necessary expertise. As analysed in the following sections, these hindrances are addressed in various ways at Member State level.

472 FRA, (2015a), p. 59.

473 Annex 1, Section 2, Social fieldwork methodology, presents information about the interviewees, number of interviews during which specific thematic headlines were discussed, quoting conventions, and other related information.

Figure 9: Implementing effective remedies: challenges and solutions



Source: FRA, 2017

12.1. Investigative and decisional powers

Non-judicial avenues generally offer greater expertise than judicial mechanisms. However, non-judicial and quasi-judicial bodies lack effectiveness if they do not have full investigative and decisional powers. These include, but are not limited to, the competence to issue binding decisions, to access all relevant data (including through hearings or visits to intelligence services' premises), to inform complainants about decisions and for individuals to appeal the final decision. Table 7 shows the powers attributed to non-judicial bodies in EU Member States.

Expert bodies have the widest powers. In 22 Member States, at least one non-judicial body has full access to the data collected. In 11 Member States, non-judicial bodies inform complainants that a control was performed – without specifying the outcome. Such competence is mainly granted to expert bodies including DPAs. Across the EU, only in a few cases can decisions of non-judicial bodies be reviewed by a judge (for instance, following an oversight body decision in Austria and France).

Effectiveness depends on capacity to issue binding decisions

"Equipping complaint-handling bodies with mere powers of recommendation is insufficient and does not constitute an 'effective remedy'. Instead, these bodies should be given quasi-judicial remedy powers, such as the power to award financial compensation."

Born, H. and Wills, A. (2012), p. 195

The authority to issue binding decisions is a key element of an effective remedy. Binding decisions should include, at minimum, the ability to order (1) the termination of the surveillance, (2) the destruction of the data collected, and (3) the payment of appropriate compensation.[474] In 18 Member States, remedial bodies – mainly expert bodies and DPAs – may issue binding decisions on complaints relating to surveillance. In Belgium, for instance, the Standing Committee I may order intelligence services to terminate surveillance and destroy the data. In the Netherlands, the complaints sub-committee of the CTIVD may decide that an investigation by the services has to stop; that the exercise of a power by the intelligence services has to stop;

474 Born, H., and Leigh, I. (2005), p. 120.

Table 7: Non-judicial bodies' remedial powers in case of surveillance, by EU Member State

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
AT	Legal Protection Commissioner				
	Austrian Ombudsman Board				
	Austrian Data Protection Authority				
BE	Standing Committee I				
	The federal Ombudsman				
	Privacy Commission				
BG	Commission for Personal Data Protection				
	Committee for Oversight of the Security Services				
CY	Commissioner for Personal Data Protection				
DE	G10 Commission				
	Federal Data Protection Commissioner				
	Parliamentary Control Panel				
DK	Danish Intelligence Oversight Board				
EE	Chancellor of Justice				
EL	Hellenic Data Protection Authority				
ES	Spanish Ombudsman				
FR	National Commission for Control of Intelligence Techniques				
	Defender of Rights				
	National Commission on Informatics and Liberty				
FI	Parliamentary Ombudsman				
	Office of the Data Protection Ombudsman				
HR	Council for Civic Oversight of Security and Intelligence Agencies				
	Ombudsman of the Republic of Croatia				
	Personal Data Protection Agency				
	Committee for Internal Affairs and National Security				
HU	Commissioner for Fundamental Rights				
	Data Protection Commissioner				
	Parliamentary Committee for National Security				
	Relevant ministries				
IE	Complaints Referee				
	Data Protection Commissioner				
IT	Garante per la protezione dei dati personali				
LU	Control Authority «Article 17»				
	National Commission for Data Protection				
LT	Ombudsperson				
	State Data Protection				
	Parliamentary Committee on National Security and Defence				

Table 7: (continued)

	Bodies with remedial competence	Decisions are binding	May fully access collected data	Control is communicated to complainant	Decision may be reviewed
MT	Commissioner of the Security Service				
NL	Review Committee for the Intelligence and Security Services				
PT	Council for the Oversight of the Intelligence				
	Portugese Ombudsman				
RO	Parliamentary Committees				
SE	Swedish Foreign Intelligence Inspectorate (SIUN)				
	Commission on Security and Integrity Protection (SIN)				
	Swedish Data Protection Authority (Datainspektionen)				
SI	Human Rights Ombudsman				
	Information Commissioner				
	Parlm. Supervision of the Intelligence and Security Services Act				
SK	Commission to Supervise the Use of IT Tools				

Note:

= Expert body
= Ombuds institution
= Data protection authority
= Parliamentary Committee
= Executive

Source: FRA, 2017

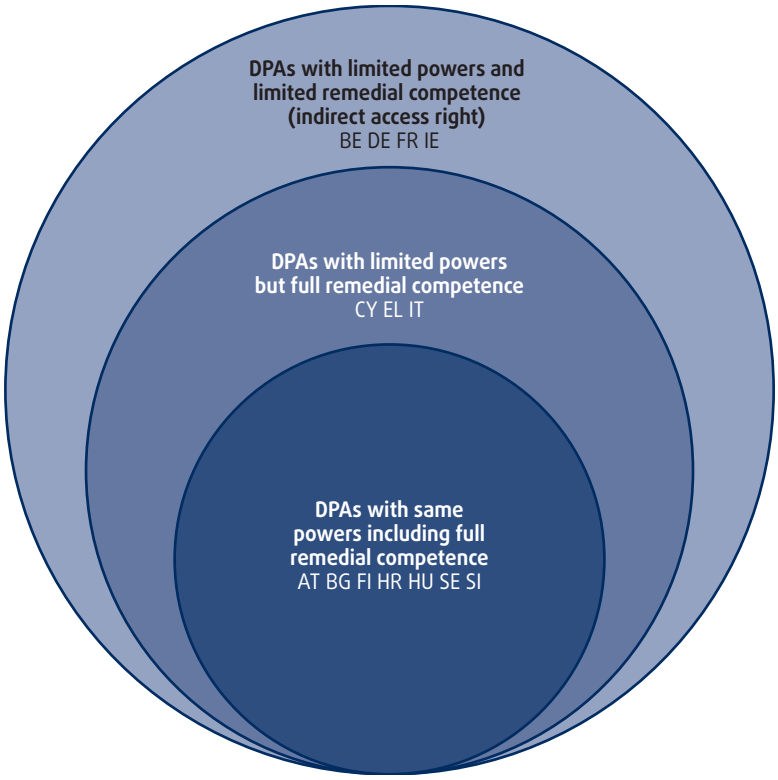
and/or the removal and destruction of data processed by the services.[475] Austria is the only country where both the expert body and the DPA have binding decision powers. Two Member States, Finland and Romania, have empowered another non-judicial body with such power: the ombuds institution and the parliamentary committees, respectively. Nonetheless, the examples introduced throughout this third part show that the power to issue binding decisions, although essential, may be greatly limited if the body's mandate does not include other crucial features, such as independence and full access to classified information and premises.

Of the 16 Member States that have established expert bodies, 12 entrust them with specific remedial powers, but only seven may issue binding decisions (in Belgium, Denmark, Ireland, Luxembourg, the Netherlands, Sweden and the United Kingdom).

DPAs in 14 EU Member States can examine individual complaints. Of these, ten may issue binding decisions; these are the seven Member States where DPAs enjoy the same powers over intelligence services as the expert oversight bodies, and Cyprus, Greece and Italy. In four other Member States (Belgium, France, Germany and Ireland), DPAs may process individual complaints or enable an individual's indirect right to access, but are not entitled to issue binding decisions. In four Member States (Cyprus, Germany, Greece and France), access is accompanied by enhanced requirements, e.g. the presence of the DPA head (Cyprus, Greece); a staff 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). FRA's fieldwork findings show that in France, Germany and Italy, such requirement proved, in practice, to be helpful for DPAs conducting on-site inspections. Figure 10 illustrates the diversity of DPAs' remedial competences over intelligence services across the EU.

475 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Art. 124.

Figure 10: DPAs' remedial competences over intelligence services



Source: *FRA, 2017*

In Belgium, France and Italy, individuals can request the DPA to check whether their data are processed by intelligence services. The DPA proceeds with the necessary check, informs the individual that the control took place but not whether and which data were processed, if such information would affect national security. Should any irregularities be noted, the DPA can request the intelligence service to redress the situation.[476]

Finally, in eight Member States – Bulgaria, Croatia, Germany, Hungary, Lithuania, Romania, Slovakia and Slovenia – parliamentary committees function as complaints-handling bodies in cases of surveillance. Only in Romania can the parliamentary committee resolve complaints through binding decisions. In Germany, the complaint forms part of a petition to parliament.[477] Over a two-year reporting period, the PKGr received 65 petitions, 40 of which dealt with alleged surveillance measures.[478] The more serious ones were forwarded to the G 10 Commission. These complaints, in fact, serve to inform the PKGr.[479]

The extent to which parliamentary committees can provide an effective remedy depends on a number of factors. These include whether members of these special parliamentary committees are properly independent, have experience in the field of intelligence, as well as whether qualified supporting staff is available.[480] In *Bucur and Toma v. Romania*,[481] the ECtHR highlighted that a lack of independence can preclude the effectiveness of remedies. According to the Committee of Ministers of the Council of Europe, the situation in Romania has

476 See for example Italy, Data Protection Code, Art. 160(2).
477 Huber, B., *in*: Schenke, W. et al. (eds.) (2014), p. 1485 and Singer, J. (2016), p. 145.
478 Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), p. 13.
479 Bartodziej, P., *in:* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1561.
480 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, 23 June 1993, Art. 5 (b) and (c), and Romania, *Decision no. 44/1998 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 External Intelligence Service*, 28 October 1998, Art. 6 (e) and (f).
481 ECtHR, *Bucur and Toma v. Romania*, No. 40238/02, 8 January 2013, para. 98.

not evolved since 2013, when the case was decided.[482] In Bulgaria and Romania, the parliamentary committee can investigate complaints; both must forward their positions, either to the relevant ministry (in Romania) or the public prosecutor (in Bulgaria).[483]

Individuals may lodge complaints relating to surveillance with their national ombuds institutions in 11 Member States; however, their mandate may explicitly exclude the issue of national security or the work of intelligence services. Only the Finnish Data Protection Ombuds institution is entitled to issue binding decisions, and only one Member State – Estonia – provides the ombuds institution with remedial powers via the relevant intelligence law.[484] Most ombuds institutions are denied access to classified information and often lack expertise in this field.[485] Consequently, in some Member States – such as Belgium – the ombuds institution will forward the question to the expert body. In Germany, the ombuds institution works in cooperation with the parliamentary oversight committee: its role is to assess the validity of the complaints before transmitting them to the parliamentary committee. Thus, the ombuds institutions' powers can be limited in this area. Complaints are typically concluded with non-binding recommendations that aim to put matters right and guide future action, rather than with binding, enforceable decisions.

The FRA 2015 report highlighted the importance of remedial bodies' adherence to general requirements of fairness, impartiality and independence.[486] In Hungary, for example, 'oversight' and complaints-handling functions relating to 'extraordinary measures' (such as the surveillance of telecommunications) are both performed by one executive institution: the government and its different ministries.[487]

12.2. Processing of complaints

Representatives from the institutions with remedial powers were asked specific questions about complaints received in the preceding three years, including the numbers per year, their outcomes and other specific details, if this information was available for discussion. For example, the average number of complaints received was discussed during approximately one third of the interviews. The content of the complaints is confidential.

"Very few citizens' complaints relate to intelligence work, and this is for two reasons: the real 'bad guys' don't attach any importance to it, or if the work is done well, they don't know about it." (Expert body)

Respondents referred to 'very rare cases' or very low numbers of complaints from individuals regarding allegedly unlawful activities by intelligence services. The average across different institutions in the selected Member States ranges from 10 to 20 complaints per year, with certain rare deviations in some Member States in relation to specific occurrences, such as the Snowden revelations, cases that became publicly-known due to disclosure by the media, or in response to terrorist attacks. In some cases, the number of complaints received is not publicly available and is confidential – for example, in Italy, the DPA does not publish the number of the complaints; this information can only be communicated to the parliamentary committee COPASIR. Some respondents said they never received any complaints and have no practical experience in handling complaints (or usually receive very few complaints per year). A few respondents expressed concern about abuses of complaint procedures – for example, a DPA noting that '[T]here are people who exercise this right creatively'. However, the relatively low numbers can hardly qualify as abuse. On the other hand, no complaints being received may raise questions regarding the effectiveness and quality of the working system.

"Three or four appeals can reasonably be expected per year, which will not be enough to establish precedents." (Expert body)

In terms of meeting the admissibility criteria (formal requirements) of complaints, the ratio between well-founded and ill-founded complaints differs per Member State and per type of institution presented. The interviews suggest there is a general tendency of complaints from individuals being ill-founded more often than being well-founded. No details or specific examples were disclosed during the interviews and very limited information was provided about the content of the complaints. The respondents described complaints as the 'usual', but acknowledged that these can be complex. They insisted that complaints are treated seriously, stating that investigating them requires expertise and access to the sources of the intelligence services.

482 Council of Europe, Department for the Execution of Judgments of the ECtHR (2016), Case of *Bucur and Toma v. Romania*, H/Exec(2016)6, 20 October 2016, para. 25.
483 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).
484 Estonia, Chancellor of Justice Act (*Õiguskantsleri seadus*), Art. 1(9).
485 FRA (2014c), p. 34.
486 FRA (2015a), pp. 70-72.
487 Hungary, *Governmental Decree No. 185/2016 on the cooperation between the service providers providing encrypted communications and the authorities entitled to conduct secret surveillance operations, 185/2016 (VII. 13.)*, 17 July 2016.

"You should also be aware that many people speculate about the intelligence services, and also many people who have personal or psychological issues also speculate a lot about that." (Expert body)

Respondents representing institutions with remedial powers were asked to describe potential or frequent complainants. Most respondents felt that the usual/typical complainants shared common characteristics, particularly implying that these are people with mental health problems. In describing potential or usual complainants, they chose their words carefully. The most common and neutral description of complainants was 'people who have difficulties'. The respondents also referred to complainants as having psychological problems, with some describing them as 'paranoid', 'mythomaniacs', and 'people who are quite simply suffering from a persecution complex'. Some respondents voiced concern about individuals lodging 'frivolous complaints'. Several noted that, in the absence of notification or other ways for individuals to access information collected about them by the intelligence services, complaints are based on assumptions or speculation about allegedly unlawful activity by the intelligence services.

"Eighty per cent of complaints from individuals come from persons with mental health problems or are manifestly unfounded cases. In this type of case, an internal process has been put in place to forewarn the prosecutor's office."

(Expert body)

"A significant part of the people who file complaints tend to have psychological problems." (Judiciary)

Frivolous complaints

"Concerns about frivolous or vexatious complaints may be remedied by rules allowing the complaint-handling body to dismiss such complaints early in the process. But caution should be exercised to avoid dismissing complaints that are difficult, politically controversial, or simply brought by difficult people."

Born and Wills (2012), p. 193

Information about the number of complaints is publicly available in a limited number of EU Member States. Information from the annual reports of expert bodies in Belgium, Germany, the Netherlands and Sweden is provided below.

In 2015, the Belgian expert body received 22 individuals' complaints (compared to 31 in 2014).[488] In 2014, most of them were dismissed (28 out of 31). By contrast, in 2015, 14 were rejected because they were ill-founded or the Standing Committee I found that it was not competent to process the complaint.[489] The remaining eight complaints were thoroughly investigated. One concerned an individual who complained about being under "oppressive" surveillance by the intelligence services. The Standing Committee I concluded that the services carried out surveillance but that the surveillance was probably carried out by a foreign service. The Standing Committee I raised the question whether the intelligence services had a 'positive obligation' under the constitution or the ECHR to protect a resident against possibly unfounded accusations by a foreign service.[490] The Standing Committee I must inform individuals about their investigations' results in general terms. A specific complaint procedure, taking into account the necessary confidentiality of the intelligence services' operations and the need for transparency, has been established by law with the introduction of the 'targeted surveillance measures'.[491]

The German G 10 Commission functions as a quasi-judicial institution[492] empowered with the ability to handle complaints, either in relation to targeted or strategic surveillance.[493] In 2015, the G 10 Commission received 16 complaints from citizens who believed that they were under surveillance. The commission could not establish any violation of their right to privacy (Article 10 of the constitution).[494] Concerning the cases brought before the administrative courts by individuals who received a notification that they had been under surveillance, the G10 Commission reported in 2015 that 14 complaints followed notification, six of which were assessed within the same year.[495]

In the Netherlands, in 2016, the CTIVD handled 11 complaints related to the AIVD (as compare to seven from April to December 2015). None of these were found to be fully well-founded, and three (four in 2015) were deemed partly well-founded. The minister followed the committee's opinion in all cases.[496] The previous annual report (covering the period 2014–2015) referred to 10 complaints, four of which were deemed partially

488 Belgium, Standing Committee I (2015), p. 7.

489 Belgium, Standing Committee I (2016), p. 7.
490 *Ibid.* p. 37–41.
491 Vande Walle, G. (2013), p. 258, and Belgium, Organic Law of 30 November 1998 on intelligence and security services (*Loi organique du 30 Novembre 1998 des services de renseignement et de sécurité*), 30 November 1998, as amended, Art. 43/4.
492 Wetzling, T. (2017), p. 5.
493 Germany, *G 10 Act*, S. 15.
494 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 6. In 2014, the G 10 Commission received 14 complaints, see Germany, Federal Parliament (*Deutscher Bundestag*) (2016b), p. 6 and in 2013, 21 complaints, see Germany, Federal Parliament (*Deutscher Bundestag*) (2015), p. 6.
495 Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), p. 6 and 8. See Wöckel, H. *in* Dietrich, J.-H. and Eiffler, S. (eds) (2017), p. 1607 and following.
496 The Netherlands, CTIVD (2016a), p. 17 and following and The Netherlands, CTIVD (2017), p. 23 and following.

or fully well-founded.[497] So, the number of complaints remains the same over the years. In the context of some of these complaints, the CTIVD raised 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. The CTIVD stated that it would favour declassifying information that would contribute to a better understanding of the working methods of the services, and in particular cases, it in fact suggested declassifying the information. Only in cases relating to the military intelligence services (GISS) did the minister not follow the CTIVD's suggestions.[498] While the CTIVD had limited remedial powers under the 2002 Act, the 2017 Law changed this and gave CTIVD biding decision powers.

In Sweden, both expert bodies – SIUN and the Commission on Security and Integrity Protection (SIN) – may be approached by citizens wishing to check whether they are under surveillance, and whether this surveillance was lawfully conducted by the intelligence services. Between 2008 and 2016, SIUN audited more than 80 cases. Between 2014 and 2016, SIUN received 46 requests from individuals wishing to check whether SIGINT surveillance was conducted according to the law.[499] These requests concerned the National Defence Radio Establishment as well as the three other entities monitored by SIUN. None of the individual requests highlighted serious faults. Of the total control work, including checks made not on the basis of a request from an individual, four opinions were delivered to the intelligence services, two of them to the National Defence Radio Establishment. SIUN never reached the stage where it may refer a case to the prosecutor or order the National Defence Radio Establishment to terminate data collection.[500]

"We disclose what we are allowed to disclose. However, we do not say, for example, that there's probably more. That would not be right. […] There is a specific formulation. We say: 'we have carried out our checks and there are no concerns from the perspective of data protection'."

(Data protection authority)

"In general, we will not confirm or deny that someone has been wiretapped. We will focus on whether there has been a wrongdoing, an illegal practice, and this we aim to communicate, even though often in an abstract way."

(Expert body)

While discussing the processing of complaints, respondents said they carry out comprehensive investigations on the basis of well-founded (in some cases ill-founded) complaints from individuals. This includes access to the intelligence service's sources or meetings with its staff, and can include inviting complainants to hearings. However, the responses received by individuals regarding complaints are more or less standard: if unlawful activity has taken place, the applicant is informed so that compensation can be sought; but if not, the response –'neither confirm nor deny' ('NCND') – can cover both situations where 'no surveillance actually took place' or where 'it did but was lawful'. As rare exceptions, in a few Member States, individuals are informed if they were under surveillance. Representatives of civil society organisations, lawyers, and academia noted that the standard 'NCND' response makes available remedies ineffective and questioned if the remedies are suited for individuals.

According to representatives of institutions dealing with individual complaints, the response might be different when the intelligence services were found to act 'illegally' or 'unlawfully'.

"I think in this highly complex area government has, in addition to the resources, the added advantage of the knowledge of what [the services] are doing and the ability to 'NCND' everything, which is a problem. We need much more transparency, robustness from the domestic court."

(Civil society organisation)

"So the complaint goes off, the [expert body] will consider it, there may be a hearing, there maybe not be, it may be that the [expert body] hears evidence from the intelligence services or the police, but maybe not, but if it does, I probably would be told, my client might be told, we wouldn't have a right to attend, we wouldn't have a right to approach them. The [expert body] makes a decision and will only notify me if they find a violation." (Lawyer)

Finally, individuals may also prefer to access justice through intermediaries, such as relevant civil society organisations. The latter may play a vital role in taking surveillance-related complaints to court when class actions are allowed, 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.[501] However, in some EU Member States, civil society organisations often lack adequate resources, and few are able to offer comprehensive services to victims of data protection violations.[502]

497 The Netherlands, CTIVD (2015), p. 19 and following.
498 *Ibid.* pp. 22–23.
499 Sweden, SIUN (2017), pp. 4-9.
500 Sweden, National Defence Radio Establishment (*Försvarets radioanstalt*) (2016).
501 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: Poland, Helsinki Foundation for Human Rights (2015).
502 FRA (2014c).

The representatives of civil society organisations interviewed for this report pointed to their contributions to, and role in, litigation, both in national and in EU courts. They litigate with pro bono legal support. All civil society organisations interviewed acknowledged that without pro bono legal support, the litigation – an important and significant part of their work – would not be possible. They stated that a legal remedy implemented in such a manner represents 'an obvious imbalance in terms of process and resources' in power relations between civil society organisations and the state. A similar imbalance affects individuals when seeking remedies. Other relevant factors include the difficulties caused by the costs involved for individuals to take their cases to court; the need for legal knowledge, expertise and support; and the stamina required.

"The only thing that we can do now is to have individual persons going to court. That is a problem, you need to have standing as an individual, you need to be individually targeted e.g. by secret services, then of course comes a question, how can you prove that you have been the target of the secret services because usually you never know, they will never notify you, maybe after 50 years. It is really difficult and has become more difficult for us to have these court cases." (Civil society organisation)

"We did the case pro bono. One of the benefits of the [expert body] is that there are no costs, compared to other proceedings. Even so, for an ordinary complainant there is no legal aid available, so the ordinary complainant would either fund themselves or find a human right organisation willing to take the case pro bono. That is an issue." (Lawyer)

Strategic litigation pursued by civil society organisations plays another important role. It raises awareness among the general public of possible rights violations in the areas of data and intelligence collection, and increases the public's interest in defending their rights and in looking for ways to prevent possible violations.

13 Raising individuals' awareness

Surveillance measures are characterised by secrecy. This is a key impediment to seeking a remedy. Surveillance must be in accordance with the law. However, in such a confidential context, the legality of a measure is not sufficient to ensure individuals' awareness of a potential breach. Several rights, though, may enable individuals to access information, and, where relevant, challenge wrongdoings or unlawful surveillance by intelligence services.

Fieldwork interviews addressed the reasons individuals have for lodging complaints. Respondents' comments mostly related to the implementation of the obligation to inform and the right of access. As one respondent from a national human rights institution put it: 'What will be the point of an individual lodging a complaint if she or he can base their arguments only on rumours?' Clear views on the issues did not emerge from the fieldwork. A variety of opinions and understandings were expressed. These are not particularly specific or well-elaborated, and include contradictory views among respondents from the same Member State. For example, some respondents considered notification or access to information to be a main prerequisite for learning about being subject to surveillance; others considered the provision as a dead letter in the legal framework; while others saw non-application to be problematic. In terms of the duty to notify, taking into account the different practices in the implementation of this obligation and the lack of systematic application in practice, this issue remains unclear, open to interpretation in terms of how to deal with it ('grey area'), not widely discussed in terms of its application, and sometimes questioned if necessary at all in the national legal framework. On the other hand, the limited information collected during the fieldwork shows that notifying individuals that they had been under surveillance has no significant impact on the abuse of complaint procedures.

Access to information and notification obligations

"The legislation should emphasize that transparency and access to information are fundamental principles of democracy and that classification of information must be used sparingly. The criteria for classification should indicate a sufficient degree of harm and certainty to warrant non-disclosure. The legislation should enable a person charged with unlawful disclosure of classified information to raise a public interest defence. The executive should be obliged to promote and facilitate public access to state-held information, including information on the intelligence services."

Born H. and Wills A., (2012), p. 64

"The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public. The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance. In addition, the public should be fully informed of the fact of any illegal surveillance. Information about such surveillance should be disclosed to the maximum extent without violating the privacy rights of those who were subject to surveillance. These Principles address the right of the public to access information and are without prejudice to the additional substantive and procedural rights of individuals who have been, or believe that they may have been, subject to surveillance."

The Tshwane Principles, Principle 10 E

"Experience shows, however, that in the majority of notifications the persons concerned do not bring legal action." (Expert body)

13.1. Freedom of information

To verify and, possibly, challenge surveillance measures, access to public documents may increase individuals' awareness of possible wrongdoings and support them, where relevant, in lodging a complaint. This right, generally grounded in freedom of information laws, contributes greatly to the accountability system. As emphasised by Born and Leigh, "Security and intelligence agencies should not be exempted from domestic freedom of information and access to files legislation. Instead they should be permitted, where relevant, to take advantage of specific exceptions to disclosure principles referring to a limited concept of national security and related to the agency's mandate."[503]

All but two EU Member States – Cyprus and Luxembourg – have enacted Freedom of Information laws, or similar laws. However, all include restrictions based on access to classified information, or the protection of national security, or the activities of intelligence services. These exemptions originate in the need for intelligence services to be able to protect the sources and methods applied to individual operations. Only Hungary does not exclude classified information or state security documents as a general rule. However, the heads of the Hungarian services have the discretion to deny the disclosure of public information on national security grounds.[504]

In Germany, the Security Check Act (*Sicherheitsüberprüfungsgesetz*) prevents citizens from requesting access to information that originates from the three federal intelligence services or other authorities and bodies of the federal state that are classified as "secret" or "top secret".[505] The Federal Administrative Court has clarified that this general exemption from the right to freedom of access to documents also covers documents originating from the intelligence services and held by supervisory authorities.[506]

This blanket exception based on national security shows that, within the legal frameworks of EU Member States, the Freedom of Information principle is, *de jure*, not adapted for individuals attempting to access relevant information and to challenge surveillance techniques. While it is clear that certain information should remain classified, total exceptions could be softened to safeguard individuals' fundamental rights. Notably, legitimate aim and proportionality tests could be conducted before denying access to public documents, or a competent authority could be in charge of assessing the level of confidentiality before issuing the denial.

Nevertheless, interviewed experts stated that there have been situations where Freedom of Information legislation proved useful to compel authorities to disclose certain findings, where national security is deemed not to be at risk and the information is not otherwise publicly available.

13.2. Notification obligation and right to access principles

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 remedial action, and, ultimately, legal scrutiny by judicial or non-judicial bodies.[507] In data protection laws, 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.[508] In the context of surveillance, even circumscribed by the necessary restrictions to safeguard national security and confidentiality,[509] these rights also enhance accountability of the intelligence services and help to develop citizens' trust in government actions.[510]

In the United Kingdom, for instance, IOCCO has the power to inform individuals if it finds that they have been adversely affected by any serious error or by any wilful or reckless conduct by a public authority.[511] Such notifications have led individuals to lodge complaints with the IPT.[512] This principle was confirmed in the Investigatory Powers Act, which obliges the Investigatory Powers Commissioner to inform persons of any "significant prejudice or harm" relating to them of which the Commissioner is aware. In doing so, the Investigatory Powers Commissioner will have to assess the seriousness of the error, to consider the potential impact on public interest or national security, and to inform the persons of their rights to apply to the IPT. However, the fact that there has been a breach of an individual's ECHR rights alone is not sufficient for an

503 Born, H. and Leigh, I. (2005), p. 44.
504 Hungary, Act CXXV of 1995 on the national security services, 27 March 1996, Article 48(1).
505 Germany, Act to Regulate Access to Federal Information (*Informationsfreiheitsgesetz, IFG*), Section 3 No. 8.
506 Germany, Federal Administrative Court (*Bundesverwaltungsgericht*), BVerwG 7 C 18.14, 25 February 2016.
507 Born H. and Wills A., (2012), p. 52.
508 See for example Germany, Federal Constitutional Court (*Bundesverfassungsgericht*), 1 BvR 2226/94, 14 July 1999, para. 169.
509 See for example GDPR, Article 23(1).
510 UN, Human Rights Council, Scheinin, M. (2010), p. 23.
511 United Kingdom, Home Office (2015), 'Code of Practice of Acquisition and Disclosure of Communications Data', March 2015, ss. 6.22 and 8.3. See also, United Kingdom, IOCCO (2016a), paras 1.14 and 2.2.
512 United Kingdom, IOCCO (2016a), p. 71.

error to be serious, thus narrowing down the classes of individuals who may be informed.[513]

The 2015 FRA report emphasised 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, and recalled the principle of judicial review enshrined in Article 47 of the Charter.[514] The ECtHR considers the issue of notification to be inextricably linked to the effectiveness of remedies before the court, as long as it no longer jeopardises the purpose of the surveillance. While the court again emphasises the crucial importance of both the notification obligation and the right to access principles, it does note that the effectiveness of remedies may be guaranteed by the existence of one *or* the other right. This specification seems to take into account the difficulties inherent in the practical implementation of these rights – especially the obligation to notify.

ECtHR case law: notification and access to information in cases of surveillance

Notification

"It may not be 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. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. Therefore, 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. As 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, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, paras. 287*

Access to information

"It is worth noting in this connection that in order to be entitled to lodge such a request the person must be in possession of the facts of the operational-search measures to which he or she was subjected. It follows that the access to information is conditional on the person's ability to prove that his or her communications were intercepted. Furthermore, the interception subject is not entitled to obtain access to documents relating to interception of his or her communications; he or she is at best entitled to receive "information" about the collected data. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved in accordance with the procedure prescribed by law, that is, he or she has not been charged or the charges have been dropped on the ground that the alleged offence was not committed or that one or more elements of a criminal offence were missing. It is also significant that only information that does not contain State secrets may be disclosed to the interception subject and that under Russian law information about the facilities used in operational-search activities, the methods employed, the officials involved and the data collected constitutes a State secret (see paragraph 52 above). In view of the above features of Russian law, the possibility to obtain information about interceptions appears to be ineffective."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 289*

Minimum requirement for remedies' effectiveness

"The Court concludes from the above that the remedies referred to by the Government are available only to persons who are in possession of information about the interception of their communications. Their effectiveness is therefore undermined by the absence of a requirement to notify the subject of interception at any point, or an adequate possibility to request and obtain information about interceptions from the authorities. Accordingly, the Court finds that Russian law does not provide for an effective judicial remedy against secret surveillance measures in cases where no criminal proceedings were brought against the interception subject."

ECtHR, Roman Zakharov v. Russia *[GC], No. 47143/06, 5 December 2015, para. 298*

513 United Kingdom, Investigatory Powers Act (2016), s. 231. Not yet in force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

514 FRA (2015a), p. 61.

13.3. Restrictions on notification obligation and right of access

The FRA 2015 report details how the obligation to inform and grant access are completely exempted in some Member States (the Czech Republic, Ireland, Lithuania, Poland and Slovakia) and restricted in the other 23 Member States.[515]

"The [expert body] drafts a report on the basis of the complaint, which is sent to the individual. […] [W]hichever of these options is chosen, it comes down to the same thing: there is no access to classified documents." (Expert body)

"The services are obliged to provide information, but there is no obligation concerning the specific content of information provided […] they must provide information, but their response can also be in the negative. For example: 'no, we have no data on file', or similar. If the matter were given close consideration, then individual legal protection would have to be improved." (Academia)

However, there are differences in the conditions and level of restrictions.[516] Limitations can be based on the *direct* aspect of the access to information, on the general aspect of surveillance, on the level of classifications, on national security, on the operational impact of surveillance, or on other procedural grounds.

The right to *indirect* access is the right for an individual to access his/her own data indirectly through the DPA or the expert body.[517] Such right exists in 12 EU Member States: Austria, Belgium, Bulgaria, Cyprus, Finland, France, Hungary, Ireland, Italy, Luxembourg, Portugal and Sweden. Between 2014 and 2016, the French DPA (CNIL) received an increasing number of indirect access requests: 159 in 2014, 243 in 2015, and 435 in 2016.[518] The French expert body (CNCTR) in charge of assessing the legality of the technique used received 51 complaints between October 2015 and October 2016.[519]

As stated in the 2015 FRA report,[520] of the five Member States with detailed legislation on general surveillance of communications, only Germany and Sweden stipulate a notification requirement in cases of general surveillance of communications. The obligation to inform does not apply if a) the search terms are not directly related to the individual (Sweden)[521] or b) if the data are deleted immediately (Germany).[522] The German 2016 reform of the BND Law does not stipulate any notification requirement in case of foreign-foreign surveillance measures.[523]

In some Member States – such as Ireland, Latvia, Spain and Sweden[524] – the obligation to inform and/or the right of access are restricted because of rules applicable to classified documents and official secrets. In Latvia, although amendments to the Investigatory Operations Law adopted on 10 March 2016 strengthened the state's obligations concerning the duty of those conducting operational activities to inform *ex post* the individual against whom the activities were conducted, such notification does not apply in cases of, among others, a possible threat to another person's legitimate rights and interests, national security or criminal procedure.[525]

The 2015 FRA report detailed how the right of access and obligation to notify may be limited on the ground that divulging the information could threaten the objectives of the intelligence services or national security.[526] In ten Member States, individuals are notified or information is provided at the end of surveillance, and only when the threat to national security has ceased to exist: Bulgaria, Croatia, Denmark, Finland, Germany, Greece, Latvia, the Netherlands, Spain and Romania.[527] In Denmark and Finland, the general obligation to inform individuals at the end of surveillance may be omitted or postponed upon a court order.[528]

Finally, in some Member States, additional conditions on *ex post* notification or access to data are enshrined in law.[529] For instance, in Sweden, individuals shall be notified of signals intelligence only if the search terms used therein are directly related to them, and not if reasons of confidentiality prevent notification.[530]

515 FRA (2015a), p. 62.
516 See also UN, GA (2014b), para. 39.
517 FRA (2015a), pp. 66-67.
518 See France, CNIL (2014) p. 48; CNIL (2015) p. 57 and CNIL (2016), p. 63.
519 France, CNCTR (2016), p. 90.
520 FRA (2015a), p. 63.
521 Sweden, Signals Intelligence Act (Lag [2008:717] *om signalspaning i försvarsunderrättelsetjänst*), Art 11 (a).
522 Germany, *G 10 Act*, S. 12.
523 Wetzling, T. (2017), p. 14.
524 See FRA (2015a) p. 64 for further information on these restrictions in Spain and Latvia.
525 Latvia, Investigatory Operations Law, Art. 24 (1).
526 FRA (2015a), p. 65.
527 See FRA (2015a) p. 64 for further information on this restriction in Romania and Denmark.
528 Denmark, Administration of Justice Act, Consolidated Act no. 1255 of 16 November 2015 with amendments (*Retsplejeloven, lovbekendtgørelse nr. 1255 af 16. november 2015 med senere ændringer*), Section 788 (1), (4).
529 See FRA (2015a) p. 65 for further information on this in Bulgaria, Croatia and Germany.
530 Sweden, Signals Intelligence Act, Arts. 11 (a) and 11 (b).

13.4. Restrictions on notification obligations and right to access with safeguards

Some Member States provide for the involvement of the expert body or a court in scrutinising whether the invoked grounds for restricting the rights of notification or access are reasonable. Examples below show that further controls assessing justifications of restrictions differ from one Member State to another. Some Member States – such as Germany and the Netherlands – provide for review of a notification's exemption by the expert oversight bodies. Others – such as Cyprus, Greece and the United Kingdom – vest their DPA with such competence. These assessments by oversight bodies also show that the notification's obligation is not implemented evenly across EU Member States.

In Cyprus and Greece**,** the DPA may decide to restrict or lift the obligations to inform and grant access on the grounds of national security, upon request of the intelligence services, and as stipulated by the data protection laws. In Germany, the G 10 Commission decides for how long the information may be withheld, unless it unanimously decides that, even after five years, disclosing the information would endanger national interests.[531]

In the United Kingdom, the intelligence services may rely upon the exemption for national security cases, which is provided in the data protection law.[532] The Secretary of State has issued certificates exempting the intelligence services from the application of data protection principles. Nonetheless, the DPA may assess whether invoking the relevant exemptions justifying nondisclosure and/or the "neither confirm nor deny response" was justified. In assessing the lawfulness of the non-disclosure of the information, the DPA may ask the services for reasoned explanations but has access to confidential information only in very exceptional cases. Individuals will not be given access to any of the explanations or confidential information provided to the Information Commissioner by the intelligence services, unless very specific exceptions are met.[533]

Promising practice

Transparent scrutiny of denials of rights

In both the **Netherlands** and **Germany**, oversight bodies assess the grounds on which notification of or access to information was denied. As no one was notified between 2007 and 2010, in 2013 the CTIVD decided to launch a special investigation on the obligation to inform. The Dutch oversight body found out that in the meantime, thirteen persons had been notified. A similar investigation started in 2016.

In Germany, the G 10 Commission may decide to notify individuals based on information provided by the intelligence services. In 2016, the oversight body decided to not yet inform 1,040 persons/institutions, and unanimously agreed that 188 would never be informed. In cases of strategic surveillance, the G 10 Commission dealt with 58 cases for information related to international terrorism. In the majority of cases (51), the BND informed the G 10 Commission that the individual could not be individualised through the surveillance measure. In six cases, the commission decided to postpone providing the information; in no cases rejected the information indefinitely; and in one case took note that the intelligence service (BND) provided the information.

See The Netherlands, (CTIVD) (2013) and CTIVD (2016), p. 14; Germany, Federal Parliament (Deutscher Bundestag) *(2017a), pp. 6 and 8*

While discussing the difficulties of notifications and the right to access information, the respondents interviewed in the selected EU Member States shared a variety of opinions. For example, in cases of general communications surveillance, it might be problematic to notify all subjects of the intelligence activities or ensure access to information when the intelligence services have no data about a specific individual. These arguments are not relevant in case of completed targeted surveillance activities. During some interviews, representatives from the oversight bodies, and other experts, questioned the principle of notification in the context of fundamental rights protection. They maintained that the value would lie in a systematic implementation of the safeguards built in the oversight process that would possibly prevent breaches of an individual's fundamental right. If the whole system of checks and balances is implemented through effective oversight, redress might not be necessary. By drawing an analogy to 'privacy by design', the proposed approach can be called 'data protection oversight by design'. The interviewees questioned the value of having the duty of notification defined in the legislative framework but not applicable in practice. The respondents called for a possibility of individual legal protection, possibility to seek redress. Representatives

531 Germany, *G 10 Act*, s. 12.
532 United Kingdom, Data Protection Act 1998, s. 28.
533 United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding on National Security Cases (DPA)', 2 September 2013.

from civil society organisations, practicing lawyers and academia tended to identify non-application of the duty to notify as problematic, especially with regard to an individual who might seek remedies. They also questioned the effectiveness of the redress, which is often linked to notification.

To conclude, even if secrecy does restrict individuals' awareness, it does not completely exclude it, either. FRA's research findings show that freedom of information principles are completely exempted in the context of surveillance. In this case, a degree of proportionality could be applied to ensure that no blanket exception based on national security is applied to freedom of information laws. Consequently, the obligation to inform and the right of access, either separately or combined, are crucial enablers of individuals' awareness. FRA research indicates that in a large majority of Member States, these rights are restricted to meet national security and confidentiality requirements, but are not left unsupervised.

14

Remedial bodies' challenges: access to classified information and necessary expertise

14.1. Access to classified information

ECtHR Rules of the Court

Rule 33 – Public character of documents

1. All documents deposited with the Registry by the parties or by any third party in connection with an application (...) shall be accessible to the public (...).

2. Public access to a document or to any part of it may be restricted in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties or of any person concerned so require, or to the extent strictly necessary in the opinion of the President of the Chamber in special circumstances where publicity would prejudice the interests of justice.

3. Any request for confidentiality made under paragraph 1 of this Rule must include reasons and specify whether it is requested that all or part of the documents be inaccessible to the public.

Rule 63 – Public character of hearings

1. Hearings shall be public unless, in accordance with paragraph 2 of this Rule, the Chamber in exceptional circumstances decides otherwise, either of its own motion or at the request of a party or any other person concerned.

2. The press and the public may be excluded from all or part of a hearing in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the Chamber in special circumstances where publicity would prejudice the interests of justice.

3. Any request for a hearing to be held in camera made under paragraph 1 of this Rule must include reasons and specify whether it concerns all or only part of the hearing.

ECtHR, Rules of the Court, Registry of the Court, 14 November 2016, pp. 17 and 34

There is no harmonisation among Member States of the conditions under which classified information may be disclosed and used as evidence during judicial proceedings. Most Member States do not allow courts to use intelligence information that is not available to the parties and that does not meet evidential standards. In Italy, for example, every piece of evidence must be disclosed to all parties. Classification of documents can only be challenged by a judge or prosecutor in cases where such information may be deemed as having been illegitimately classified.[534]

The FRA 2015 report highlighted how NCND policy can make remedial bodies inaccessible in practice.[535] To tackle this challenge, and increase remedies' effectiveness and transparency, some Member States have established alternative mechanisms. These include the use of 'second-hand' evidence, the 'assumed facts', the 'closed material procedures', the establishment of open hearing and *in camera* sessions and the use of 'shielded witnesses'.

The United Kingdom has developed adapted procedures aimed at enhancing transparency in access to information for complaints involving classified intelligence. The Investigatory Powers Tribunal may assume, "for the sake of the argument", that the facts asserted by the complainant are true ('assumed facts').[536] It may also implement the so-called 'Closed Material Procedures', which allow the court to use classified information as evidence.[537] Section 68(6) of the RIPA, which was not amended by the IPA, provides that "[i]t shall be the duty of the persons specified in subsection (7) to disclose or provide to the Tribunal

534 See ECtHR, *Nasr and Ghali v. Italy*, No. 44883/09, 23 February 2016; Bigo, D., Carrera, S., et al. (2014), p. 112.
535 See FRA (2015a), p. 69.
536 United Kingdom, IPT, (2016), p. 8.
537 Bigo, D., Carrera, S., et al. (2014), pp. 21-25.

all such documents and information as the Tribunal may require for the purpose of enabling them (a) to exercise the jurisdiction conferred on them by or under section 65; or (b) otherwise to exercise or perform any power or duty conferred or imposed on them by or under this Act." In such cases, only the judges and security-cleared 'special advocates' may access secret information. Finally, the IPT may decide to hold open *inter-partes* hearings for cases involving classified information, either on the basis of agreed or assumed facts. The practice to hold open hearings have been increasingly used by the IPT, reaching a quarter of all the complaints decided by the Tribunal in 2015.[538]

It has been the long-standing policy of the United Kingdom government to give a 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 "if allegations of interception or surveillance are made, but not denied, then, in the absence of the NCND policy, it is likely to be inferred by a complainant that such acts are taking place",[539] and that it does not interfere with the right to privacy in cases where there is no relevant information held on the complainant.[540]

Similarly, in France, the 2015 intelligence law significantly enhanced the remedies available to individuals.[541] Complainants can now bring a case before a specialised chamber (*formation spécialisée)* of the Council of State, the highest administrative court. Judges sitting on the specialised chamber are security cleared *ex officio*. The procedure requires first that either the CNCTR or the CNIL – depending on the object of the complaint – performs initial checks (see section on quasi-judicial bodies). To safeguard the secrecy of the documents handled while at the same time ensuring effective remedies, asymmetric adversarial proceedings are prescribed by law. The complainant, who can be heard, does not see any confidential documents communicated by the services or the CNCTR and/or CNIL to the specialised chamber. The chamber sits in camera when dealing with secret documents. If no surveillance measure was implemented against the complainants, the chamber informs them that no illegality was observed after verification, without stating whether a surveillance measure was implemented. If an illegality is found, the complainant is informed and the chamber annuls the authorisation of the intelligence measure and orders the deletion of the collected data.

The specialised chamber of the Council of State also applies a policy where no confirmation nor denial is provided to the complainant, although only in cases where no illegality has been established. In such cases, the decision of the panel will not state whether a surveillance technique has or has not been implemented, nor will it assert whether the complainant is or is not included in a database managed by intelligence services. On the other hand, where unlawful surveillance – either in the application of a surveillance technique or in the processing of data – has been established by the Council of State, it informs the complainant and requests the annulment of the authorisation to implement a surveillance technique or the rectification, update or deletion of the data illegally processed. In May 2017, the specialised chamber issued for the first time a deletion order addressed to the Ministry of Defence, because it illegally processed personal data.[542]

Some states may use additional protection by bringing classified information as evidence through testimonies of anonymous witnesses. This is the case in Germany, Spain and the Netherlands. In the Netherlands, the Act on Shielded Witnesses allows members of the security services to disclose anonymously classified information during a specific procedure. Such procedure must be held before the trial, in closed session, and the information is only disclosed to the judge and security-cleared special advocates.[543] In Spain and Germany, courts may rely on 'second-hand' evidence, consisting of declarations made by officials who did not have direct access to the classified information but have received a description of such information. The information remains 'confidential' and should therefore be disclosed only to a limited and security-cleared number of persons.[544] These mechanisms, though, still present some limits, as they imbalance the adversarial procedure, in which the defendant, excluded from the hearings, will not have the possibility to challenge the evidence.

Some Member States allow judicial bodies to declassify information – for example, in France and Poland. In Poland, the Prosecutor General is entitled to challenge the secrecy clause (*klauzula tajności*) of classified information by either modifying or completely declassifying it.[545] In France, in cases where the specialised chamber considers the illegality to constitute an offence, it will forward all information to the prime minister, who will decide whether to declassify all or part of the confidential information.[546]

538 United Kingdom, IPT, (2016), p. 23.
539 *Ibid.* p. 10.
540 United Kingdom, IPT (2014).
541 France, Interior Security Code, Art. L. 841-1 and L. 841-2 as well as Administrative Justice Code, Art. L. 311-4-1 and L. 773- to L. 773-8.
542 France, Council of State (*Conseil d'Etat*), *M. A.B.*, No. 396669, 5 May 2017.
543 Bigo, D., Carrera, et al. (2014), pp. 25-26
544 *Ibid.* pp. 28 and 30.
545 Poland, Law on Prosecutor Office (*Prawo o prokuraturze*), 28 January 2016, Art. 57.5.
546 France, Administrative Justice Code (*Code de justice administrative*), Art. L773-7.

Striking a balance

"[B]oth the principle of the separation of powers as well as the existence of other constitutional demands require that [the legislator] strikes a reasonable balance between the rights of the individuals involved to apply for judicial legal remedy and the right to a fair trial as well as [...] the constitutional requirements inherent to safeguarding the fundamental interests of the Nation."

France, Constitutional Court (Conseil constitutionnel), Mrs Ekaterina B., spouse of D., and others, Decision 2011-192 QPC, *10 November 2011 [translation by Constitutional Court]*

"As for the requirements to be met by judicial review of the existence and validity of the reasons invoked by the competent national authority with regard to State security of the Member State concerned, it is necessary for a court to be entrusted with verifying whether those reasons stand in the way of precise and full disclosure of the grounds on which the decision in question is based and of the related evidence. Thus, the competent national authority has the task of proving, in accordance with the national procedural rules, that State security would in fact be compromised by precise and full disclosure to the person concerned of the grounds which constitute the basis of a decision taken (...). It follows that there is no presumption that the reasons invoked by a national authority exist and are valid. In this connection, the national court with jurisdiction must carry out an independent examination of all the matters of law and fact relied upon by the competent national authority and it must determine, in accordance with the national procedural rules, whether State security stands in the way of such disclosure.

If that court concludes that State security does not stand in the way of precise and full disclosure to the person concerned of the grounds on which a decision (...) is based, it gives the competent national authority the opportunity to disclose the missing grounds and evidence to the person concerned. If that authority does not authorise their disclosure, the court proceeds to examine the legality of such a decision on the basis of solely the grounds and evidence which have been disclosed. On the other hand, if it turns out that State security does stand in the way of disclosure of the grounds to the person concerned, judicial review (...) of the legality of a decision (...) must (...) be carried out in a procedure which strikes an appropriate balance between the requirements flowing from State security and the requirements of the right to effective judicial protection while limiting any interference with the exercise of that right to that which is strictly necessary."

CJEU, C-300/11, ZZ v. Secretary of the State of Home Department, *4 June 2013, paras. 60-64*

"Nonetheless, it would have been desirable – to the extent compatible with the preservation of confidentiality and effectiveness of the investigations concerning the applicant – for the national authorities, or at least the Supreme Administrative Court, to have explained, if only summarily, the extent of the review they had carried out and the accusations against the applicant. (...) Having regard to the proceedings as a whole, to the nature of the dispute and to the margin of appreciation enjoyed by the national authorities, the Court considers that the restrictions curtailing the applicant's enjoyment of the rights afforded to him in accordance with the principles of adversarial proceedings and equality of arms were offset in such a manner that the fair balance between the parties was not affected to such an extent as to impair the very essence of the applicant's right to a fair trial."

ECtHR, Regner v. The Czech Republic [GC], *No. 35289/11, 19 September 2017, paras. 160-161*

14.2. Necessary expertise

Past FRA research has identified the judges' lack of specialisation in data protection as a serious obstacle to effectively remedy data protection violations.[547] 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.

In the area of surveillance, 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 services may lead a judge to defer to the national intelligence services and their claim that national security and other special circumstances apply.[548]

Lack of expertise can be circumvented by establishing specific mechanisms. In most cases, where bodies are granted remedial powers but lack technical understanding of the matters, complementarity is established with either *ad hoc* experts or non-judicial expert bodies. Another form of tackling the lack of specialisation of the judges is the establishment of quasi-judicial bodies. The following section details how some Member States have developed these mechanisms to allow expert assessment of complaints.

547 FRA (2014c).

548 Forcese, C. (2012), p. 186.

Cooperation and complementarity between remedial and expert bodies

Some expert bodies, although not able to issue binding decisions, play an essential complementary role within the remedial landscape. Their expert understanding of both the technicalities and the legal framework put them in a good position to review complaints. Thus, when such experts are allowed to communicate with judicial or non-judicial bodies entitled to issue binding decisions, such cooperation can fill the expertise gap.

In France, individuals can ask the CNCTR to check whether a domestic or international surveillance technique was illegally implemented against them.[549] The commission follows the same verification procedure as for *ex post* controls launched on its own initiative.[550] Once completed, individuals are informed that a verification procedure took place. No further information is provided. Should the verification reveal an illegality, the CNCTR can address a recommendation to the prime minister, the relevant minister and the intelligence service requesting the suspension of the surveillance measure and the destruction of the data collected.[551] When the recommendations are not followed, the president or three members of the CNCTR can bring the case before the Council of State.[552] The CNCTR received 51 such verification requests during the first year since its establishment.[553] The Danish Oversight Board (TET) proceeds in a similar manner. However, in very specific cases with special circumstances, it can grant individuals full or partial access to information held by the services.[554]

In the Netherlands, the Intelligence and Security Services Act adopted in 2017 modifies the remedial mechanism available to individuals. While until the new law comes into force, the Dutch expert body (CTIVD) acts as an "independent complaints advisory committee"[555] in the sense that individuals are not able to complain directly to the CTIVD and the latter is not able to issue binding decisions, the 2017 Act creates a sub-committee within the CTIVD, responsible for handling complaints and issuing binding decisions.[556]

549 France, Interior Security Code, Art. L. 833-4 and L. 854-9.
550 France, CNCTR (2016), p. 90.
551 France, Interior Security Code, Art. L. 833-6.
552 *Ibid.* Art. L. 833-8.
553 France, CNCTR (2016), p. 90.
554 Denmark, Act on the Danish Security and Intelligence Service, Consolidated Act no. 1600 of 19 December 2014 with amendments, Section 13 (2) and Denmark, Act on the Danish Defence Intelligence Service, Consolidated Act no 1 of 4 January 2016, Section 10 (2). See also TET's website.
555 The Netherlands, CTIVD (2015), p. 19.
556 The Netherlands, Act on the Intelligence and Security Services 2017 (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 2017*), Arts. 97, 114 and 126.

The FRA 2015 report highlighted existing cooperation between some DPAs and the courts, and in particular the *Schrems v. Data Protection Commissioner* case.[557] Complementarity is also crucial at an earlier stage, where some non-judicial bodies act as a filter to assess the legitimacy of the complaints to transfer only well-founded ones to the competent remedial body. This is the case, for instance, in Belgium, where citizens' petitions submitted to the Belgium Ombudsman (*Médiateurs*) and referring to the intelligence services can be forwarded to the Belgian expert body, the Standing Committee I. Before transferring a complaint to the Standing Committee I, the Ombudsman will assess the complaint and preselect relevant petitions from those that are deemed irrelevant because, for example, they are based on 'paranoia'. Such partnership among bodies is an important tool to enhance remedies' effectiveness, as it enables the competent remedial body to focus its assessment only on well-grounded complaints.

This trend was confirmed during the interviews FRA conducted in selected Member States. In France, for example, the members of the specialised chamber of the Council of State (*Conseil d'Etat*) have been trained on the techniques used by the intelligence services. In Sweden, the integrity protection counsels (some of whom are former judges) – who are appointed by the government to protect the interest of the people before the Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*) – noted that the court provides them with training on the legal framework and substance to facilitate their work. Representatives of the United Kingdom's Investigatory Power Tribunal arranged visits of judges to the premises of the intelligence services or law enforcement institutions to permit them to gain direct knowledge of general surveillance of communication.

Quasi-judicial bodies

Four Member States – France, Germany, Ireland and the United Kingdom – introduced a system of specialised judges or courts to deal with cases in the area of surveillance. In addition, oversight bodies in Germany and Belgium (the G10 Commission and the Standing Committee I) are given powers similar to those of a court, qualifying them as quasi-judicial mechanisms. The composition, competences and procedures followed by the British IPT, the Irish Complaints Referee, the Belgian Standing Committee I and the German G10 Commission are detailed in the FRA 2015 report.[558] In France, the 2015 law on intelligence

557 FRA (2015a), p. 68.
558 FRA (2015a), pp. 68-69.

established a special litigation procedure, through which a specialised chamber (*formation spécialisée)* of the Council of State has competence to decide on complaints related to surveillance techniques. This formation is composed of a president and four judge-rapporteurs. Specific procedures were designed to conciliate the obligation to respect the secrecy of the files with the adversarial procedure.[559]

In the United Kingdom, between 2014 and 2017, the IPT handed down seven judgments in relation to intelligence and security services.[560] The Independent Reviewer of Terrorism Legislation recommended that the IPT 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.[561] Of these recommendations, the Investigatory Powers Act followed the suggestion regarding appeals on points of law.[562] However, applicants need to be given permission (leave) to appeal by the IPT, or if that is refused, by the relevant appellate court.[563]

This report's findings confirm the FRA 2015 report's conclusions that quasi-judicial mechanisms contribute to the development of expertise in this area, and reinforce remedial actors' access to classified information.[564]

Number of complaints received by specialised judicial or quasi-judicial bodies

In 2015, 35 % of the 251 complaints received by the IPT were directed against 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 (42 %); local authorities (12 %); and other public authorities, such as the Department for Work and Pensions (10 %). 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 2015. General statistics on the outcomes of 2015 complaints indicate, however, that the IPT upheld the complaint and ruled in favour of the complainant in eight of 251 cases (which covers all complaints resolved by the IPT in 2015, including those carried over from previous years).

United Kingdom, IPT (2016), p. 22

In October 2016, the Council of State issued its first decisions. In March 2017, 146 complaints were registered (136 concerning intelligence files and 10 concerning intelligence measures). A total of 52 decisions delivered. Some of these decisions highlighted the compatibility of the procedure with the ECHR.

France, Council of State, Contrôle des techniques de renseignement, *19 October 2016, CNCTR (2016), pp. 91-93; and France, DPR & CNCTR (2017), p. 37*

Finally, individuals who are unsatisfied with the decisions made by a judicial or non-judicial body may appeal this decision. In some cases, individuals may appeal a decision at national level: in Austria, for instance, individuals may lodge a complaint to the DPA following a decision made by the Legal Protection Commissioner in cases where security is at stake.[565] However, in most cases, the only route available will be to apply to the ECtHR. In the United Kingdom, until adoption of the Investigatory Powers Act in 2016, the only route for appeal following a decision by the IPT was the ECtHR. This absence of judicial review was challenged in 2017, and the Divisional Court confirmed that RIPA did not provide for appeal to the decision of the IPT.[566] Article 67A of the Investigatory Powers Act has tackled this issue and now provides the possibility for individuals to appeal any determination of the Tribunal to either the Court of Appeal in England and

559 France, Conseil d'Etat.
560 United Kingdom, IPT, *Belhaj v. Straw*, IPT/13/132-9H, 7 February 2014, *Liberty, Privacy International, Bytes for All and Amnesty v. UK*, judgments of 5 December 2014 and 6 February 2015, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 22 June 2015, *Privacy International and Greennet & Others v. the Secretary of State for Foreign and Commonwealth Affairs and GCHQ*, IPT 14/85/CH, 12 February 2016, *Privacy International v. the Secretary of State for Foreign and Commonwealth Affairs, GCHQ, MI5 and MI6*, IPT/15/110/CH, 17 October 2016, and *Privacy International & Others*, [2016] UKIPTrib 15_110-CH, 8 September 2017.
561 Anderson, D. (2015), p. 305.
562 United Kingdom, Regulation of Investigatory Powers Act 2000, Section 67A.
563 United Kingdom, Investigatory Powers Act 2016, s. 67A (6) (b). Not yet into force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).
564 FRA (2015a), pp. 68-69.
565 Austria, Police State Protection Act (*5. Bundesgesetz mit dem das Bundesgesetz über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatschutzes (Polizeiliches Staatsschutzgesetz – PStSG) erlassen und das Sicherheitspolizeigesetz geändert werden*), BGBl. I Nr. 5/2016, Art. 14.
566 United Kingdom, *R (On the Application Of) v Investigatory Powers Tribunal, Court of Appeal - Administrative Court, February 02, 2017,* [2017] EWHC 114 (Admin), 2 February 2017.

Wales or the Court of Session, whichever appears to be the most appropriate to the court.[567]

Previous sections identified two main challenges for both judicial and non-judicial remedial bodies in reviewing complaints: denials of access to classified information and a lack of expertise, much needed in such a complex area. However, FRA's research findings show that innovative systems introduced in some Member States – alternative mechanisms to access classified data, complementarity between remedial and expert bodies, establishment of quasi-judicial bodies and adapted adversarial procedures – may circumvent the main obstacles to judicial bodies implementing effective remedies, by introducing partial access to information and a certain level of expertise. On this basis, remedial bodies will have the ability to perform informed investigations and deliver reasoned decisions. An effective remedy is secured when a binding decision includes the order to terminate the surveillance measure, destroy the data and provide individuals with appropriate compensation. Less than two thirds of EU Member States provide remedial bodies with both access to the information and binding decisions. General surveillance of communications makes effective remedies even more difficult to implement. Remedies can only be provided on an individual basis, i.e. after identification of the individual who has submitted a complaint within the general data collected.

567 United Kingdom, Investigatory Powers Act (2016), s. 67A. Not yet in force and will be brought into force in due course by means of regulations made by the Secretary of State (See United Kingdom, Investigatory Powers Act 2016, Explanatory Note).

General conclusions

ECtHR case law: using oversight to enhance citizens' trust

"[T]he external, preferably judicial, a posteriori control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance [...] by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained. The significance of this control cannot be overestimated in view of the magnitude of the pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks."

ECtHR, Szabo and Vissy v. Hungary, No. 37138/14, 12 January 2016, para. 79

While this report shows that most EU Member States have enacted intelligence laws and have tasked independent expert bodies with overseeing the work of their intelligence services, it also reveals that opinions of these bodies' efficiency are mixed. Similarly, although diverse remedies are provided for in law, critics contend that actually accessing them is a less straightforward matter. Failing to confront these flaws carries the risk of undermining the public's trust in their governments' pledges to uphold the rule of law even when confronted with challenges that may make short-cuts look tempting.

With international intelligence cooperation as an absolute must in light of today's myriad threats, accountability, too, has to take on cross-border dimensions. Introducing safeguards specifically tailored to international cooperation would both ensure that intelligence sharing is conducted in a fundamental rights-compliant manner and reinforce the credibility of any data received. This would ultimately strengthen trust among partners – in turn encouraging more cooperation efforts, which have the potential to bring widespread benefits to the European public and beyond. Effective cooperation among oversight entities in different Member States could play an important role in fostering such trust.

"We want to strengthen our ties with the [other] European oversight committees, parliamentary, non-parliamentary, expert bodies, does not matter, everybody is welcome here and we do visits to them, and not only to say 'hello, how are you', but we also are trying to set up a system that we can work together." (Expert body)

Effective accountability systems involve a plurality of actors and require continuity, i.e., provide for oversight before, during and after any surveillance measures are utilised. As the European Court of Human Rights has emphasised, and as outlined in this report, certain safeguards are indispensable for ensuring accountability, particularly given the need for secrecy to carry out effective surveillance work. These include providing for reviews of the legality of measures deployed, and ensuring that entities overseeing the work are independent, have adequate resources (including expert knowledge), are accorded sufficient competences (including access to classified data), and are transparent.

Data protection rules and other rule of law principles should not be seen as potential hurdles to protecting the security of Europe's citizens, but instead as sources of mutual benefits for individuals and intelligence services. Respecting these rights and principles paves the way for more accurate data collection and analysis, renewed trust among European citizens towards their intelligence services and, as a result, a more effective defence of national security.

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.

Anderson, D., Independent Reviewer of Terrorism Legislation (2016), *Report of the bulk powers review*, London, August 2016.

Belgium, House of Representatives (2016), 'Magazine La chambre', *LaChambre.be*.

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.

Belgium, Standing Intelligence Agencies Review Committee (Standing Committee I) (*Comité permanent de contrôle des services de renseignements et de sécurité* – Comité Permanent R) (2016), *Rapport d'activités 2015 Activiteitenverslag 2015*, 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.

Born, H. (2003), *Parliamentary Oversight of the Security Sector – Principles, mechanisms and practices*, Geneva, Centre for the Democratic Control of Armed Forces (DCAF) and Inter-Parliamentary Union (IPU).

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. (2015), *Making international intelligence cooperation accountable*, Geneva, Centre for the Democratic Control of Armed Forces (DCAF).

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

Bos-Ollermann, H. (2016), *New surveillance legislation & intelligence oversight challenges: the Dutch experience*, International Intelligence Oversight Forum 2016.

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.

Bulgaria, National Bureau for Control over Special Intelligence Means (*Национално бюро за контрол на специалните разузнавателни средства, NBKSRS*) (2017), *Report of the National Bureau for Control over Special Intelligence Means for the performance of the operations in 2016* (*Доклад На Националното Бюро За Контрол На Специалните Разузнавателни Средства За Извършената Дейност През 2016 Г)*, Sofia, 31 May 2017.

Burgstaller, M. and Kubarth, L. (2016), 'Zentrale Daten des Rechtsschutzbeauftragten für 2015', SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (3).

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.

Council of Bars and Law Societies of Europe - CCBE (2016), *Recommendations on the protection of client confidentiality within the context of surveillance activities*, Brussels, CCBE.

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, Commissioner for Human Rights (2016), *National human rights structures: protecting human rights while countering terrorism*, 6 December 2016.

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 (2016b), *Mass Surveillance – Who is watching the watchers?*, Strasbourg, Council of Europe Publishing.

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

Croatia, Council for Civilian Oversight (*Vijeće za građanski nadzor sigurnosno-obavještajnih agencija*) (2011), Summary of work report for 2010 (*Sažetak Izvješća O Radu Za 2010. Godinu*), Zagreb, March 2011.

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.

Deeks, A. (2016), 'Global Change and Megatrends, Implications for intelligence and its oversight', in: Goldman, Z. and Rascof, S. eds, *Global Intelligence Oversight*, Oxford University Press, Oxford, 2016.

Dietrich, J.-H. and Eiffler, S. (eds) (2017), *Handbuch des Rechts der Nachrichtendienste*, Boorberg Verlag, Stuttgart.

Dreusicke, L. (2017), 'Präsidentin des BGH in Osnabrück: Wer das Ausspähen des BND kontrollieren soll', *Osnabrücker Zeitung*, 27 April 2017.

European Commission (2016), Communication from the Commission to the European Parliament, the European Council and the Council, "Enhancing Security in a world of mobility; improved information exchange in the fight against terrorism and stronger external border", COM(2016)602, Brussels, 14 September 2016.

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, Juncker, J.-C. (2016), 'Juncker after Brussels terror attacks: "We need a Security Union"', Joint Press Conference with French Prime Minister Manuel Valls, 24 March 2016.

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.

Finland, Ministry of Interior (2017), *Civilian Intelligence Legislation, Working Group Report, Ministry of Interior 8/2017 (Siviilitiedustelulainsäädäntö. Työryhmän mietintö, Sisäministeriön julkaisu 8/2017)*, Helsinki, 19 April 2017.

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 (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 (2015a), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Members States' legal framework*, Luxembourg, Publication Office.

FRA (2015b), *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies - Legal update – Guidelines for FRANET,* Vienna, 30 November 2016.

FRA (2017), *Monthly data collection on the current reform of intelligence legislation in Belgium, Finland, France, Germany, the Netherlands, Sweden and the United Kingdom – Guidelines for FRANET*, Vienna, 25 November 2016.

France, Adam, P., Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement, DPR*) (2017), *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2016* (Annual Report 2016), Doc. No. 4573 (Assemblée nationale), Doc. No. 448 (Sénat), Assemblée Nationale and Sénat, 2 March 2017.

France, Défenseur des Droits (2017), *Avis du Défenseur des droits n°17-05*, 7 July 2017.

France, Commission Nationale Consultative des Droits de l'Homme (2015), *Avis sur le projet de loi relatif au renseignement dans sa version enregistrée le 1er avril 2015 à la Présidence de l'Assemblée nationale*, 16 April 2015.

France, Commission Nationale Consultative des Droits de l'Homme (2016), *Avis sur le projet de loi de lutte contre le crime organisé et le terrorisme*, 17 March 2016.

France, Commission Nationale Consultative des Droits de l'Homme (2017a), *Avis sur la loi relative à la sécurité*, 23 February 2017.

France, Commission Nationale Consultative des Droits de l'Homme (2017b), *Avis sur le projet de loi visant à renforcer la sécurité intérieure et la lutte contre le terrorisme*, 6 July 2017.

France, Le Monde, *Jacques Toubon : le projet de loi antiterroriste est « une pilule empoisonnée »*, 22 June 2017.

France, National Commission on Informatics and Liberty (*Commission nationale de l'informatique et des libertés*, CNIL) (2016), *Rapport d'activité 2015*, Paris, La documentation française.

France, CNIL (2015), *Rapport d'activité 2014*, Paris, La documentation française.

France, CNIL (2014), *Rapport d'activité 2013*, Paris, La documentation française.

France, National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement, CNCTR*) (2016), *1er rapport d'activité 2015/2016*, Paris.

France, Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement, DPR*) & National Commission on Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement, CNCTR*) (2017), *Colloque consacré au contrôle et à l'évaluation de la politique publique du renseignement, mercredi 22 mars 2017, projet de compte rendu*, Paris.

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.

Gajdošová, J. (2017), 'Legal redress mechanisms for individuals against intelligence action', in Dietrich/Sule (eds.), *Intelligence Law and Policies in Europe: a handbook*, forthcoming.

Germany, German Institute for Human Rights (*Deutsches Institut für Menschenrechte*) (2016), Menschenrechtliche Anforderungen an die Ausland-Ausland-Fernmeldeaufklärung und ihre Kontrolle, Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages am 26. September 2016.

Germany, Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) (2017), *Activity report on data protection for the years 2015 and 2016 (26. Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016)*, Bonn, Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bonn, 30 May 2017.

Germany, Federal Parliament (*Deutscher Bundestag*) (2016a), *Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Berichtszeitraum November 2013 bis November 2015)*, Drucksache No. 18/7962, 21 March 2016.

Germany, Federal Parliament (*Deutscher Bundestag*) (2016b), *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 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2014),* Drucksache No. 18/7423, 29 January 2016.

Germany, Federal Parliament (*Deutscher Bundestag*) (2017a), *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 G 10 (Berichtszeitraum 1. Januar bis 31. Dezember 2015),* Drucksache No. 18/11227, 16 February 2017.

Germany, Federal Parliament (*Deutscher Bundestag*) (2017b), *Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes – Beschlussempfelung*, Drucksache No. 18/12850, 23 Juni 2017.

Gohin, O. and Latour, X. (eds.) (2016), *Code de la sécurité intérieure 2016*, LexisNexis, Paris.

Greece, Authority for Communication Security and Privacy (*Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών*) (2016), *Activity Report for the year 2015*, State Printing Office.

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.

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

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.

Italy, COPASIR (2015), 'Report on so-called "Butterfly" and "Return" operations and on the affair "Flamia"' ('*Relazione sulle cosiddette operazioni "Farfalla" e "Rientro" e sulla vicenda "Flamia"*'), Rome, 12 March 2015.

Italy, COPASIR (2017), *Relazione annuale (Attività svolta dal 1 gennaio 2016 al 31 dicembre 2016)*, Doc. XXXIV No.4, Senate of the Republic (*Senato della Repubblica*), Chamber of Deputies (*Camera dei Deputati*), 22 February 2017.

King J. (2016), 'Introductory remarks by the Commissioner-designate Sir Julian King to the LIBE Committee', Press release, Strasbourg, 12 September 2016.

Kojm, C. (2016), 'Global Change and Megatrends, Implications for intelligence and its oversight', in: Goldman, Z. and Rascof, S. eds, *Global Intelligence Oversight*, Oxford University Press, Oxford, 2016.

Korff, D. et al (2017*), Boundaries of Law – Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes – Global Report*, World Web Foundation.

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

Lefebvre, N. (2015), *Les services de renseignement européens face au terrorisme : coopération ou cloisonnement*, Presses Académiques Francophones, Saarbrücken, 2015.

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

Lorenz, P. (2017), 'BND-Kontrolle am BHG: Unabhängiges Gremium nimmt Arbeit auf', *Legal Tribune Online*, 9 March 2017.

Luxembourg, Commission (*autorité de contrôle*) of the Criminal Investigation Code (Code d'Instruction Criminelle) (2016), *Report of the execution of the commission's mission during the years 2014 and 2015 (Rapport rendant compte de l'exécution de la mission de l'autorité de contrôle pendant les années 2014 et 2015)*, Luxembourg, 16 March 2016.

Luxembourg, Commission Nationale la Protection des Données (CNPD) (2016), *Rapport Annuel 2015,* 13 June 2016.

Mills, A. and Sarikakis, K. (2017), 'Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism', Big Data & Society, July – December 2016.

Omand, D. (2014), 'The future of intelligence. What are the threats, the challenges and the opportunities?', in Duyvesteyn, I., de Jong, B., van Reijn, J. eds, *The Future of Intelligence, Challenges in the 21st century*, London and New York, Routledge, 2014.

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 (2015), *Improving the protection of whistleblowers*, Report Doc. 13791, Strasbourg, 6 June 2015.

Palacios, J.-M. (2016), 'L'expérience d l'Intcen européen : un concept commun du renseignement pour une communauté culturellement diverse' in Laurent, S.-Y. and Warusfel, B. (1st ed), *Transformations et Réformes de la sécurité et du renseignement en Europe*, Presses Universitaires de Bordeaux, p. 297.

Peers, S. (2016), *EU Justice and Home Affairs Law, Volume II: EU Criminal Law, Policing and Civil Law* (4th ed), Oxford, Oxford University Press.

Ranking Digital Rights (2017), *2017 Corporate Accountability Index*, Washington DC, Ranking Digital Rights.

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

Singer, J. (2016), *Praxiskommentar zum Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes*, Springer-Verlag, Berlin Heidelberg.

Sule, S. (2006), *Spionage – Völkerrechtlich, nationalrechtliche und europarechtliche Bewertung staatlicher Spionagehandlungen unter besonderer Berücksichtigung der Wirtschaftsspionage*, Nomos, Baden-Baden.

Sule, S. (2017), 'EU law restraints on Intelligence Activities in view of National Security' in: Dietrich, J.-H. and Sule S. (1st ed.), *Intelligence Law and Policies in Europe: A Handbook*, Oxford, C.H. Beck, Hart, Nomos (*forthcoming*)

Sweden, Swedish Parliament (2007), Parliamentary communication (Riksdagsskrivelse 2007/08:266) on the Government Bill "Adaptation of Defence Intelligence Activities" *(Proposition 2006/07:63, En anpassad försvarsunderrättelseverkamhet*), 8 March 2007.

Sweden, State Defence Intelligence Commission (*Statens inspektion för försvarsunderrättelseverksamheten*, SIUN) (2017), *Annual Report 2016 (Årsredovisning och årsberättelse 2016)*, Stockholm, 21 February 2017.

Sweden, National Defence Radio Establishment (*Försvarets radioanstalt*) (2016), Article about the Swedish Foreign Intelligence Inspectorate's review of the National Defence Radio Establishment (*Artikel I DN om SIUN-granskning av FRA*), 12 December 2016.

Sweden, State Official Reports (*Statens Offentliga Utredningar*) (2016), *The general responsibility of the supervision of private life (Ett samlat ansvar för tillsyn över den personliga integriteten)*, Stockholm 2016.

Töpfer, E. (2013), *Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei,* Berlin: Deutsches Institut für Menschenrechte (Policy Paper, 21).

The Netherlands, General States (*Staten-Generaal*) (2017), Parliamentary Document 34588, Nr. 67, 2 May 2017.

The Netherlands, National Government (*Rijksoverheid*) (2016), Infographic about AIVD and MIVD's method of interception of information (*'Gemoderniseerde Wet op de inlichtingen- en veiligheidsdiensten: extra bescherming veiligheid én privacy'*), Press Release 28 October 2016.

The Netherlands, Review Committee on the intelligence and Security Services (CTIVD) (2009), Review Report no. 22A *on the cooperation of the GISS with foreign intelligence and/or security services,* The Hague, 12 August 2009.

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

The Netherlands, CTIVD (2012), Monitoring Report No. 33 (*Toezichtsrapport CTIVD, nr. 33 inzake de rubricering van staatsgeheimen door de AIVD*), The Hague, 13 June 2012.

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

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

The Netherlands, CTIVD (2016a), *Annual Report 2015*, The Hague, 7 June 2016.

The Netherlands, CTIVD (2016b), *on the implementation of cooperation criteria by the AIVD and the MIVD*, The Hague, 4 May 2016.

The Netherlands, CTIVD (2016c), *The CTIVD's View on the ISS Act 20.. Bill*, November 2016.

The Netherlands, CTIVD (2016d), *Review report No. 49 on the exchange of unevaluated data by the AIVD and the MIVD, May 2016*.

The Netherlands, CTIVD (2017), *Annual Report 2016*, The Hague, 24 July 2017.

Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*)(2016), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page.

United Kingdom, Home Office (2015), 'Code of Practice of Acquisition and Disclosure of Communications Data', March 2015.

United Kingdom, Home Office (2017), 'Interception of communications: draft code of practice', 23 February 2017.

United Kingdom, House of Commons Library (2017), Intelligence and Security Committee, Briefing Paper, No. 02178, 14 June 2017.

United Kingdom, House of Lords (2016), Transcripts of debate on Investigatory Powers Bill, 17 October 2016.

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

United Kingdom, ISC (2016), *Annual Report 2015-16,* London, 5 July 2016.

United Kingdom, ISC (2016), *Report on the draft Investigatory Powers Bill*, London, 9 February 2016.

United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2017), *Statement on work completed since July 2016*, London, 27 April 2017.

United Kingdom, Intelligence Services Commissioner (2016), *Report of the Intelligence Services Commissioner for 2015*, No. HC 459 SG/2016/96, London, July 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2014), *Annual Report of the interception of communications commissioner (covering the period of January to December 2013)*, No. HC 1184 SG/201425, London, April 2014.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016a), *Annual Report for 2015 (covering the period January to December 2015)*, No. HC 255 SG/2016/68, London, September 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016b), *Review of directions given under section 94 of the Telecommunications Act 1984*, No. HC 33 SG/2016/67, London, July 2016.

United Kingdom, Interception of Communications Commissioner (IOCCO) (2016c), *IOCCO Points to Consider on the Investigatory Powers Bill* (*IP Bill*), London, 23 March 2016.

United Kingdom, IPT (2016), *Investigatory Powers Tribunal Report 2011 – 2015*.

United Kingdom, Ministry of Justice (2014), *'Memorandum of understanding on National Security Cases (DPA)'*, 2 September 2013.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 (2014a) Resolution on the Right to Privacy in the digital age, Doc. A/RES/69/166, 18 December 2014.

UN, GA (2014b), 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, GA (2016a), Resolution on the Right to Privacy in the digital age, Doc. A/C.3/71/L.39/Rev.1, 16 November 2016.

UN, GA (2016b), Resolution adopted by the General Assembly on 1 July 2016: The United Nations Global Counter-Terrorism Strategy Review, Resolution A/RES/70/291, 19 July 2016.

UN, GA (2016c), Resolution on the right to privacy in the digital age, Doc. A/RES/71/199, 19 December 2016.

UN, GA (2016d), Report of the Special Rapporteur on the right to privacy, Cannataci, J., Doc. A/71/368, 30 August 2016.

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 (2015), Concluding observations on the fifth periodic report of France, CCPR/C/FRA/CO/5, 21 July 2015.

UN, Human Rights Council (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, Scheinin, M.*, Doc. A/HRC/10/3, 4 February 2009.

UN, Human Rights Council (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, Scheinin, M.*, Doc. A/HRC/14/46, 17 May 2010.

UN, Human Rights Council (2014), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Emmerson, B.*, Doc. A/69/397, 23 September 2014.

UN, Human Rights Council (2016), Resolution on the safety of journalists, Doc. A/HRC/33/L.6, 26 September 2016.

UN, Human Rights Council (2016), *Report of the Special Rapporteur on the right to privacy, Cannataci, J.*, Doc. A/HRC/31/64, 24 November 2016.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Emmerson, B.*, Doc. A/HRC/34/61, 21 February 2017.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the right to privacy, Cannataci, J.*, Doc. A/HRC/34/60, 24 February 2017.

UN, Human Rights Council (2017), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Kaye, D., Doc. A/HRC/35/22, 30 March 2017.

UN, Human Rights Council (2017), *Resolution on the right to privacy in the digital age*, Doc. A/HRC/RES/34/7, 7 April 2017.

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.

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 Walle, G. (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.

Wetzling, T., Stiftung neue Verantwortung (2017), 'Germany's intelligence reform: More surveillance, modest restraints and inefficient controls'.

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.

Working Group on Data Protection in Telecommunications (2017), *Towards International Principles or Instruments to Govern Intelligence Gathering*, Working Paper of the 61st Meeting, 24-25 April 2017, Washington D.C., USA.

Indexes

Case law index

Court of Justice of the European Union

European Court of Human Rights

National courts

Legal instruments index

EU legislation

CoE legislation

National legislation

Annex 1: Data collection and coverage

Legal update in EU 28

The legal analysis 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.[568] The main data collection took place between August 2014 and September 2016. Later on, the selected Member States provided FRA with a series of monthly overviews. Franet contractors provided their latest deliverables in June 2017.

Additional information was gathered through desk research and exchanges with key partners, including a number of FRA's national liaison officers and individual experts in various Member States. These include Austria, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Romania, Sweden and the United Kingdom. The opinions and conclusions in this report do not necessarily represent the views of the organisations or individuals who helped develop the report.

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.[569] 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.[570] Additional promising practices discussed during fieldwork are published in this report.

The legal comparative analysis 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 private life – in other words, whether the secret surveillance was "in accordance with the law". Following the ECtHR jurisprudence, this report presents the safeguards that the law should put in place to be considered compatible with the ECHR.[571] These relate to the approval mechanism of the surveillance measure and the oversight mechanism controlling its implementation, as well as to available remedies.

568 See FRA (2014b), FRA (2015b) and FRA (2017). See all Franet Guidelines online.
569 See, for example, Venice Commission (2007); Council of Europe (2016b); Born, H. and Wills, A. (eds.) (2012); Hans Born, H., Leigh I. and Wills, A. (2015); Anderson, A. (2015).
570 UN, Human Rights Council, Scheinin, M. (2010).
571 See Cameron, I. (2013), p. 164.

Social fieldwork methodology

Research Member States

The social fieldwork is based on qualitative research in the following seven EU Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom.

The selection of the Member States was determined by a set of interrelated factors. In the 2015 report *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, FRA presented the findings of the mapping of the legal frameworks in the EU Member States that regulate surveillance by intelligence services and their oversight. The report presented an overview of the institutions and bodies that operate in the field, discussing their different types, mandates and powers. On the basis of the findings of this institutional approach, the Member State selection for the fieldwork stage aimed to capture the variety of actors involved in the field of surveillance by the intelligence services and its oversight and to cover the whole range of different powers, mandates and national constellations of main actors in certain Member States. In line with this main ground, five out of the seven Member States have detailed legislation on general surveillance of communications. The size of the country played a role in this context in terms of institutions available, their number and staff working in the institutions, their openness and availability to discuss the issues.

Objectives

The objective of the field research was to provide FRA with country-specific information on the practical implementation of the national legal frameworks governing the intelligence services with respect to compliance with fundamental rights. The research aimed to study how the oversight of intelligence services was exercised in practice, to analyse the specificities of the day-to-day work of the oversight bodies and their effectiveness in the selected Member States. It thus has both exploratory and explanatory aspects. The research did not cover surveillance techniques or the content of the data collected.

The analysis of the data collected aims to identify cross-cutting and overarching issues that can be extrapolated to other EU Member States and discussed within their national context. The data collected and the findings are not used to provide country-specific reports or to

'check' the issues identified by the respondents with regard to their specific national contexts.

The methodology applied to the social research aims to identify prevailing understandings of and opinions about the legal framework that currently regulates oversight of intelligence gathering – a task that is shared by different actors in the field, such as different types of oversight bodies, data protection authorities, ombuds institutions, national human rights institutions, civil society organisations, practicing lawyers, academics and media representatives. The data collected provide insights into, and broader understanding of, the challenges of upholding fundamental rights in the area of oversight. It also provides an assessment of applied oversight practices and remedies from the perspective of different actors involved.

Data collection

The main data collection was carried out from December 2015 to July 2016, with a few interviews conducted in the late autumn of 2016. The final data set consists of 72 interviews in the selected EU Member States (see Table 1).

Table 1: Interviews by Member State

Member State	Number of interviews
Belgium	8
Germany	8
France	17
Italy	5
The Netherlands	8
Sweden	14
The United Kingdom	12
Total	**72**

Source: FRA, 2017

Table 2 presents a breakdown of the interviews by the institutions and bodies. The interviews with the representatives of the oversight bodies comprise the biggest share in the dataset (nearly half of the interviews). Both the type of institution approached and number of the interviews per Member State depended on the national context.

In the context of this research, the interviewees were addressed as individuals with special knowledge on intelligence, surveillance, oversight and related matters. The focus was on collecting the experts' process-related knowledge on gathering intelligence in accordance with existing fundamental rights standards.

Table 2: Interviews, by institution represented

Institution/organisation	Number of interviews
Expert body	16
Parliamentary committee	8
Executive control	4
Judiciary	6
Data protection authority	11
Ombuds institution, national human rights institution	5
Civil society organisation (including media representatives)	12
Academia	5
Lawyer	5
Total	**72**

Source: FRA, 2017

All potential interviewees were contacted with official FRA letters, as representatives of a specific public authority, body or organisation. In the communication, strict anonymity and confidentiality of the interviews were agreed on. Where quotes or statements from the interviews are used in publications, FRA committed to using no reference or using a generalised reference to avoid enabling personal identification.

FRA expressed its interest in interviewing separately the head of the institution and the staff (or member of the body) with relevant responsibilities that cover the areas of the research interest. In the final outcome, the respondents are distributed equally by their positions in the institutions, i.e., the final sample includes interviews with the heads (chairs, directors, presidents) of the authorities and the responsible staff in equal shares (22 interviews per each category). This breakdown was not applied for lawyers, academia and civil society organisations, where the same person might represent both positions. During most interviews, two respondents participated (in a few cases, more than two respondents were present, and the highest number of interviewees per interview was six). With regard to gender, in more than half of the interviews (44 out of 72), only men were present. In 15 cases, only women were present as interviewees. In the remaining 13 cases, both men and women were present during the interviews.

In the framework of the research, civil society organisations that have expertise in the area of data protection and surveillance specifically were approached. Such organisations were available in all the researched Member States except for Italy. In selecting the organisations, their experience on the international level was taken into account. The scale and scope of the activities vary among the civil society organisations and

across countries. Some have been operating for several decades, and some for several years. With regard to their background, mainly lawyers are active or work in the civil society organisations. Their legal expertise in some cases is supported by technical experts, or certain knowledge is developed through the involvement in the activity field. Many of these organisations have been involved in litigation on a variety of issues related to data protection or privacy, including cases on alleged unlawful data processing by intelligence agencies.

All the interviews were carried out by senior FRA research staff members, who travelled to the selected Member States. Most interviews were conducted face to face, with a few undertaken by telephone to suit the needs of the interviewee(s) and the researchers (ie, to find a time slot in the agendas and to reduce travelling).

On average, interviews lasted about one-and-a-half hours. Most of the interviewees kindly agreed to the interviews being audio recorded. When recording was not possible, notes were taken during the interview. For this reason, two FRA representatives were present during the interviews.

Most of the interviews took place in the respective national languages of the countries. FRA staff translated the anonymised transcripts and notes of the interviews from Italian and Swedish to English. The *Translation Centre for the Bodies of the European Union* translated the anonymised transcripts and notes of the interviews from French and German to English. The information retained its classified status, with a security grading 'confidential' assigned.

Interview content

The semi-structured interviews were designed to obtain detailed accounts of the following issues:

- assessment of the institutional setting of the authority, its mandate, power, and legal framework and its latest developments;
- implementation of oversight in practice, scope and content of oversight processes, including measures to ensure that intelligence gathering is compliant with fundamental rights;
- assessment of remedial mechanisms for individuals in case of fundamental rights violations;
- needs for reform, possible improvements in daily activities to ensure the fundamental rights compliance of the intelligence services and its oversight.

Interview guidelines followed the same structure of mainly open questions that were used to set an agenda, with the freedom to change the order of questions depending on the answers. The pre-defined structure contributed to capturing the perspectives and opinions of different actors involved about the same issues, with some adjustments in relation to the specificity of the experiences.

The sequence of the questions and the topics covered during each interview differed across different institutions, taking into account their relevance (including recent developments in the Member State, the institution's powers and competences, etc.). Therefore, there are differences in the nature and volume of information obtained from different respondents, which might lead to varying levels of consistency in the conclusions or findings on specific themes due to the volume of information. Overview of oversight operational practices, which was discussed only during 16 interviews, is an example. Although the discussions provided valuable in-depth information on, and explanations and understanding of, the procedures carried out by the oversight bodies, the analysis, generalisation and presentation of the data are limited due to the specificity of each institution, Member State context, and confidentiality issues. They mainly provide background information. For most cases, the main focus was on identifying trends in the data, i.e. looking for and combining statements and opinions that were similar or identical across different research participants. Table 3 provides a list of themes presented in the report and the number of interviews that covered them.

Data analysis

The analysis of the data collected through the semi-structured interviews was carried out by using the qualitative data analysis software 'NVivo 10'. The data analysis was constructed around the main topics and questions asked, following the interview guideline, and the key findings from the legal analysis of the 28 EU Member States. No interview or response to a specific question was considered on its own. Constant comparison of the data that went through automated and manual coding (categorising data on the basis of similarity, repetitiveness of the observations, concepts, topics and issues raised) enabled the researchers to identify emerging themes and opinions. The findings from the fieldwork contribute to understanding different aspects of intelligence collection and its oversight; it does not aim to validate the legal analysis results.

In the data analysis process, an inductive approach was mainly applied, which aimed to generate new information from the data (raw interview text data), explore the research subject matter from a different/new perspective (along the legal analysis), and establish (develop) understanding of the underlying opinions and views that are evident in the raw data collected

Table 3: Thematic areas presented in the report, by number of interviews

Theme	Number of interviews during which issue was discussed
Legal framework	67
Clarity of legal framework	53
Effective oversight	35
Mandate of the body	33
Independence of the body	16
Transparency of the oversight activities	29
Main challenges to upholding fundamental rights	38
Definition of national security	15
Resources and technical capacities	64
Oversight institutional framework	60
Cooperation with other institutions	46
Remedies	54
Duty of notification, right to access information	17
Whistle-blowers	14

Source: FRA, 2017

for this report. However, this approach does not make it possible to explain the causality of the issues and provide grounded explanations; instead, it provides a 'straightforward' approach for deriving findings in the context of interview guiding questions (namely, it condenses extensive and varied raw interview data through recurrent and most relevant themes or categories into a brief, summary format). Also, this type of qualitative research is based on the interviewees' opinions and judgments rather than factual results.

While looking for relationships and patterns in the data, the type of institution or organisation that the respondents represented was used as the main breakdown dimension. Other possible characteristics, such as country, position within the institution, or any other specific information, was considered with a particular focus only during the analysis process but disregarded while finalising the results and presenting the findings.

Presentation of the findings

The findings from the fieldwork complement the conclusions of the comparative national legal analysis and follow up on specific issues identified during the data collection or in earlier FRA reports. The analysis of the interview data is influenced by the content of, and language used during, the interviews. Therefore, the terminology used in the discussion of the findings predominantly originates from the respondents and is not necessarily closely connected to the legislative regulation (ie, does not follow the text of the regulation). It is worth mentioning that, during the interviews, respondents attempted to explain the complexity of their day-to-day practices and procedures in an understandable way.

The quotes included in the text of the report have been selected for being particularly illustrative or representative of the research findings. They primarily serve illustrative purposes. Only translated quotes are presented. They have been slightly edited, but only to improve understanding and readability. All the interviews were carried out in confidence; references to the interviewees are therefore kept general. In most cases, the category specified next to the quote refers to the body represented, e.g. expert body, parliamentary committee, data protection authority or civil society organisation, etc. Where interviewed individual experts hold an academic position or are practicing lawyers, broader categories are applied – such as 'academia' or 'lawyer'. The presentation of the findings does not aim to single out a specific country, so the countries are mentioned in the text where relevant, but are not specified alongside the quotes. Before publication of the report, all respondents consented to being cited in the way the citations and references are presented in the report.

Annex 2: Overview of intelligence services in the 28 EU Member States

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
AT	Federal Agency for State Protection and Counter Terrorism/*Bundesamt für Verfassungsschutz und Terrorismusbekämpfung* (BVT) (part of the police)	http://www.bmi.gv.at/cms/bmi_verfassungsschutz/meldestelle/	N.A.	Annual report 2016 (87 pages)
	Military Intelligence Service/*Heeresnachrichtenamt* (HNA)	http://www.bundesheer.at/organisation/beitraege/n_dienste/index.shtml	N.A.	-
	Military Defence Agency/ *Heeresabwehramt* (HAA)	-	N.A.	-
BE	State Security/ *Staatsveiligheid /Sûreté de l'Etat* (SV/SE)	-	N.A.	-
	General Information and Security Service/ Algemene Dienst Inlichting en Veiligheid / Service Général du Renseignement et de la Sécurité (ADIV/SGRS)	-	N.A.	-
BG	State Intelligence Agency/*Nationalna Razuznavatelna Služba* (NRS)	www.nrs.bg	N.A.	Annual Report 2016 (18 pages)
	State Agency for National Security / Държавна Агенция "Национална сигурност (SANS)	http://www.dans.bg/index.php	N.A.	Access to information Report 2016 (1 page)
	State agency "Technical operations" / Държавна агенция „Технически операции (SATO)	https://www.dato.bg/	N.A.	Access to information Report 2016 (1 page)
	Military Information Service/*Sluzhba Voenna Informatsia*	http://dis.mod.bg/	N.A.	-
CY	Cypriot Intelligence Service/Κυπριακή Υπηρεσία Πληροφοριών (ΚΥΠ)	-	N.A.	-
CZ	Security Information Service/*Bezpečnostní informační služba* (BIS)	https://www.bis.cz/	N.A.	Annual Report 2015 (26 pages)
	Office for Foreign Relations and Information/ Úřad pro Zahraniční Styky a Informace (UZSI)	www.uzsi.cz	N.A.	-
	Military Intelligence/*Vojenské Zpravodajství*	http://www.vzcr.cz/	N.A.	Annual Activities Report 2015 (19 pages)
DE	Federal Office for the protection of the Constitution/ *Bundesamt für Verfassungsschutz* (BfV)	https://www.verfassungsschutz.de/en/index-en.html	2,813	Annual Report 2016 (38 pages)
	Federal Intelligence Service/*Bundesnachrichtendienst* (BND)	www.bnd.bund.de	circa 6,500	Not publicly available
	Military Counter-Intelligence Service/ *Militärischer Abschirmdienst* (MAD)	http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/start/weitdstst/mad	1,086	-
	State Office for the Protection of the Constitution of *Baden-Württemberg*/ Landesamt für Verfassungsschutz Baden-Württemberg	http://www.verfassungsschutz-bw.de/,Lde/Startseite	N.A.	Annual Report 2016 (181 pages)
	Bavarian Office for Protection of the Constitution/ *Bayerische Landesamt für Verfassungsschutz*	http://www.verfassungsschutz.bayern.de/	N.A.	Report for first half of 2017 (47 pages)
	Berlin Senate Administration for Home Affairs, Department of Protection of Constitution/*Senatsverwaltung für Inneres, Abteilung Verfassungsschutz Berlin*	https://www.berlin.de/sen/inneres/verfassungsschutz/	N.A.	Annual Report 2016 (221 pages)
	Brandenburg Ministry of Interior and Municipalities, Department of Protection of Constitution/*Ministerium des Innern und für Kommunales, Abteilung Verfassungsschutz Bradenburg*	http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/lbm1.c.336855.de	N.A.	Annual Report 2015 (344 pages)

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
DE	Bremen State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Bremen*	http://www.verfassungsschutz.bremen.de/	N.A.	Annual Report 2016 (97 pages)
	State Office for the Protection of Constitution of the Free and Hanseatic City of Hamburg/*Landesamt für Verfassungsschutz der Freien und Hansestadt Hamburg*	-	N.A.	Annual Report 2015 (244 pages)
	Hessen State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Hessen*	https://lfv.hessen.de/	N.A.	Annual Report 2015 (244 pages)
	Lower Saxony Ministry of Interior, Sport and Integration, Department 5/*Ministerium für Inneres, Sport und Integration, Abteilung 5 Niedersachsen*	https://www.verfassungsschutz.niedersachsen.de/startseite/	N.A.	Annual Report 2016 (401 pages)
	Mecklenburg-Vorpommern Ministry of Interior, Department II 5/*Mecklenburg-Vorpommern Innenministerium, Abteilung II 5*	http://www.verfassungsschutz-mv.de/	N.A.	Annual Report 2015 (194 pages)
	North Rhine-Westphalia Ministry of Interior and Municipalities, Department for the Protection of Constitution/*Nordrhein-Westfalen Ministerium für Inneres und Kommunales, Abteilung Verfassungsschutz*	http://www.mik.nrw.de/verfassungsschutz/aktuelles.html	N.A.	Annual Report 2015 (263 pages)
	Rhineland-Palatinate Ministry of Interior and Sport, Department for the Protection of Constitution/*Rheinland-Pfalz Ministerium des Innern und für Sport, Abteilung Verfassungsschutz*	https://mdi.rlp.de/de/unsere-themen/sicherheit/verfassungsschutz	N.A.	Annual Report 2016 (119 pages)
	Saarland State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Saarland*	http://www.saarland.de/verfassungsschutz.htm	N.A.	Annual Report 2016 (90 pages)
	Saxony State Office for the Protection of Constitution/*Landesamt für Verfassungsschutz Sachsen*	http://www.verfassungsschutz.sachsen.de/index.html	N.A.	Annual report 2016 (420 pages)
	Saxony-Anhalt Ministry of Interior and Sport, Department for the Protection of Constitution/*Sachsen-Anhalt Ministerium für Inneres und Sport, Abteilung Verfassungsschutz*	https://mi.sachsen-anhalt.de/verfassungsschutz/	N.A.	Annual Report 2016 (224 pages)
	Schleswig-Holstein Ministry of Interior, Department for the Protection of Constitution/*Schleswig-Holstein Innenministerium, Abteilung Verfassungsschutz*	http://www.schleswig-holstein.de/DE/Themen/V/verfassungsschutz.html	N.A.	Annual Report 2016 (172 pages)
	Thüringen Ministry of Interior and Municipalities, Office for the Protection of Constitution /*Thüringen Ministerium für Inneres und Kommunales, Amt für Verfassungsschutz*	http://www.thueringen.de/th3/verfassungsschutz/	N.A.	Report 2014/15 (232 pages)
DK	Danish Defence Intelligence Service/*Forsvarets Efterretningstjenst* (FE)	www.fe-ddis.dk	N.A.	Report 2015/16 (30 pages)
	Danish Security and Intelligence Service/*Politiets Efterretningstjeneste* (PET) (part of the police)	https://pet.dk/	N.A.	Annual Report 2015 (28 pages)
EE	Information Board/*Teabeamet* (TA)	https://www.teabeamet.ee/	N.A.	Estonia's International Security Environment 2017 (44 pages)
	Estonian Internal Security Service/*Kaitsepolitseiamet* (KAPO)	https://www.kapo.ee/	N.A.	Yearbook 2016 (45 pages)
	Intelligence Battalion of the Estonian Defence Forces /*Kaitseväe peastaabi luureosakond*	-	N.A.	-
EL	National Intelligence Service/Εθνική Υπηρεσία Πληροφοριών (EYP)	www.nis.gr	N.A.	-
	Directorate of Military Intelligence of the National Defence General Staff/Διεύθυνση Στρατιωτικών Πληροφοριών του Γενικού Επιτελείου Εθνικής Άμυνας	-	N.A.	-

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
ES	National Intelligence Centre/*Centro Nacional de Inteligencia* (CNI)	https://www.cni.es/	N.A.	-
	Intelligence Centre of the Armed Forces/ *Centro de Inteligencia de las Fuerzas Armadas* (CIFAS)	http://www.emad.mde.es/CIFAS/	N.A.	-
FI	Finnish Defence Intelligence Agency/ *Tiedustelulaitos* (FDIA)	http://puolustusvoimat.fi/en/about-us/finnish-defence-intelligence-agency	N.A.	-
	Finnish Security Intelligence Service/ *Suojelupoliisi/Skyddspolisen* (SUPO)	http://www.supo.fi/	N.A.	Yearbook 2016 (28 pages)
FR	Directorate General of External Security/ *Direction Générale de la Sécurité Exterieure* (DGSE)	http://www.defense.gouv.fr/dgse	5,376*	-
	Directorate of Defence Intelligence and Security/*Direction du renseignement et de la sécurité de la défense* (DRSD)	http://www.defense.gouv.fr/drsd	1,190*	-
	Directorate of Military Intelligence/ *Direction du renseignement militaire* (DRM)	http://www.defense.gouv.fr/ema/directions-et-services/la-direction-du-renseignement-militaire/la-drm	1,715*	-
	Directorate General of Interior Security/ *Direction générale de la sécurité intérieure* (DGSI)	http://www.interieur.gouv.fr/Le-ministere/DGSI	3,200**	-
	National Directorate of customs intelligence and investigations/*Direction nationale du renseignement et des enquêtes douanières (DNRED)*	http://www.douane.gouv.fr/	760*	Results 2016 (50 pages)
	Service du traitement du renseignement et action contre les circuits financiers clandestins (Tracfin)	http://www.economie.gouv.fr/tracfin/accueil-tracfin	132*	Annual Activities Report 2016 (87 pages)
HR	Security Intelligence Agency/*Sigurnosna-Obavjestanja Agencija* (SOA)	https://www.soa.hr/	N.A.	Public Report 2016 (49 pages)
	Military */Vojna Sigurnosna-Obavjestanja Agencija* (VSOA)	-	N.A.	-
HU	Information Office/ *Informacios Hivatal* (MKIH)	http://www.mkih.hu/	N.A.	-
	Constitution Protection Office/ *Alkotmányvédelmi Hivatal*	http://www.ah.gov.hu/	N.A.	-
	Special Service for National Security/ *Nemzetbiztonsági Szakszolgálat* (NBSZ)	http://nbsz.gov.hu/	N.A.	-
	Counter Terrorism Centre/ *Terrorelhárítási Központ* (TEK) (service belonging to the police)	http://tek.gov.hu/	N.A.	-
	Counter-Terrorism Information and Criminal Analysis Centre/ *Terrorelhárítási Információs és Bűnügyi Elemző Központ* (TIBEK) (starting from 17 July 2016)	http://tibek.gov.hu/	N.A.	-
	Military National Security Service/*Katonai Nemzetbiztonsági Szolgála* (KNBSZ)	http://knbsz.gov.hu/hu/index.html	N.A.	National Security Review 2016 (127 pages)
IE	Directorate of Intelligence (G2)	-	N.A.	-
	Garda Síochána National Surveillance Unit (NSU) (belonging to the police)	-	N.A.	-
IT	Information and Internal Security Agency/ *Agenzia informazioni e sicurezza interna* (AISI)	http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html	N.A.	Common Activity report for AISI and AISE 2016 (128 pages)
	Information and External Security Agency/ *Agenzia informazioni e sicurezza esterna* (AISE)	http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html	N.A.	
	Department of information and security/ *Reparto informazioni e sicurezza* (RIS)	https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html	N.A.	-

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
LT	State Security Department/ *Valstybes Saugumo Departamentas* (VSD)	http://www.vsd.lt/	N.A.	Annual Activity Report 2016 (15 pages)
	Second Investigation Department under the Ministry of National Defence/*Antraisi Departamentas Prie Krasto Apsaugos Ministerijos*	https://kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html	N.A.	Annual Activity Report 2016 (9 pages)
LU	State Intelligence Service/*Service de Renseignements de l'Etat* (SREL)	http://www.gouvernement.lu/971456/service-de-renseignement-de-l-etat	N.A.	-
LV	Constitutional Protection Bureau/ *Satversmes Aizsardzibas Birojs* (SAB)	http://www.sab.gov.lv/	N.A.	-
	Defence Intelligence and Security Service/ *Militārās izlūkošanas un drošības dienests* (MIDD)	http://www.midd.gov.lv/Par_mums.aspx	N.A.	-
	Security Police/ *Drošības policija*	http://www.dp.gov.lv/lv/	N.A.	Annual Report 2016 (36 pages)
MT	Security Service / *Servizz tas-Sigurtà*	-	N.A.	-
NL	General Intelligence and Security Service/ *Algemene Inlichtingen- en Veiligheidsdienst* (AIVD)	https://www.aivd.nl/	circa 1,500	Annual report 2016 (19 pages)
	Military Intelligence and Security Service/ *Militaire Inlichtingen- en Veiligheidsdienst* (MIVD)	https://www.defensie.nl/organisatie/bestuursstaf/inhoud/eenheden/mivd	795	Annual Report 2016 (50 pages)
PL	Foreign Intelligence Authority/*Agencja Wywiadu* (AW)	http://www.aw.gov.pl/	N.A.	-
	Military Counter-intelligence Service/ *Sluzba Wywiadu Woyskowego* (SWW)	http://www.sww.wp.mil.pl/pl/index.html	N.A.	-
	Internal Security Agency/*Agencja Bezpieczeństwa Wewnętrznego* (ABW)	https://www.abw.gov.pl/	N.A.	Internal Security Review 2017 (compliltion of articles)
	Central Anti–Corruption Bureau/*Centralne Biuro Antykorupcyjne* (CBA)	https://cba.gov.pl/	N.A.	-
PT	Strategic Intelligence and Defence Service/ *Serviço de Informações Estratégicas de Defesa* (SIED)	https://www.sied.pt/	N.A.	-
	Service of Security Intelligence/ *Serviço de Informações de Segurança* (SIS)	https://www.sis.pt/quem-somos/o-sis	N.A.	-
	Information System of the Portuguese Republic/Sistema *de Informações da República Portuguesa* (SIRP)	https://www.sirp.pt/	N.A.	'Year in Review' 2015 (38 pages)
RO	External Intelligence Service/*Serviciul de Informatii Externe* (SIE)	https://www.sie.ro/	N.A.	-
	Defence General Directorate for Information/*Direcția Generală de Informații a Apărării* (DGIA)	http://www.mapn.ro/structuri/dgia/	N.A.	-
	Romanian Intelligence Service/ *Serviciul Roman de Informatii* (SRI)	https://www.sri.ro/	N.A.	Annual Activity Report 2016 (2 pages)
	Department for Information and Internal Protection/ *Direcția Generală de Informații și Protecție Internă* (DGIPI)	http://dgpi.ro/	N.A.	Work started in June 2017
SE	National Defence Radio Establishment/ *Försvarets Radioanstalt* (FRA)	http://www.fra.se/	700	Annual Report 2016 (28 pages)
	Military Intelligence and Security Agency/ *Militära underrättelse- och säkerhetstjänsten*	http://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/	886	Annual Report 2015 (17 pages)
	Security Service/ Säkerhetspolisen, (SÄPO)	http://www.sakerhetspolisen.se/	1,100	Annual Report 2016 (71 pages)

EU MS	Security/Intelligence Service	Website	Number of staff (number publicly available)	Annual Activity reports publicly available (length in total page numbers)
SI	Slovene Intelligence and Security Agency/ *Slovenska obveščevalno-varnostna agencija* (SOVA)	http://www.sova.gov.si/	N.A.	-
	Intelligence and Security Service of the Ministry of Defence/ *Obveščevalno-varnostna služba Ministrstva Republike Slovenije za obrambo* (OVS MORS)	-	N.A.	-
SK	National Security Authority/*Národný bezpečnostný úrad* (NBÚ)	http://www.nbusr.sk/	N.A.	Activity report 2016 (23 pages)
	Slovak Information Service/*Slovenská informačná služba* (SIS)	http://www.sis.gov.sk/	N.A.	Activity report 2016 (18 pages)
	Millitary Intelligence/*Vojenské spravodajstvo* (VS)	http://vs.mosr.sk/	N.A.	Activity report 2016 (9 pages)
UK	Security Service or MI5	https://www.mi5.gov.uk/	4,037	-
	Secret Intelligence Service (SIS) or MI6	https://www.sis.gov.uk/	2,479	-
	Government Communications Headquarters (GCHQ)	https://www.gchq.gov.uk/	5,564	-
	Defence Intelligence (DI)	https://www.gov.uk/government/groups/defence-intelligence	3,697	-

Notes:

N.A. = not available.

– = not applicable (either no website or no public annual report).

** France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 29.*

*** France, website of Académie du renseignement.*

Source: FRA, 2017

Annex 3: Key features of expert oversight bodies' (excl. DPAs) annual reports of selected EU Member States

	Austria* *RSB*	Belgium *Standing Committee I*	Bulgaria *NBKSRS*	Croatia** *Council for Civilian Oversight*	Denmark*** *Defence TET*
Year of publication/reporting period	2016/2015	2016/2015	2017/2016	2011/2010	2017/2016
Length (in pages)	13	131	27	6	44
Available in English and/ or partially in English	✓	✓	-	-	✓
Publication of two versions: one public and one classified	✓	✓	-	✓	-
Description of existing/ new legislation	✓	✓	✓	-	✓
Expert body mandate and powers	✓	✓	-	✓	✓
Surveillance measures	✓	✓	✓	-	✓
Statistics and reasons on authorisations granted/refused	✓	✓	✓	N.A.	
Statistics on *ex post* controls	✓	✓	✓	-	✓
Statistics on investigations	N.A.	✓	✓	✓	
Statistics on breaches of safeguards	-	✓	✓	-	✓
Statistics on surveilled persons	-	-	✓	-	
Oversight methods	✓	✓		✓	✓
International cooperation/data transfer to foreign services	-	✓	-	-	
Remedies and statistics on complaints-handling	-	✓	✓	✓	✓
Internal functioning	-	✓	✓	✓	✓
Inter-institutional dialogue	-	✓	✓	✓	✓
International cooperation among expert bodies	-	✓	✓	-	
Recommendations	-	✓	✓	-	✓
Implementation of past recommendations	-	✓	-	-	✓
Separate publication on specific investigations	-	✓	-	-	

Notes:

N.A. = *not applicable.*

– = *Not done or not covered in the report.*

* *The report of the Legal Protection Commissioner (Rechtsschutzbeauftragter) is confidential, but a summary is published every year in a specialised journal on police studies. See Burgstaller, M. and Kubarth, L. (2016).*

** *The report of the Council for Civilian of Oversight (Vijeće za građanski nadzor sigurnosno-obavještajnih agencija) is submitted to the President of Parliament and is confidential, but a summary is published occasionally.*

*** *Defence TET (Forsvarets Efterretningstjeneste (FE))'s report is available on TET's website.*

**** *The G 10 Commission does not issue any independent reports. Its annual report is prepared by the Parliament Control Panel. See Germany, Federal Parliament (Deutscher Bundestag) (2017).*

Source: *FRA, 2017*

France *CNCTR*	Germany**** *G10*	Greece *ADAE*	Luxembourg *Autorité de contrôle*	Sweden *Siun*	The Netherlands *CTIVD*	United Kingdom *IOCCO / ISComm*
2016/10.2015 to 10.2016	2017/2015	2016/2015	2016/2014-15	2017/2016	2016/1.4 to 31.12.2015	2016/1.9 to 31.12.2015
204	10	79	18	33	40	99 / 71
✓	-	✓	-	-	✓	N.A.
-	-	-	-	-	-	✓
✓	-	N.A.	✓	✓	✓	✓
✓	✓	✓	✓	✓	-	✓
✓	-	-	✓	✓	-	✓
✓	-	N.A.	N.A.	✓	-	✓
✓	N.A.	✓	✓	✓	-	✓
-	N.A.	✓	-	✓	✓	-
-	N.A.	-	-	✓	-	✓
✓	✓	-	-		-	-
✓	-	✓	-	✓	-	✓
-	✓	-	-	✓	-	-
✓	✓	✓	✓	✓	✓	N.A.
✓	-	✓	✓	✓	✓	✓
✓	-	✓	✓	✓	-	✓
✓	-	✓	✓	✓	-	-
✓	-	✓		✓	-	✓
✓	-	-	-	-	-	✓
N.A.	✓	-	-	-	✓	✓

Annex 4: Key features of parliamentary oversight committees' reports, in fieldwork countries with public reports

	Italy *COPASIR*	France *DPR*	Germany *PKGr*	Sweden *Defence Committee*	United Kingdom *ISC*
Date of latest report/reporting period	2017 (covering 2016)	2017 (covering 2016)	2016 on (11.2013 to 11.2015)	2017*	2016 on (09.2015 to 07.2016)**
Obligation to report	✓	✓	✓	✓	✓
Length (in pages)	43	93	14	26	21
Comment on legislation	✓	✓	✓	✓	✓
Parliamentary committee mandate and powers	✓	✓	✓	✓	✓
Parliamentary Committee internal functioning	✓	✓	✓	✓	✓
Number of sessions or hours of work	✓ (59)	✓ (20 sessions - 75 h.)	✓ (32 sessions)	-	✓ (25 sessions)
Number of hearings	✓ (41)	✓ (23)***	-	-	✓ (17)
List of witnesses heard	✓ (28)	✓	✓	-	✓
Content of the hearings	✓	-	-	-	-****
Administration of the Intelligence Services	-	-	-	✓	✓
Expenditure of Intelligence Services	-	✓*****	✓	-	✓******
Policy focus/threats highlighted by the Intelligence Services	✓	✓	✓	✓	✓
Surveillance measures	-	-*******	✓	-	N.A.
Statistics on *ex post* controls	-	-	-	-	N.A.
Statistics on own investigations	✓	-	✓	-	N.A.
Statistics on breaches of safeguards	-	-	-	-	N.A.
Statistics on surveilled persons	-	-	-	-	N.A.
Oversight methods	✓	✓	✓	-	✓
Remedies and statistics on complaints-handling	N.A.	N.A.	✓	-	N.A.
Inter-institutional dialogue	✓	✓	✓	-	✓
Recommendations	-	✓	✓	✓	✓
Ad hoc thematic reports	✓	-	✓	-	✓

Notes: *N.A* = not applicable.
– = not mentioned or not addressed in report.
* The Defence Committee's report is a response to the government's report submitted to parliament, on the use of signals intelligence by the Swedish intelligence services in 2016.
** The ISC's Annual Report covering 2016-17 is ready but not published yet due to the dissolution of the parliament ahead of General Elections in the United Kingdom. A summary of the ISC's work done since July 2016 has been published in a press statement. See United Kingdom, Intelligence and Security Committee of Parliament (2017).
*** Twenty-three hearings, seven interviews/exchanges of views, four visits. See France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 15.
**** The content of all hearings is available on ISC's website under 'Transcripts and Public Evidence'.
***** The DPR is informed annually by the National intelligence coordinator (Coordonateur national au renseignement) about the expenditures of the services. See France, Adam, P., Parliamentary Delegation on Intelligence (2017), p. 22. The control of the special funds is carried out by the Audit Commission on Special Funds (CVFS), which belongs to the DPR.
****** Only the combined budgets of MI5, SIS and GCHQ are presented in ISC's Annual Report. The individual figures for each of the intelligence services have been redacted because they would allow the UK's adversaries to more accurately deduce the scale and focus of the services' activities.
******* The DPR refers to the report by the CNCTR.

Source: *FRA, 2017*

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct information centres.
You can find the address of the centre nearest you at: http://europa.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:
– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696 or
– by email via: http://europa.eu/contact

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications

You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

doi:10.2811/792946 TK-04-17-696-EN-N

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

HELPING TO MAKE FUNDAMENTAL RIGHTS A REALITY FOR EVERYONE IN THE EUROPEAN UNION

With terrorism, cyber-attacks and sophisticated cross-border criminal networks posing growing threats, the work of intelligence services has become more urgent, complex and international. Such work can strongly interfere with fundamental rights, especially privacy and data protection. While continuous technological advances potentially exacerbate the threat of such interference, effective oversight and remedies can curb the potential for abuse.

This report is FRA's second publication addressing a European Parliament request for in-depth research on the impact of surveillance on fundamental rights. It updates FRA's 2015 legal analysis on the topic, and supplements that analysis with field-based insights gained from extensive interviews with diverse experts in intelligence and related fields, including its oversight.

FRA - EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS
Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel. +43 1580 30-0 – Fax +43 1580 30-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Publications Office

ISBN 978-92-9491-765-2