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

Summary

Article 7 of the Charter of Fundamental Rights of the European Union guarantees all individuals in the European Union (EU) the respect for private and family life, while Article 8 guarantees the right to the protection of their personal data. It requires that such data be processed fairly for specific purposes, and secures each person's right of access to his or her personal data, as well as the right to have such data rectified. It also stipulates that an independent authority must regulate compliance with this right. Article 47 secures the right to an effective remedy, including a fair and public hearing within a reasonable timeframe.

When media worldwide began to publish the 'Snowden documents' in June 2013, it brought to light the existence of extensive global surveillance programmes by intelligence services. The Snowden revelations were not the first to hint at programmes of large-scale communication surveillance set-up in the aftermath of the 11 September 2001 attacks. The sheer magnitude of these revelations, however, remains unprecedented, potentially affecting people's privacy around the world. Surveillance no longer merely targets state or business secrets, but allows for the interception of people's communications on a large scale. This interferes both with the respect for private and family life of individuals and with the right to privacy and data protection – both safeguarded at EU level by the Charter of Fundamental Rights of the European Union (the Charter). As such, the EU and its Member States have an obligation to protect these, including in the context of surveillance, and to provide victims with remedies to challenge unlawful surveillance.

"Such mass, indiscriminate surveillance is inherently disproportionate and constitutes an unwarranted interference with the rights guaranteed by Articles 7 and 8 of the Charter."
(CJEU, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, Advocate General's Opinion, 23 September 2015)

The revelations triggered an array of reactions. In the intelligence community, particularly among specialised bodies responsible for overseeing intelligence services, dedicated inquiries and special reports on the Snowden relevations further scrutinised their implications. The EU institutions reacted strongly. The European Commission, the Council of the European Union and the European Parliament all reported on the revelations, expressed concern about mass surveillance programmes, sought clarification from United States' authorities, and worked on "rebuilding trust" in US–EU relations. Although it is too early to assess the full impact of the Snowden revelations, post-Snowden inquiries in some EU Member States concluded that their current national legal frameworks require reforming. This was further underlined by the European Parliament Resolution of March 2014 on the United States 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), launching a *European Digital Habeas Corpus*.

"The Snowden revelations gave us a chance to react. I hope we will turn those reactions into something positive and lasting into the next mandate of this Parliament, a data protection bill of rights that we can all be proud of."
(Claude Moraes, MEP, Rapporteur in the NSA EP inquiry, Press release, 12 March 2014)

Mapping EU Member States' legal frameworks related to surveillance

In April 2014, the European Parliament requested the European Union Agency for Fundamental Rights (FRA) "to undertake in-depth research on the protection of fundamental rights in the context of surveillance". The FRA did so, mapping the 28 EU Member States' legal frameworks related to surveillance and providing an overview of existing fundamental rights standards. It focused on oversight mechanisms and on remedies available to individuals alleging infringements of their right to privacy.

The FRA legal research does not examine surveillance techniques as such. It reviews how current legal frameworks enable the use of such techniques, and explores the crucial role specialised bodies play in overseeing the work of intelligence services. In addition, it scrutinises to what extent the relevant safeguards protect privacy and data protection across the 28 EU Member States.

'Intelligence services' have a foreign mandate and focus on external threats, while 'security services' have a domestic mandate and focus on domestic threats. The FRA report uses 'intelligence services' as a generic term for both.

This summary presents FRA's main research findings, which are published in full in the report entitled *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (see Further information).

Data collection and coverage

For this research, FRA examined the legal frameworks on surveillance in the 28 EU Member States, analysing laws and relevant fundamental rights standards to present a comparative analysis of the legal context of surveillance across the EU.

Based on answers provided by Franet, the agency's multidisciplinary research network, FRA collected data and information through desk research in all 28 EU Member States. Additional information was gathered through exchanges with key partners, including a number of FRA's national liaison officers in the Member States, specialised bodies, and individual experts. The 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.

A second socio-legal report with FRA opinions, based on empirical research, will be published at a later stage, further expanding on the findings presented here.

Fundamental rights safeguards and EU law

"The hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether."
(*United Nations (UN), Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2014),* Fourth annual report submitted to the General Assembly, *A/69/397, 23 September 2014*)

The EU Member States are all bound by minimum international human rights law standards developed by the United Nations (UN), which are of universal application, such as the Human Rights Council Resolution on the right to privacy in the digital age (Doc. A/HRC/28/L.27, 24 March 2015). Various UN expert and treaty bodies condemned mass surveillance practices following the Snowden revelations. Council of Europe standards, including European Court of Human Rights (ECtHR) case law, also outline minimum standards. In addition, EU law, as interpreted by the Court of Justice of the European Union (CJEU), is relevant. Finally, in an area where only limited international regulations – other than existing international human rights law – directly apply, self-regulatory measures and soft law are also important.

The report focuses on the rights to privacy and data protection, which are enshrined in Articles 7 and 8 of the Charter. The right to data protection is also laid down in primary and secondary EU law, ensuring that, in their respective scope of application, processing of personal data is carried out lawfully and

only to the extent necessary to fulfil the legitimate aim pursued. These rights extend to all persons, whether they are citizens of the EU or third-country nationals. According to Article 52 (1) of the Charter, any limitation to this right must be necessary and proportionate, genuinely meet objectives of general interest recognised by the Union, be provided by law, and respect the essence of such rights.

Despite the existence of international guidelines, there is no uniform understanding of 'national security' across the EU. Neither EU legislation nor CJEU case law further define this concept, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified.

This unclear delineation of 'national security' has repercussions for the applicability of EU law. Article 4 (2) of the Treaty on the European Union provides that "national security remains the sole responsibility of each EU Member State". This does not mean that the 'national security' exemption renders EU law entirely inapplicable. The interpretation of 'national security' at Member State level and the manner in which surveillance programmes are carried out can be assessed by the EU institutions, particularly the CJEU.

Types of surveillance: targeted and untargeted

The FRA research examines how both targeted and untargeted surveillance are organised under the EU Member States' legal frameworks.

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

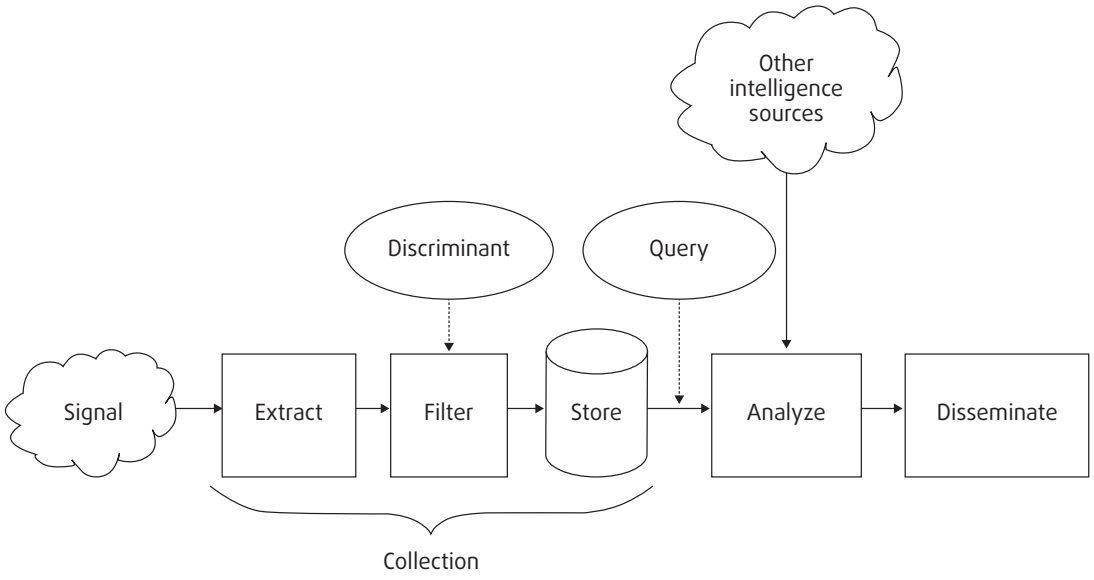
- targeted interception relates to "[i]nterception where the person, organisation or technical characteristic at whom/which the data collection is targeted can be specified in advance";
- untargeted interception relates to "[i]nterception where the person, organisation or technical characteristic at whom/which the data collection is targeted cannot be specified in advance".

CTIVD, *Annual Report 2013-2014*, The Hague, 31 March 2014, p. 45–46

The sheer scale of data collected through the uncovered surveillance programmes – such as PRISM, Xkeyscore and Upstream – triggered wide-reaching reactions. 'Mass surveillance' (often understood as untargeted) involves collecting vastly different amounts of data than with traditional, secret (targeted) surveillance methods, such as telephone tapping. The latter is based on the prior suspicion of a specific individual or organisation. This type of surveillance is prevalent in, and acknowledged by, EU Member States' laws. The overwhelming majority of EU Member States' legal frameworks do not regulate or even refer to 'mass surveillance' as such. Only a few EU Member States have detailed legislation on signals intelligence (SIGINT), which is the generic term used to describe the interception of signals from various sources by intelligence services. The FRA research uses the term signals intelligence throughout its analysis.

SIGINT derives from military intelligence. It refers to the automated gathering of information through the interception and collection of digital data related to intelligence activity. The figure highlights that collected signals are filtered using discriminants or selectors – a set of parameters placed in the filtering process, either *a priori* or dynamically, to define the criteria that will determine which data to store in order to obtain the relevant information (for example, "all email addresses used in communications with Yemen").

Figure: Conceptual model of signals intelligence



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

The United States National Research Council of the National Academies has referred to signals intelligence as an encompassing term for any data stored on an electronic device. The Venice Commission uses SIGINT as a collective term for means and methods for intercepting and analysing radio (including satellite and cellular phone) and cable-borne communications.

FRA's analysis of the legal frameworks that regulate surveillance methods of intelligence services shows that the laws of five EU Member States (France, Germany, the Netherlands, Sweden and the United Kingdom) detail the conditions that permit the use of both targeted and untargeted surveillance, such as signals intelligence. Other Member State laws insufficiently specify these conditions, hampering a legal analysis of the exact procedures in place on collecting signals intelligence. Even though the laws in these countries do not specifically refer to SIGINT, it may nonetheless be carried out. However, given that the practice is prescribed only in unpublished regulatory measures in these countries, an analysis of the applicable legal frameworks will not shed any light on the matter.

Key findings

Intelligence services and surveillance laws

Objective and structure of intelligence services

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

- Almost all EU Member States have established at least two different intelligence services bodies, one for civil and one for military matters; the latter are not covered in this report. Civil intelligence services are generally subordinate

to interior ministries, and sometimes also to the prime minister or president.

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

Protecting national security

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

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

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

Legal regulation of surveillance

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

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

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

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

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

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

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

Oversight of intelligence services

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

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

Executive control and coordination between oversight bodies

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

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

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

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

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

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

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

Parliamentary oversight

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

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

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

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

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

Expert oversight

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

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

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

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

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

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

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

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

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

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

Remedies

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

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

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

Obligation to inform and the right to access

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

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

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

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

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

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

Judicial remedies

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

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

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

Non-judicial remedies

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

- The oversight bodies (including DPAs) in charge of dealing with complaints are independent institutions in the great majority of Member States.
- Where an executive oversight body has remedial powers, the question of independence arises when it also has the power to warrant surveillance. Parliamentary and expert oversight bodies have more autonomous administrative structures – but autonomy does not guarantee an effective remedy unless also supported by sufficient knowledge. How members of oversight bodies are appointed, and their place in the administrative hierarchy, are also important aspects to consider when assessing a body's independence.
- DPAs in 13 EU Member States have the power to examine individual complaints and issue binding decisions. But in three of these, the power to access files and premises is limited. In five Member States, additional requirements – mandating the presence of the head or a member of the DPA during inspections at intelligence service premises – apply.
- Five out of the seven Member States that entrust their expert oversight bodies (other than DPAs) with specific remedial powers do so by allowing these bodies to issue binding decisions. In one EU Member State, an executive oversight body also has remedial powers, including the power to issue binding decisions. Parliamentary committees in four Member States are entitled to hear individual complaints, but only one can resolve them with binding decisions.
- Ombudsperson institutions, which exist in all 28 EU Member States, mostly deal with administrative failures rather than with the actual merits of surveillance. Only one Member State provides the ombudsperson institution with remedial powers via the relevant intelligence law. In addition, the ombudsperson institutions' powers can be quite limited, and proceedings typically conclude with non-binding recommendations that aim to put matters right and guide future action, rather than with a binding, enforceable judgement. This obviously impacts the effectiveness of the remedies they are able to provide.
- Other elements that can facilitate an individual's access to remedies include more relaxed rules on the evidentiary burden and class actions, as well as effective whistleblower protection. The Parliamentary Assembly of the Council of Europe considers whistleblowing to be the most effective tool for enforcing the limits placed on surveillance.

Conclusions

Addressing an area of restricted EU competence, the report highlights the diversity among Member States with regard to how intelligence services are organised and perform their essential tasks.

Surveillance measures greatly interfere with individuals' rights. Given their secret nature, individuals are bound to rely on a degree of trust in public authorities, which in turn must safeguard individuals' fundamental rights. Attaining the level of trust a society should have vis-à-vis its intelligence service requires accountability. Clear and accessible legislation, strong oversight mechanisms, proper control mechanisms and effective remedies are only some of the elements essential to achieving this kind of accountability, which undeniably remains difficult due to the secrecy intelligence services operate in. Introducing and maintaining clear and accessible legislation and strong oversight mechanisms at Member State level merely constitutes the first step towards a transparent and fundamental rights-compliant system – difficulties in doing so suggest that obstacles remain.

The reactions to the Snowden revelations have highlighted the need to adapt and strengthen the relevant legal frameworks in the EU and across its Member States. The FRA research shows that a number of legal reforms have already been carried out. Periodical assessments of the functioning and legitimacy of the frameworks that govern intelligence service activity must become an integral part of the oversight systems. How to further reform the legal frameworks to address the lack of adequate oversight is also a key question. In addition, reforms in the EU Member States need to take into account recent technological developments to ensure that oversight mechanisms are afforded the requisite tools and expert knowledge. Achieving all of this is undeniably challenging, but vital for performing the difficult task of protecting security while safeguarding fundamental rights.

Protecting the public from security threats and safeguarding fundamental rights involves a delicate balance. Brutal terror attacks and technological innovations making possible large-scale communications data monitoring have further complicated the matter, triggering concerns about violations of the rights to privacy and data protection in the name of national security protection. The Snowden revelations, which uncovered extensive and indiscriminate surveillance efforts worldwide, made clear that enhanced safeguards of these rights are needed.

This report, drafted in response to the European Parliament's call for thorough research on fundamental rights protection in the context of surveillance, maps and analyses the legal frameworks on surveillance in place in EU Member States. Focusing on so-called 'mass surveillance', it also details oversight mechanisms introduced across the EU, outlines the work of entities tasked with overseeing surveillance efforts, and presents the remedies available to individuals seeking to challenge such intelligence activity. By demonstrating the complex considerations involved, this report underscores how difficult it can be to address what are often seen as competing priorities, and contributes to the continuing debate on how to best reconcile them.

Further information:

For the full FRA report – *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* see http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

See also other FRA publications in this field:

- FRA-Council of Europe (2014), *Handbook on European data protection law*, Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (available in various languages)
- FRA (2014), *Access to data protection remedies in EU Member States*, Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states and the report summary http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary (available in various languages)

An overview of FRA activities on data protection is available at: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Publications Office

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria
Tel: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

ISBN 978-92-9491-040-0

TK-04-15-738-EN-N doi:10.2811/67533