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

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.

Intelligence services play a crucial role in protecting national security and helping law enforcement to uphold the rule of law. With terrorism, cyber-attacks and organised crime posing growing threats in the EU, the work of intelligence services has become increasingly urgent, complex and international.

Digital surveillance methods serve as important resources in intelligence efforts, ranging from intercepting communications and metadata through to database mining. But these activities may also interfere with diverse fundamental rights, particularly privacy and data protection.

"[A]ny interference can only be justified under Article 8 paragraph 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 […]."
(ECtHR, *Roman Zakharov v. Russia* [GC], No. 47143/06, 4 December 2015, para. 227)

In the aftermath of the Snowden revelations, the European Parliament adopted a resolution that, among others, 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, particularly with respect to judicial remedies. In response, FRA published its 2015 report on *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume I: Member States' legal frameworks*.

Much has happened since 2015, including: serious terrorist attacks; migration pressures across the Mediterranean, prompting suspension of Schengen area free movement arrangements; and a rising tide of cyber-attacks. The new threats and new technology have triggered extensive reforms. Several EU Member States have introduced legislation to strengthen intelligence gathering, 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.

FRA's second report on surveillance – *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volume II: field perspectives and legal update* – therefore updates the agency's legal analysis. It also supplements that analysis with field-based insights gained from extensive interviews with diverse experts. Taken together, the two reports constitute FRA's response to the European Parliament's request to study the impact of surveillance on fundamental rights. This summary outlines the main findings from the second report.

Surveillance: legal update and field perspectives

The second part of FRA's research reviews the legal frameworks regulating intelligence work in the EU's 28 Member States, examines applicable oversight mechanisms, and takes a look at remedies available to individuals who believe their rights have been violated.

Legal framework for intelligence

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

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

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 persistent lack of clarity as a major source of uncertainty.

"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."
(Expert body)

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

According to the 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. European courts also consider the collection of data by intelligence services to amount to an interference. Such interference needs to be justified to be human rights compliant.

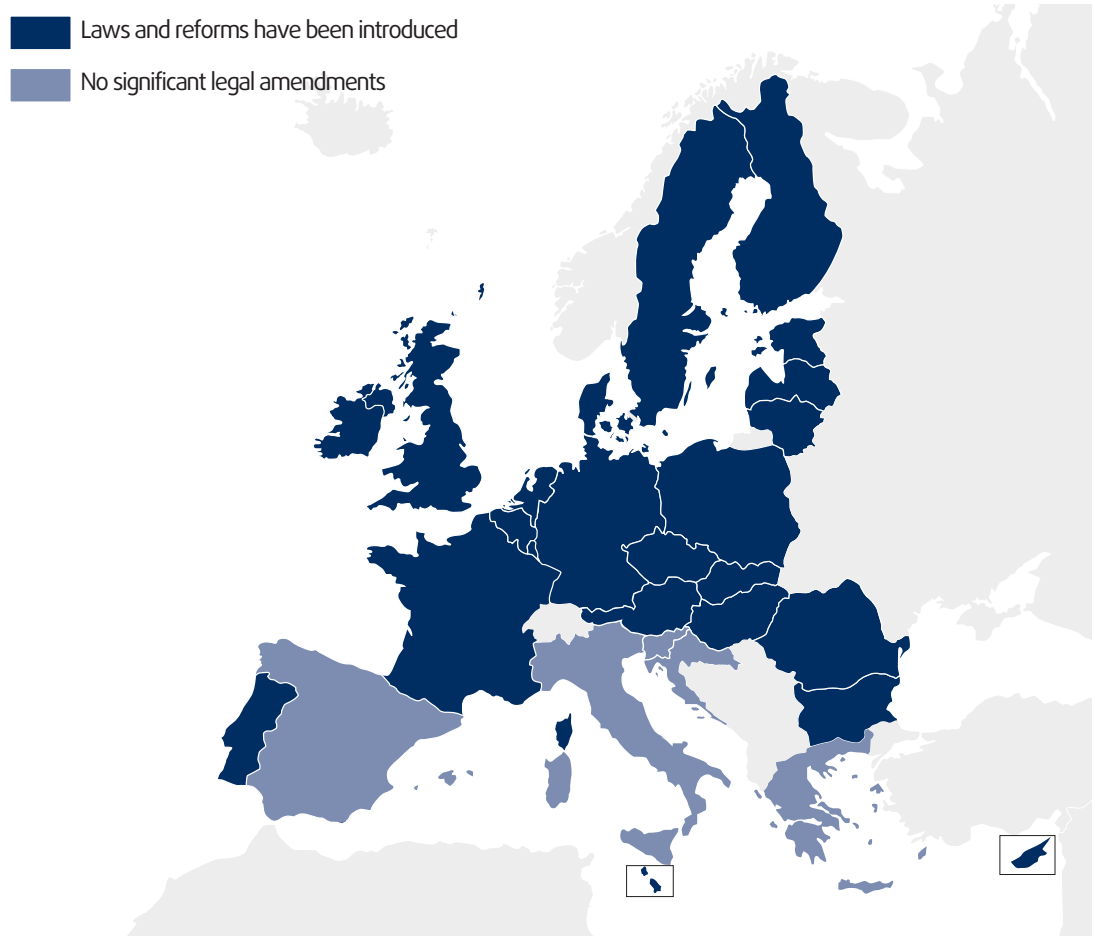
Data collection and coverage

The second wave of FRA's research builds on its 2015 report by providing a socio-legal analysis. Specifically, it:

- updates the first 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 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.

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



Source: FRA, 2017

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.

Targeted surveillance is regulated in some detail by almost all 28 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 the 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.

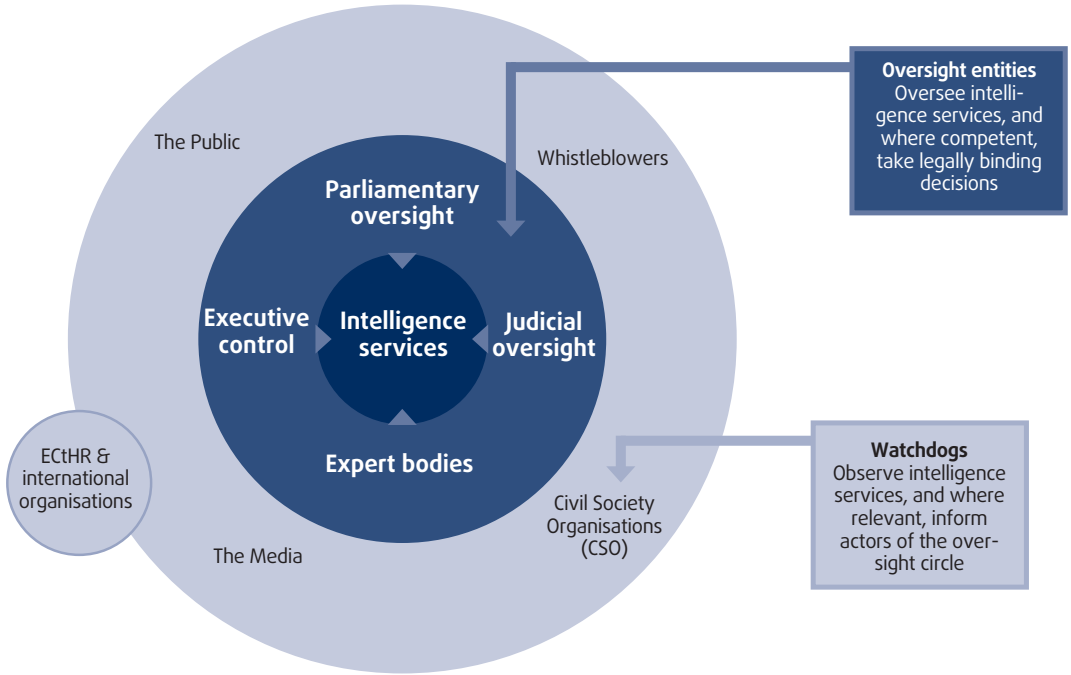
Accountability

Various entities oversee the work of intelligence services across the 28 EU Member States, 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.

"Oversight is not lack of trust, but willingness to clarify."
(Parliamentary committee)

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.

Figure 2: Intelligence services' accountability scheme



Source: FRA, 2017

Almost all interviewees from oversight bodies maintained that they are able to resist external influence, but some lawyers, civil society representatives 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 access relevant data and information sometimes boils down to limited technical capacities regarding oversight functions. Interviewees acknowledged that these factors pose a problem – and that the sensitivity of the work can discourage individuals from seeking external expertise.

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

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

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

Promising practice

Promoting transparency in oversight

Some EU Member States achieve enhanced transparency while respecting necessary secrecy. Oversight bodies' approaches to transparency, however, vary across countries, ranging from publishing regular reports to having websites or using social media. Some examples of how oversight bodies seek to promote transparency follow.

Regularly issuing detailed reports

The Italian Parliamentary Committee for the Intelligence and Security Services for State Secret Control, COPASIR, the French Parliamentary Delegation on Intelligence, DPR, the German Parliamentary Control Panel, PKGr, and the United Kingdom's Intelligence and Security Committee of Parliament, ISC, all 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 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)

Reports on number of individuals under surveillance

The annual reports of the French National Commission of Control of the Intelligence Techniques, CNCTR, and the German G10 Commission 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 2016 annual report of the Belgian Standing Committee I 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).

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.

"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)

"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)

"[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)

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 a significant number of Member States (27) only require prior approval from the executive.

"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)

"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)

Promising practice

Enhancing international cooperation among oversight bodies

Equal access to information obtained through international cooperation could allow enhanced international cooperation among oversight bodies. In 2015, oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland launched a 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; The Netherlands, CTIVD (2017), p. 33.

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 a 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 per year.

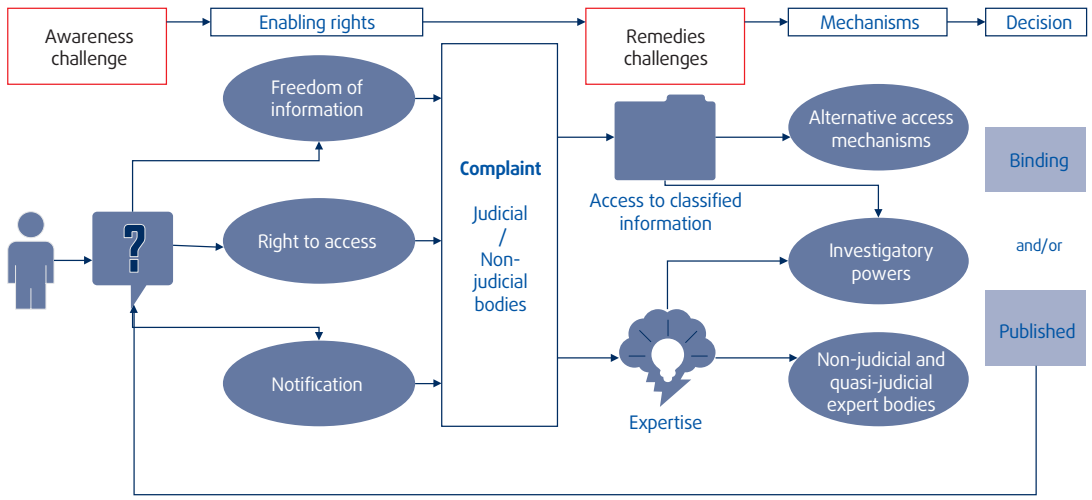
"The average citizen does not even know where to address a complaint." (Data protection authority)

"[The legal framework governing the protection of whistleblowers] 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)

"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)

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.

Figure 3: Implementing effective remedies: challenges and solutions



Source: FRA, 2017

"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 [classify] everything, which is a problem. We need much more transparency, robustness from the domestic court."
(Civil society organisation)

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.

"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 [intelligence services] or even a[n intelligence services] subordinate 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)

Promising practice

Transparent scrutiny of denial of rights

In 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 the Netherlands, in 2013 the Oversight Committee for the Intelligence and Security Services, 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 Federal Intelligence Service, 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 BND provided the information.

See The Netherlands, (CTIVD) (2013) and CTIVD (2016), p. 14; Germany, Federal Parliament (Deutscher Bundestag) (2017a), pp. 6 and 8.

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.

Key findings and FRA opinions

The following opinions build on the key findings of FRA's research on *Surveillance by intelligence services*, as outlined in Volume II on 'field perspectives and legal updates'.

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 amongst 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 that, 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

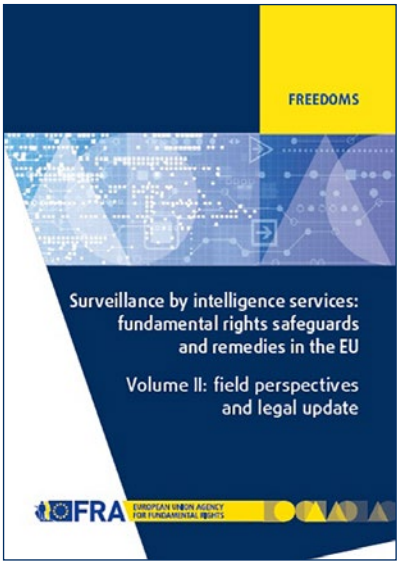
EU Member States should ensure that where judicial or non-judicial remedial bodies lack relevant expertise to effectively assess individuals' complaints, specific systems are established to address these gaps. Cooperation with expert oversight bodies, technical experts or members of the intelligence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



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.

Further information:

For the full FRA report – *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update* – see http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

Other relevant FRA publications include:

- FRA (2015), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Vol. I: Member States' legal frameworks*, Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services
- 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 EU languages; update forthcoming in May 2018)

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 978-92-9491-985-4

TK-02-18-203-EN-N doi: 10.2811/84431