MEMO / 23 October 2017

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

Why was this work carried out?

In June 2013, Edward Snowden, a contractor working at the US National Security Agency (NSA), revealed to the media information about extensive global surveillance programmes by intelligence services. The EU institutions reacted promptly with political declarations and resolutions. The European Parliament decided to conduct an in-depth inquiry into the NSA surveillance programme. This led to the European Parliament Resolution of 12 March 2014 which also called on FRA to carry out research into the protection of fundamental rights in large-scale surveillance operations.

Since then, subsequent terrorist attacks have once again thrown the spotlight on the question of finding the right balance between safeguarding fundamental rights while also maintaining security through the work of national intelligence services.

How was the work carried out?

This second volume, '*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*', explores legal changes since the first volume in 2015 and how these laws are applied in practice. It is based on data from all EU Member States on the legal framework governing surveillance collected by FRA's multidisciplinary research network, FRANET. It was complemented by field research in seven Member States: Belgium, France, Germany, Italy, the Netherlands, Sweden and the UK. This involved more than 70 interviews with a range of stakeholders either directly involved with or concerned with data protection and privacy issues related to surveillance. These included overseers and controllers from the executive, indepedent expert bodies, parliamentary committees, the judiciary and actors from the civil society. The report also contains quotes from the experts.

What did the research cover?

The project focused on existing safeguards in relation to two particular fundamental rights: respect for private and family life, and the protection of personal data in the EU's Fundamental Rights Charter. It analysed how national institutions, in charge of upholding fundamental rights, ensure democratic oversight over intelligence services and how they provide remedies for rights violations.

It led to a comparative analysis of the EU Member States' legal frameworks regarding surveillance with an overview of existing fundamental rights standards. It also provided data on the day-to-day implementation of national legal frameworks in seven Member States relating to surveillance. It also looked at international cooperation between intelligence services.

The project did not analyse surveillance techniques but rather maps the legal frameworks that enable these techniques. It did not cover data collection for military purposes and law enforcement, including data retention.

What is national security?

Although Member States share the common aim of protecting national security, what this actually means is not harmonised across the EU. How this translates to mandates and areas of activity also varies, and may extend to organised crime and cybercrime, for example.

Which types of surveillance did FRA look at?

Intelligence can be collected using a variety of techniques and en masse. They are different ways of referring to these technqiues but in general terms it is often called 'mass surveillance'. However, 'mass surveillance' as a term is not used in national law. FRA used the term general surveillance of communications. It covers targeted surveillance and untargeted surveillance. Targeted surveillance, such as telephone tapping, is when the the person or organisation is suspected. Untargeted is when there neither prior suspicion nor a specific target.

Who is responsible for intelligence across the EU?

Intelligence services in the EU are extremely diverse as the organisation of the intelligence community is closely linked to the country's historical developments. In some Member States, two intelligence services carry out the work; in others, five or six bodies are in charge of it. Some differentiate between civil and military intelligence. A list of all intelligence services is annexed in the report.

Is surveillance regulated?

Intelligence services are regulated by law in all Member States.

These laws specify the mandates and powers of national intelligence services. However, the laws can range from one legal act to complex frameworks where several laws and ordinances regulate specific aspects of the service. (See Annex 2 of report)

Most legal frameworks only regulate in detail targeted surveillance, either towards individuals or defined groups/organisations. France, Germany, the Netherlands, Sweden and the UK have detailed laws on the conditions for using general surveillance of communications Finland is in the process of reforming its laws and should have detailed legislation on general surveillance of communications, if adopted.

What has been the impact of the many reforms that have taken place in Member States?

The reforms have increased transparency on surveillance powers granted to intelligence services. They have provided a legal basis for the use of some new tools; however, this was criticised by some civil society respondents. However, while legal reforms have brought improvements, many aspects remain unclear.

Who carries out the checks and balances needed to oversee surveillance measures?

Oversight of surveillance measures is normally undertaken either by the judiciary or an expert body. In 19 Member States judicial bodies are involved generally when authorising targeted surveillance measures (See Table 4 in report). In 16 Member States it involves expert bodies and in 21 Member States it is one or two specialised parliamentary committees. (See Figure 6 in report)

In all Member States, data protection authorities (DPAs) safeguard the right to the protection of personal data. In seven Member States, DPAs have the same powers over intelligence services as over all other data controllers, in 10 their powers are limited, and in 11 they have no powers over intelligence services. (See Figure 8 in report).

What are the limits to effective oversight?

Effective oversight requires independent bodies to have sufficient resources, powers and competences. Oversight bodies must also work together to ensure all aspects of the work of intelligence services is covered. They must also make greater efforts to be transparent to allow for public scrutiny.

All 28 Member States include at least one independent body in the oversight of intelligence. While interviewees from oversight bodies confirmed that their institutions are independent and impartial, some academics and civil society respondents questioned this.

Effective oversight also calls for proper coordination between the various oversight bodies to ensure that all aspects of the work of intelligence services are covered. If oversight bodies do not have a clear, comprehensive understanding of the work of the entire national intelligence community, all areas of their work will not be covered and gaps in oversight will result. This hinders the effectiveness of the oversight system.

Oversight bodies in all five Member States with detailed legal provisions on general surveillance of communications can initiate their own controls. However, in only three do they have some form of binding powers (Germany, Sweden and the UK).

All Member States also provide at least one of their oversight bodies with full access to all relevant data and information. However, lack of technical expertise remains one of the biggest challenges.

While transparency is improving, partly through the publication of annual reports, some considered the information in such reports uninformative.

When it comes to authorisation of targeted surveillance measures, 22 Member States include an independent authority - judicial or expert in the process (See Table 4 in report). In six Member States, all types of targeted surveillance may be implemented without ex ante oversight by an independent body. Only three of the five Member States that have detailed provisions on general surveillance of communications, must involve an independent body in authorising such measures (See Table 5 in report). However, in all five Member States, an independent body oversees the implementation) of these measures.

How can victims seek justice?

The right to an effective remedy is essential for access to justice. It allows individuals to seek redress for rights violations. Previous FRA research on access to data protection remedies identified a number of remedial avenues and the issues associated with them.

Every Member State gives individuals the possibility to complain about privacy violations via the courts. Non-judicial remedies - expert (including DPAs), executive and parliamentary oversight bodies and ombudsperson institutions - are more accessible 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 (Czech Republic, Latvia, Poland - See Table 6 in report). In ten of the 25 EU Member States that do, individuals can complain to only one non-judicial body, and in the remaining 15, they can complain to two or more bodies.

Even though the possibility to seek justice exists, in practice on average, according to the experts interviewed, only 10 to 20 complaints are filed per year.

What are the problems in getting justice?

Various factors hamper access to justice. These include low levels of awareness about the existence of remedies and non-implementation of the right to access information and/or the notification obligation caused in part by the secrecy surrounding surveillance work. In eight Member States, the obligation to inform and the right to access are not provided for at all in law. In the other 20, restrictions apply, such as the need to protect national security, national interests or the reason behind the surveillance.

Although courts can be used, general access to justice barriers such as costly and lengthy procedures apply as well as the difficulties surrounding providing evidence. In addition, judges, unless specialised, may lack the specialist knowledge to tackle such cases.

Different non-judicial bodies playing different roles with different powers coupled with the large amount of data collected also make it difficult to take remedial action.

What controls are there over international cooperation between intelligence services?

Almost all EU Member States' laws (except for Malta) have grounded international intelligence cooperation into law. However, only a few provide details in their legislation on the procedures intelligence services must follow to establish international cooperation. Before establishing cooperation agreements, intelligence services from eight Member States must follow confidential internal rules (Belgium, Denmark, Germany, Lativa, Lithuania, The Netherlands, Portugal and the UK). A small number of Member States' laws prescribe a review of international cooperation agreements by independent bodies (Belgium, Luxembourg, The Netherlands).

Of the only 11 EU Member States that provide for oversight of international cooperation by law, three have excluded information from foreign services from oversight (France, Ireland, Spain); four do not differentiate between oversight for international sharing of data and for domestic sharing of data (Denmark, Finland, The Netherlands, Romania); and four have limited the scope of the control over information obtained through such cooperation (Germany, Luxembourg, Portugal, Sweden).

What can be done to improve the situation?

The analysis points to the need to strengthen the national legal frameworks that govern surveillance. Efforts should be made to ensure laws are clearly understood by all concerned and that they provide effective comprehensive and robust oversight mechanisms. They should also ensure that oversight bodies' staff have the required technical expertise to assess surveillance work.

Oversight bodies' mandates should also extend to international intelligence cooperation which should be subject to with clearly defined legal rules on intelligence sharing. Expert bodies should be exempt from the principle that prevents third parties from accessing and overseeing intelligence passed from the foreign to the national intelligence body.

Member States should also provide access to effective remedies for people who have been victims of violations of their right to privacy and data protection. This includes granting judicial and non-judicial bodies with the powers and expertise to assess complaints. When needed, it should allow for cooperation with experts bodies to get the necessary technical know-how.

Are there examples of good practices?

The report gives examples of good practices that were identified during the research. These include:

- In the UK, surveillance measures were explained in simple terms in codes of practice and on intelligence services' websites.
- Oversight bodies in Belgium, Denmark, France, Greece and The Netherlands publish 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.
- In The Netherlands and Germany, oversight bodies assess the grounds on which notification of or access to information was denied.

For further information, please contact the FRA Media Team:
Email: media@fra.europa.eu / Tel.: +43 1 58030-642

FRA's work on Information society, privacy and data protection issues and related publications can be found at online.