MEMO / 18 November 2015

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. In particular, the European Parliament decided to conduct an in-depth inquiry into the NSA surveillance programme. The inquiry's results fed into the European Parliament Resolution of 12 March 2014. Part of the Resolution called on FRA to conduct research into the protection of fundamental rights in the context of large-scale surveillance.

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?

The report, '*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*', is based on data from all EU Member States on the legal framework governing surveillance collected by FRA's multidisciplinary research network, FRANET. Additional information was gathered through desk research and exchanges with key stakeholders, individual experts as well as a number of government officials in the Member States who have been appointed as FRA's main contact point as national liaison officers.

What did the research cover?

FRA's project focuses on existing safeguards in relation to the two particular fundamental rights when it comes to large-scale communication surveillance by intelligence services: respect for private and family life, and the protection of personal data (Article 7 and Article 8 of the EU Charter of Fundamental Rights). The project analyses how national institutions, in charge of upholding fundamental rights, ensure democratic oversight over intelligence authorities and how they provide remedies against rights violations.

This report contains a comparative analysis of the EU Member States' legal frameworks regarding surveillance with an overview of existing fundamental rights standards. The report does not analyse surveillance techniques but rather maps the legal frameworks that enable these techniques. It also does not assess the implementation of the respective laws.

The scope of the project focuses on the legal regimes governing surveillance by national intelligence authorities. It does not cover data collection for law enforcement, including data retention laws.

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?

FRA looked at targeted surveillance and untargeted surveillance often refered to as 'mass surveillance'. 'Mass surveillance' as a term is not used in national law. When surveillance is mentioned it tends to refer to signals intelligence i.e. the automated gathering of information through the interception and collection of digital data by the use of search terms not necessarily linked to an individual. Targeted surveillance, such as telephone tapping, is when the data target - the person, organisation or technical characteristic - is specified in advance.

How are intelligence services organised 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.

What is the legal basis for surveillance?

Intelligence services are regulated by law in all but two Member States. The Portuguese constitution prohibits its intelligence service from undertaking surveillance. Cyprus is discussing legislation that will regulate its intelligence services' surveillance practices.

The mandates and powers of the national intelligence services are regulated by relevant domestic laws, ranging from one unique legal act to complex frameworks where several laws and ordinances regulate specific aspects of the service.

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 signals intelligence.

How is oversight organised?

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, all areas of their work will not be covered and gaps in oversight will result. This will hinder the effectiveness of the oversight system. Seven Member States have sought to address this by having an oversight system involving different types of bodies.

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

There is have parliamentary oversight in all Member States, except for Ireland, Malta, Finland and Portugal. Of these only Cyprus, Greece and Sweden have not set up specific parliamentary committees to oversee the governmental policies carried out by intelligence services. However, although some parliamentary committees can request access to intelligence information, none can demand it.

Although parliamentary oversight is crucial, it must be complemented by other oversight bodies, particularly 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.

Expert bodies need to be not just legally but also technically knowledgeable. Some Member States ensure this by including experts from a range of different fields, including information and communications technology. Others rely heavily on a combination of current or former judges and parliamentarians. 15 Member States have expert bodies exclusively dedicated to intelligence service oversight (See Table 2). They can authorise surveillance measures, investigate complaints, request documents and information from the intelligence services, or give advice to the government and/or parliament.

In all Member States, data protection authorities (DPAs) safeguard the right to the protection of personal data. In seven Member States they have the same powers over intelligence services as they do over any other data controller, in nine their powers are limited and in 12 they have no powers over intelligence services (See Table 3).

Which remedial avenues are available?

The right to an effective remedy is an essential component of 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.

The secrecy surrounding surveillance work impinges on the right to be notified and to have access to information which are essential for any remedial action. 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 begind the surveillance.

Non-judicial bodies - expert (including DPAs), executive and parliamentary oversight bodies and ombudsperson institutions - play an important remedial role also in surveillance cases. However, different bodies playing different roles with different powers coupled with the large amount of data collected make it difficult to take remedial action.

In most Member States, DPAs can deal with with most complaints about privacy violations because of surveillance. In 13 Member States, DPAs can deal with complaints and issue binding decisions but in eight of these, there are constraints such as limited access to files or the intelligence services premises (See Figure 6). In seven Member States, there are also expert oversight bodies (other than DPAs) which have the power to provide remedies, of which only five can issue binding decisions. Parliamentary committees in four Member States are entitled to hear individual complaints but only in Romania can they resolve them via a binding decision. Only the Netherlands has granted the ombudsperson institution remedial powers under the relevant intelligence law.

Every Member State gives individuals the possibility to complain about privacy violations via the courts. 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.

What can be done to improve the situation?

The legal 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 comprehensive oversight mechanisms thar are effective and offer access to remedies for people who have been victims of violations of their right to privacy and data protection.

How will FRA follow up on the results?

The second stage of the project will consist of field research in selected Member States. The plans are to carry out field research in Belgium, France, Germany, Italy, the Netherlands, Sweden and the UK. This will involve interviews with a range of stakeholders either directly involved with or concerned with data protection and privacy issues related to surveillance. It will provide data on the day-to-day implementation of national legal frameworks relating to surveillance.

The findings from the fieldwork will be combined with the legal analysis in a final report. This report is due by the end of 2016.

FRA's work on Information society, privacy and data protection issues and related publications can be found at:
http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection.
For further information, please contact the FRA Media Team:

Email: media@fra.europa.eu / Tel.: +43 1 58030-642