Safeguarding internal security in compliance with fundamental rights law

FRA contribution

High-level conference on a renewed EU Internal Security Strategy

Brussels, 29 September 2014

Key messages

This paper examines the inter-relatedness between security and fundamental rights as one of the key challenges in the area of internal security. It calls for mainstreaming fundamental rights into the design of internal security measures to increase their proportionality and legitimacy. Examples of key messages in relation to specific issues include:

- **Passenger Name Record (PNR)**: Safeguards such as clear and strict limitations on purpose, protection of personal data and increased transparency of the system towards passengers should be part of any potential attempt to create an EU PNR system.
- **'Foreign fighters'**: Measures to contain the threat posed by EU citizens acting as 'foreign fighters' must be proportionate to their purpose, by taking into account, for instance, that surveillance of a specific group or profiling of potential suspects based solely or mainly on their ethnicity or religion constitutes unacceptable discriminatory treatment. Cooperation with relevant communities needs to be reinforced to prevent radicalisation as well as to avoid loss of legitimacy.
- **Surveillance**: Reform of EU Member States' surveillance frameworks needs to address issues of transparency and democratic oversight of intelligence services, while recognising the inherent need for secrecy in their operations.

Background

As the European Union enters the 'post-Stockholm programme' era, marked by the adoption of new Strategic Guidelines for legislative and operational planning for the coming years within the area of freedom, security and justice,[1] the EU fundamental rights landscape is also transforming itself. Major structural developments, such as the upcoming accession of the EU to the European Convention on Human Rights (ECHR), the reform of the data protection regime and the end of the transitional period for the former 'third pillar', will provide a new framework for the protection of core European Union (EU) values – human dignity, freedom, democracy, equality, the rule of law and respect for fundamental rights. A new EU framework introduced by the European Commission also aims at strengthening the rule of law in EU Member States, in reaction to concerns over the effective operation of mechanisms established at national level.[2]

Despite these developments, the impact of fundamental rights considerations on some EU policies remains a challenge, including the design of responses to internal security threats. There is no doubt about the existence and severity of these threats and the need to react to them in an effective and expedient manner. Organised crime, the threat of terrorist activities amplified by the proximity of open conflict areas (particularly in the Middle East) and cybercrime in its numerous manifestations are just some of the urgent problems that the EU faces and needs to counter. The present Internal Security Strategy[3] subscribes to respect human rights and fundamental freedoms, some of the key measures proposed or already taken at the EU or Member State level, however, make it apparent that safeguarding internal security in a way compliant with fundamental rights constitutes a serious challenge for policymakers – one that needs to be addressed during the forthcoming debate on the renewed strategy.[4]

---

1 European Council (2014), *Conclusions*, EUCO 79/14, p. 2–6. Brussels, 27 June 2014. For the FRA contribution to the discussion on the new strategic guidelines, see: FRA (2013), *Fundamental rights in the future of the European Union's Justice and Home Affairs*, Vienna, http://fra.europa.eu/en/publication/2013/fundamental-rights-future-european-unions-justice-and-home-affairs.

2 European Commission (2014), *Communication from the Commission to the European Parliament and the Council: A new EU Framework to strengthen the Rule of Law*, COM(2014) 158 final/2, Brussels, 19 March 2014.

3 European Council (2010), *Internal Security Strategy for the European Union: Towards a European security model*, Luxembourg, Publications Office of the European Union (Publications Office).

4 In the present Internal Security Strategy, the European Council also highlighted that it understands 'security in itself as a basic right', which would be a topic for a separate debate. For an interesting contribution to this issue, see: European Group on Ethics in Science and New Technologies to the European Commission (2014), *Ethics of security and surveillance technologies*, Luxembourg, Publications Office, pp. 38–40.

Some consider adverse effects on fundamental rights to be a necessary by-product of security measures, or even inherent to them and imperative for their operability. According to the principle of proportionality enshrined in Article 52 of the Charter of Fundamental Rights of the EU, however, "limitations on the exercise of the rights and freedoms recognised by the Charter may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." The key to increasing proportionality therefore lies in adjusting the scope of the measures, and either eliminating elements that are not strictly necessary or introducing them in a fundamental rights-consistent manner.

Taking into account the shared competences between the EU and its Member States in the area of internal security and the 'national security' exemption enshrined in Article 4 (2) of the Treaty on European Union, the issue is relevant at both the EU and Member State level. Rulings of national courts across the EU, as well as of the European Court of Human Rights (ECtHR), have repeatedly confirmed that even reasons of national security should not prevent the application of fundamental rights safeguards.[5]

With the above in mind, the following sections present **examples of three highly topical policy issues**:

- the use of Passenger Name Record (PNR) information for law enforcement purposes;
- measures taken vis-à-vis 'foreign fighters';
- the large-scale surveillance of digital communication by intelligence services.

In that they are closely linked to countering terrorist threats, these issues have the potential to remain part of the internal security debate in the coming years. In all these areas, it is possible to illustrate the key concerns and suggest a more balanced, fundamental rights-consistent approach.

Passenger Name Record

The gathering and exchange of PNR data has been a contentious fundamental rights issue since the bilateral negotiations between the EU and the United States of America (US) began in 2003. The fundamental

[5] See, for instance, United Kingdom, House of Lords, *A and Others v. Secretary of State for the Home Department* [2004], UKHL 56; or recently ECtHR, *Al Nashiri v. Poland*, No. 28761/11, 24 July 2014 (ruling of the Chamber, pending referral to the ECtHR Grand Chamber).

rights ramifications of the proposed intra-EU system, ranging from data protection and profiling-related issues to the overall lack of proportionality,[6] have proved no less sensitive, and were the primary reason for opposition against the proposed directive in the European Parliament in 2013.

The current calls by the European Commission and the Council for reactivating the PNR file are anchored in the wider framework of increasing EU efforts to counter terrorist threats, and are included in the recent Council conclusions on terrorism and border security.[7] The Strategic Guidelines advocate the development of the EU PNR system to help prevent radicalisation and extremism, and to address the phenomenon of 'foreign fighters'. The EU Counter-Terrorism Coordinator has urged the EU legislator to adopt the directive for the same reason. The elements that have attracted considerable criticism in the past, however, remain on the table.

Some of the fundamental rights considerations previously raised are inherent to any PNR system. Use of PNR data by law enforcement authorities to assess the risk posed by individual passengers amounts to profiling and is as such accompanied by risks of discrimination and 'false positive' matches. To be able to make any claim of proportionality, any potential future attempt to create an EU PNR system would benefit from an enhanced set of fundamental rights safeguards, such as those FRA presented in March 2014 as guidance for EU Member States that are considering setting up a domestic PNR system.[8] While not remedying all potential fundamental rights risks, introducing **clear and strict limitations on purpose, protection of personal data, increased transparency of the system towards passengers** and other safeguards identified by FRA would alleviate some of the system's weaknesses without compromising its primary security function.

---

6 See also FRA (2011), *Opinion on the proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime,* FRA Opinion 01/2011, Vienna, https://fra.europa.eu/en/opinion/2011/fra-opinion-proposal-passenger-name-record-pnr-directive.

7 Council of the European Union (2014), *Council conclusions on terrorism and border security*, Luxembourg, 6 June 2014.

8 FRA (2014), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, available at: http://fra.europa.eu/en/news/2014/fra-provides-guidance-member-states-setting-national-pnr-systems.

Foreign fighters and radicalisation

The phenomenon of EU citizens participating in armed conflicts outside the EU, while not entirely new, represents a pressing security risk given the nature of some of the conflicts involving EU 'foreign fighters' and the link to domestic religious radicalisation. It has become part of the PNR debate as well as the wider integration discourse. It is thus an issue that requires complex and innovative solutions going beyond security policy considerations, both at EU and Member State level. This, in turn, underpins the need to take fundamental rights into account when devising these solutions.

One of the core problems is the **lack of a clear definition of the problem**, that is, the stage at which a person can be considered a risk and targeted by security measures. Given that according to estimates more than 2,000 fighters holding EU citizenship are in Syria alone, effective surveillance of all returnees can be difficult, also due to a lack of resources. The much discussed preventive measure of confiscating the travel documents of selected individuals, or other steps preventing potential foreign fighters from leaving the EU territory, raise concerns related to the right to free movement as guaranteed in Article 45 of the EU Charter of Fundamental Rights. Taking into account the jurisprudence of the Court of Justice of the European Union (CJEU) and the ECtHR,[9] such preventive measures must be proportionate and subject to strict limitations and judicial review.

The complexity of the issue is further increased by the lack of tangible information about the actual extent and severity of the risk. The estimates of EU Member State nationals travelling to Syria and other conflict areas to directly engage in combat operations are difficult to verify. The reasons to visit the conflict area might be more complex, particularly in the case of persons originating from the area and thus having family in the region, which can lead to personal motivations. Even more importantly, the hypothetical degree of the security risk posed by a returned foreign fighter is also a highly individualised issue, and in the likely absence of specific knowledge about the person's conduct and experience during the conflict, any such judgement is prone to generalisation. It should also be borne in mind that EU Member State nationals are becoming increasingly involved in the conflict in the Ukraine, where political or nationalistic views rather than religious ones seem to be the chief motivation.

[9] See, for instance: CJEU, C-430/10, *Hristo Gaydarov v. Director na Glavna direktsia "Ohranitelna politsia" pri Ministerstvo na vatreshnite raboti*, 17 November 2011, or ECtHR, *Ignatov v. Bulgaria*, No. 50/02, 2 July 2009.

The nature of the conflicts in question and the fact that some of them attract persons of specific ethnic and/or religious backgrounds raises additional fundamental rights considerations. Monitoring persons suspected of criminal activity constitutes a legitimate preventive instrument, but measures that consist of **surveillance of a specific group or profiling of potential suspects based on ethnicity or religion *alone* create the risk of unacceptable discriminatory treatment**, both under the ECHR and the EU Charter of Fundamental Rights. While ethnicity or religion may be one of the factors considered when implementing security measures, they cannot be the sole or main reasons. [10] Besides constituting a breach of fundamental rights, discriminatory profiling can also lead to negative effects at community level such as loss of trust towards the authorities. Concentrating the attention and resources of law enforcement authorities towards a specific profile might also make it more difficult to detect threats that do not correspond with the given stereotype.

In this regard, **introducing or reinforcing existing cooperation with relevant communities in individual EU Member States will be necessary**, both to identify specific risks and as part of the overall effort to prevent an escalation of the problem in terms of further radicalisation. The Radicalisation Awareness Network set up by the European Commission in 2011 provides a useful platform for sharing best practices and it could have significant long-term effects if it also pays due attention to combating the root causes of radicalisation, which include discrimination and marginalisation. The May 2014 report of the EU Counter-Terrorism Coordinator contains some useful proposals in this regard, including the development of effective communication responses and appropriately targeted counter-narrative material, and offering alternative ways of engagement (such as in the relief effort) to particular young people who might otherwise consider participating in the armed conflicts.[11]

Finally, it needs to be emphasised that **radicalisation in the EU is not limited to specific ethnic or religious groups**. This is reflected in the diversity of perpetrators and motivations behind terrorist attacks in Europe in recent years. The Merah attacks in France and the killings in the Jewish Museum of Belgium seem to share common traits in their

[10] For more detail, see FRA (2010), *Towards more effective policing, understanding and preventing discriminatory ethnic profiling: A guide,* available at: http://fra.europa.eu/en/publication/2012/towards-more-effective-policing-understanding-and-preventing-discriminatory-ethnic.

[11] Council of the European Union (2014), *Foreign fighters and returnees from a counter-terrorism perspective, in particular with regard to Syria: state of play and proposals for future work*, 9280/14, Brussels.

antisemitic motive and the religious radicalisation of the perpetrators.[12] The National Socialist Underground (NSU) group in Germany, on the other hand, is believed to have murdered citizens of foreign origin for xenophobic reasons. Similarly, outside the EU, the Breivik attacks in Norway were driven by Islamophobia and anti-multiculturalism, extended to all advocates of a multicultural society.

In this context, statistics provided by Europol's most recent EU Terrorism Situation and Trend Report reveal a striking disproportion between the high proportion of persons arrested in connection with religiously inspired terrorism and the relatively low share of completed attacks that can be classified as religiously motivated. [13] Both the EU and Member States need to be continuously aware of these facts and be sensitive when developing security measures to avoid legitimising xenophobic reactions towards specific groups within European society.

Past FRA research has shown that discrimination plays a major role in the subjective feeling of unhappiness and social marginalisation. A comparative study published in 2010 focusing on the experiences of Muslim and non-Muslim youth in France, Spain and the United Kingdom revealed that **support for violence, both in its individual form and in the use of war and/or terrorism, is higher among young people who feel socially marginalised**. [14] Young Muslims reported having experienced discrimination and social marginalisation more often than non-Muslim youth, citing cultural background and religion as the most common underlying reasons. In addition, as evidenced by FRA research, the response of authorities towards minorities can contribute towards feelings of systematic social marginalisation. Some figures from the European Union Minorities and Discrimination Survey (EU-MIDIS), published by FRA in 2009, illustrate this. Some 11 % of survey respondents who identified as Muslim indicated that they had been a victim of what they considered to be a racially motivated crime in the 12 months preceding the survey; the overwhelming majority of them,

[12] At the same time, despite the background of the alleged perpetrator of the Belgian murders as a 'foreign fighter', the initial radicalisation of the perpetrators/suspects is in both cases being ascribed to their stay in prison, which steered the expert debate to whether enough attention is being paid to this environment.

[13] Among the 152 terrorist attacks reported by EU Member States in 2013, no attack has been specifically classified as religiously inspired terrorism. Europol's report, nonetheless, refers to several disrupted plots and two attacks that "appear to be linked" to religious radicalisation. Out of 535 persons arrested for terrorism-related offences in the EU, 216 (40 %) were arrested for religiously inspired terrorism, compared with 159 out of 537 persons (30 %) in 2012. For more information, see: European Police Office (2014), *European Union terrorism situation and trend report 2014*.

[14] FRA (2010), *Experience of discrimination, social marginalisation and violence: A comparative study of Muslim and non-Muslim youth in three EU Member States*, Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2012/experience-discrimination-social-marginalisation-and-violence-comparative-study .

however, chose not to report their experience of victimisation to the police, often referring to their lack of confidence that the police would be able to do anything about it. In addition, 40 % of Muslim respondents who had been previously stopped by the police believed that this was specifically due to their immigrant or minority status.[15] This lack of trust and feeling of insufficient protection not only contributes to the feeling of social marginalisation, but can also hinder the cooperation of law enforcement authorities with the relevant communities when it is most needed. Addressing discrimination and hate crime against Muslims should therefore be an integral component of policies that aim to prevent radicalisation and growth of extremism.

Large-scale surveillance

The EU was confronted with the Snowden revelations on large-scale surveillance while it was discussing an overarching reform of its own data protection framework and exploring the option to accede to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The revelations led to a series of responses by EU institutions. These responses primarily aim to review the security cooperation framework between the EU and the US, and the risks posed by discrepancies between the EU and US data protection regimes, but also to strengthen the efforts to update the EU internal privacy rules to the new challenges.[16]

At the same time, the large-scale surveillance revelations gave rise to questions as to the real extent of large-scale surveillance within the EU – questions that will continue to be asked as the **rapid development of information and communication technologies increasingly enables states to potentially access the private lives of their citizens online**. The debate is worldwide, as shown by the United Nations (UN) General Assembly Resolution on the Right to Privacy in the Digital Age, which was adopted in reaction to the revelations and calls on states to "put an end to violations of those rights and to create the conditions to prevent such violations".[17] In this context, it should be highlighted that the EU Strategic Guidelines for legislative and operational planning for

[15] FRA (2009), *EU-MIDIS Data in Focus Report 2: Muslims*, Luxembourg, Publications Office, http://fra.europa.eu/en/publication/2010/eu-midis-data-focus-report-2-muslims.

[16] See, for example: European Parliament (2013), *Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*, P7_TA(2013)0322; Council of the EU (2013), *Report of the Council of the European Union of 27 November 2013 on the findings by the EU Co-chairs of the ad hoc EU–US Working Group on Data Protection,* 16987/13; or European Commission (2013), *Rebuilding trust in EU–US data flows,* COM(2013) 846 final, Brussels, 27 November 2013.

[17] United Nations (2013), *The right to privacy in the digital age*, Resolution of the General Assembly of the United Nations of 18 December 2013.

the coming years within the area of freedom, security and justice contain no reference to the surveillance debate. Instead, they call for "intensifying operational cooperation while using the potential of ICT innovations". Although national security remains the sole responsibility of each Member State, EU competence to act to safeguard the application of EU law needs to be recognised.

Besides interfering with the right to private life (Article 7 of the Charter) and the protection of personal data (Article 8 of the Charter), large-scale surveillance of communication has potential implications for other rights, such as the freedom of expression and information (Article 11 of the Charter), and the right to an effective remedy and to a fair trial (Article 47 of the Charter). Perhaps the most troubling aspect of the surveillance debate, however, is the lack of transparency of the surveillance schemes, which has also been highlighted by Article 29 of the Working Party in its opinion on surveillance of electronic communications for intelligence and national security purposes.[18] While it is clear that secrecy is an essential element of the operation of intelligence services, the absence of transparency and sufficient information prevents individuals from accessing remedies and, particularly given the lack of effective oversight of intelligence services' activities across the EU, nullifies any efforts to impose public accountability upon these services.

Any reform of the Member States' surveillance frameworks therefore needs to take the **issues of increased transparency and democratic oversight of intelligence services** as their starting point. This includes reviewing the competences of current oversight and monitoring mechanisms. Where the system of oversight relies on parliamentary supervision, effective access to information and expertise is necessary to carry out sufficient scrutiny. The same applies to systems based on other mechanisms, such as those involving national data protection authorities or other external oversight bodies, also securing their independence. The EU should, to the maximum extent of its competence, play an active role in these processes. In this respect, findings of a current FRA project on national intelligence authorities and surveillance in the EU – focusing on fundamental rights safeguards and remedies – will be communicated to the European Parliament by the end of 2014.[19]

While the core debate on large-scale surveillance focuses on the activities of states and their agencies, the **role of the private sector should also be recognised and addressed**. Businesses in the information and

[18] Article 29 Data Protection Working Party (2014), *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 819/14/EN, 10 April 2014.

[19] See the website of the project at: http://fra.europa.eu/en/project/2014/national-intelligence-authorities-and-surveillance-eu-fundamental-rights-safeguards-and.

communication technology (ICT) sector act as providers of telecommunication services or online platforms that may be targeted by surveillance, but also, for example, as suppliers of technologies that can be used for surveillance purposes. UN Guiding Principles on Business and Human Rights emphasise that businesses should not only avoid causing or contributing to adverse effects on human rights through their own activities, but also seek to prevent such effects if they are otherwise directly linked to their operations.[20] It is important that the EU's response within the policy on corporate social responsibility, the ICT Sector Guide, includes the responsibilities of companies in the face of potential government requests for cooperation for law enforcement purposes among the duties to protect human rights. .[21] This responsibility is of course not limited to the ICT sector, and is equally applicable to other businesses ranging from airline operators to banks. With the growing importance of information and communication technologies in daily life and the corresponding reliance of state authorities on monitoring and surveillance of this environment, the ability of businesses to deal with government requests in a way compliant with fundamental rights is going to play a vital role.

Concerns over the fundamental rights compatibility of security measures that rely on gathering and storing communication data have also been voiced vis-à-vis instruments at the EU level. Most notably, the CJEU judgement on the Data Retention Directive confirmed the need to carefully assess the proportionality of measures that otherwise satisfy the "objective of general interest, namely the fight against serious crime and, ultimately, public security".[22]

Outlook

The proportionality between achieving a legitimate security interest and safeguarding fundamental rights needs to become a leading feature of the debate on the future of Europe's security, both at the EU and Member State policy level. The issue is not limited to the examples outlined above and is equally relevant in other areas, such as the tracking of financial transactions or cybercrime, where criminalisation of hate speech or incite-

[20] United Nations (2011), *Guiding principles on business and human rights*, http://business-humanrights.org/en/un-guiding-principles.

[21] European Commission (2013), *ICT Sector Guide on implementing the UN Guiding Principles on business and human rights*, Luxembourg, Publications Office, http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf. The European Commission published two other guides, aimed at employment and recruitment agencies, and oil and gas companies.

[22] CJEU, Joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014.

ment to terrorism encounters the freedom of expression.[23] In this context, the EU Cybersecurity Strategy represents a good starting point in highlighting that "cybersecurity can only be sound and effective if it is based on fundamental rights and freedoms as enshrined in the EU Charter of Fundamental Rights and EU core values."[24] What this statement means in practical terms needs to be addressed when looking at the interplay between security and fundamental rights.

In its 2013 Annual Report,[25] FRA called for the adoption of an internal EU strategic framework on fundamental rights that would integrate the interventions of the EU institutions, as well as the activities at the national, regional and local level into more structured cooperation, encompassing the earlier proposal by the European Parliament to launch a European fundamental rights policy cycle.[26] In the field of security, the existence of such a framework could facilitate a more coordinated debate on the compatibility of proposed measures with fundamental rights, provide viable alternatives, and help avoid complications both within the legislative process and in the subsequent implementation.

Finally, resolving the fundamental rights-security dilemma or, rather, introducing fundamental rights into the equation, is crucial for safeguarding the legitimacy of EU and Member States' security policies in the eyes of European citizens. The recent large-scale surveillance revelations have challenged people's trust in democratic institutions and in the role of the state in general. Discussions on measures aimed at the prevention of radicalism and extremism, including the issues of PNR and foreign fighters, are occurring in a precarious context in which certain groups within the European society feel unjustly targeted, which might further undermine their trust in the authorities and the trust between communities. Respecting fundamental rights and ensuring the proportionality of internal security policies is instrumental to regaining this trust and rebuilding confidence within the European Union.

---

[23] See, for instance, UNODC, *Comprehensive study on cybercrime (draft)*, Chapter 4.3, http://www.unodc.org/documents/20organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[24] European Commission (2013), *Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace*, p. 4, JOIN(2013) 1 final, Brussels, 7 February 2013.

[25] FRA (2014), *Fundamental rights: challenges and achievements in 2013. Annual report 2013*, Focus, Luxembourg, Publications Office, p. 7–20, https://fra.europa.eu/en/publication/2014/fundamental-rights-challenges-and-achievements-2013.

[26] European Parliament (2012), *Resolution of 12 December 2012 on the situation of fundamental rights in the European Union*, para. 20, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0500&language =EN&ring=A7-2012-0383.