Fundamental Rights Forum
connect.reflect.act

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Working group 19:

The right to freedom of expression and the right to privacy in the context of increased security concerns in Europe: Challenges and promising practices

Background

Currently, governments are dealing with a heightened level of security by increasing the collection and analysis of personal data, following violent attacks in Europe and other parts of the world. This applies equally to law enforcement authorities and national intelligence services. The 2015 European Agenda on Security and the Internal Security Strategy have paved the way for enhancing the exchange of data and the better use of the EU's large-scale databases and other communications platforms. These include the (future) EU's Passengers Name Records Directive, the 'Smart borders' package, the Schengen Information System (SIS II), Europol's European Counter Terrorism centre and its Internet Referral Unit. Moreover, enhanced cooperation between national intelligence and law enforcement services is being discussed in terms of data exchange. The impact of these measures on privacy and freedom of expression can be significant, particularly given the urgency with which they are being adopted.

On the part of data processing by intelligence services, FRA research has shown that Members States' laws do not provide clear and effective safeguards for protecting private life and the personal data of individuals. As a result there is a clear need for effective oversight systems. FRA research also mentions the impact on freedom of expression, such as the protection of journalistic sources or whistleblowing measures.

The EU has also finalised reforming its data protection rules. They aim to boost the individual's rights while allowing unhampered exchange of data between national law enforcement authorities. In addition, the re-negotiated EU-US Umbrella Agreement will pave the way for the exchange of law enforcement data while protecting personal data. However, several judgments from the Court of Justice of the European Union (CJEU) have demonstrated the importance attached to having a high level of privacy and data protection in the EU. European Court of Human Rights (ECtHR) judgments on secret surveillance measures have also highlighted the impact of such measures on freedom of expression and privacy. Accommodating freedom of expression and privacy, while maintaining security, raises many questions that need to be further discussed. Those measures should also be seen in the general context of implementing the Digital Single Market strategy as well as the political agreement on reforming the EU data protection rules, the recent adoption of the Network and Information Security Directive and the revision of the e-privacy Directive.

Objectives

This workshop explored the impact of security measures on privacy and freedom of expression. Law enforcement and intelligence laws and policies as well as measures to counter terrorism helped frame the discussion. References were made to case law of the ECtHR and the CJEU when applying the European Convention on Human Rights (ECHR) and the EU's Charter of Fundamental Rights. The workshop will feed into FRA's current and future work on surveillance and safeguarding fundamental rights.

Speakers

- Barbora Bukovská, Legal Director, Article 19
- Joseph Cannataci, UN Special Rapporteur on the Right to privacy, OHCHR
- Dunja Mijatović, Representative on Freedom of the Media, OSCE
- Joanna Cavan, Head, Interception of Communications Commissioner's Office (IOCCO)
- Katharine Sarikakis, Professor, Head Media Governance and Industries Research Lab, University of Vienna
- Mario Oetheimer, Head of Sector Information Society, Privacy and Data Protection, FRA

Main messages

1. Security and privacy are not mutually exclusive. It is a false dichotomy.
2. An impact is already visible – for example, on watchdog journalism, including the willingness to interact with journalists. The space to hold minority views is shrinking.
3. Lawmakers and regulators can safeguard key fundamental rights while preserving the security of individuals by ensuring legislative clarity, transparency and accountability. The culture of secrecy must be challenged. There is a need for effective remedies and robust oversight.

Next steps

- Policy makers should ensure legislative clarity by outlining a clear, legal and legitimate (linked to public participation) framework.
- Various actors should strive to raise awareness and a legal understanding of privacy and legal rights, remedies and security tools, but also limitations thereof, such as surveillance and data gathering. Such actors include governments, media, intelligence/security agents, civil society, and the education sector.
- Member States, private entities, and the technology expert community should create safe spaces for dissent.
- Oversight bodies should promote transparency through regular reporting and monitoring, including statistical data, compliance and the acknowledgment of failure.

- Member States should enhance and secure the independence of oversight bodies over intelligence agencies.
- Member States should secure effective and timely remedies for individuals.
- Member States, oversight bodies and independent experts should assess the impact and effectiveness of mass surveillance, especially prior to legislative reform.