Privacy and Surveillance

Background

As stated by the former UN Special Rapporteur for freedom of expression, David Kaye, in his Report on privacy and surveillance in 2019: "*we live in an age of readily available, easy to abuse and difficult to detect tools of digital surveillance*". Digital surveillance tools are ubiquitous in modern societies, although they are not often visible.

In recent years, in addition to the traditional threats that civil society organisations, whistle-blowers and human rights defenders face, digital technologies have added another layer. Surveillance possibilities against CSOs have grown exponentially in reach and scope due to the use of new digital tactics by states and other actors. These tactics can be used for both mass and targeted surveillance, online and offline. Tools of mass surveillance include monitoring electronic communications, CCTV, facial recognition, biometric databases, and drones. Targeted surveillance is also made possible by wiretapping devices and various forms of equipment interference techniques, such as malware and spyware.

As the capabilities of various forms of surveillance are increasing, so are the concerns about the protection of fundamental rights, in particular the rights to freedom of expression and to privacy. Potential impact on civil societies covers a large spectrum, from direct intimidation or restrictions, to indirect limitations such as self-censorship.

Mass surveillance, and arbitrary targeted surveillance of human rights defenders and CSOs because of their work, are both illegal under international human rights law. The right to privacy and freedom of expression are guaranteed and protected by international human rights law, including by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR), and can only be limited under very specific circumstances. However, many recent examples show how far rights can be eroded if technologically-driven challenges are not addressed. For instance, many measures taken by states to fight the coronavirus pandemic, including via limitation of certain rights during states of emergency, might put these safeguards under stress. In addition, some efforts have been made by the international community to limit the export of technologies for repressive use (the non-binding Wassenaar Arrangement on Export Controls).

In the EU, Article 7 of the Charter of Fundamental Rights of the EU guarantees all individuals 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 stipulates that an independent authority must regulate compliance with this right. Article 47 secures the right to an effective remedy. In recent years, increasing security pressures stemming from terrorist threats or the rising tide of cyber-attacks have triggered extensive reforms in several EU Member States in relation to the surveillance capacity of their intelligence services. In most Member States, legal safeguards are well established in the

legislation. Legal clarity, independent oversight and effective remedies, notably, are key to guaranteeing that surveillance techniques are used in fundamentally rights-compliant ways.

Objectives

1. Raise awareness of the threats of mass and arbitrary targeted surveillance tools for the general population, looking specifically at the threats to civil society, whistle-blowers and human rights defenders, as well as how surveillance impacts them and their work.
2. Reflect on existing EU and other international instruments and legislation to combat mass and arbitrary targeted surveillance.
3. Share best practices between civil society actors, including human rights defenders, on how they can combat arbitrary surveillance and protect themselves against the pressures and obstacles it generates.

Methodology

This working group will host one main thematic session (open to the general public) and two smaller interactive sessions: one open, and a closed one exclusive to human rights defenders. During the interactive sessions, the participants will discuss in smaller groups and build on their concrete experience to draw specific recommendations for the EU.

Main thematic session (public)

"Arbitrary mass and targeted surveillance: are we facing an irreversible process?"

10 December 2020, 14:30–16:30 CET

To respond to the issues discussed above, this session will examine in detail how human rights can be preserved when so many political activities and communications of CSOs and human rights defenders are surveilled by states, with few legal or technological constraints. The session will also seek to identify possible legislative, technological and policy solutions to respond to these problems.

Interactive session I (closed)

"Exchange between Human Rights Defenders: how surveillance technologies have impacted their human rights work"

9 December 2020, 16.30–18.00 CET

Which strategies and tactics have been the most successful for mitigating harm? The session will allow participants to discuss the types of surveillance technology and practices they have encountered; the effects this has had on their ability to carry out human rights work, and on their safety; and how they managed – for instance, which strategies and protection tools did they use to counter negative effects? Participants will reflect on recommendations for the EU and other multilateral institutions, the private sector and governments on how they can improve digital protection for human rights defenders.

Interactive session II (public)

"How to challenge surveillance through litigation?"

10 December 2020, 9.00–10.30 CET

Strategic litigation against surveillance – challenging surveillance practices through courts – has been deployed by a number of CSOs and human rights defenders around the world. However, there are significant barriers to successful litigation and formal complaints, including a lack of judicial oversight, effective remedies, causes of action, enforcement and data preservation. This interactive session will provide an opportunity for participants to exchange experience on litigating surveillance cases and share practical tips on how to be effective in this work.