Organization for Security and Co-operation in Europe
The Representative on Freedom of the Media
Teresa Ribeiro

Communiqué No. 1/2023

Communiqué by the OSCE Representative on Freedom of the Media On the Use of Digital Surveillance Technology on Journalists

For secure and democratic societies, journalists and other media actors must be able to perform their work freely and independently, without interference, restrictions, or fear for their own and other people's safety. The use of digital surveillance technology poses a significant threat to this fundamental principle: when journalists are targeted and monitored with such technology, they are seriously hampered in their ability to carry out their essential work.

The use of digital surveillance technology is on the rise, including on journalists. Numerous investigations, such as those led by the Pegasus Project and by specialized non-governmental organizations, have brought to light a troubling pattern: an increasing number of journalists worldwide have been targeted by surveillance software.

This fact compromises journalists' security and raises serious concerns about privacy breaches as well as chilling effects on media freedom. By monitoring journalistic communication and collecting confidential information and highly sensitive data, the users of such technology severely impact the media's ability to conduct their work safely, thereby posing a serious threat to media freedom, democratic societies and our common security.

Most importantly, the employment of digital surveillance technology hampers the media's ability to protect their communication, their investigations and their sources, a fundamental and well-established principle of journalism. The confidentiality of sources is central to journalists' ability to properly investigate stories, and to the protection of individuals and whistle-blowers who provide information to them. General Comment No. 34 to the International Covenant on Civil and Political Rights (ICCPR) provides that states parties "should recognise and respect that element of the right of freedom of expression that embraces the limited journalistic privilege not to disclose sources". The European Court of Human Rights, in a landmark ruling in 1996, ruled that the protection of sources is one of the basic conditions for press freedom. "Without such protection," the Court stated, "sources may be deterred from informing the public on matters of public interest," and the vital public-watchdog role of the press may be undermined.

Next, the use of digital surveillance technology not only leaves journalists with a profound sense of exposedness and vulnerability, it also increases the risks they face. Journalists who are targeted by digital surveillance technology may be subjected to harassment, false charges, unwarranted imprisonment, or physical violence. It also endangers those in proximity to the individual under surveillance.

An additional challenge is that both journalists and newsrooms now face yet another burden of having to allocate additional resources to safeguard against such threats, diverting valuable time and funds. On top of this, the detection of some digital surveillance technology proves to be a complex and demanding challenge, as sophisticated stealth tools coupled with covert constant monitoring makes it difficult to identify potentially compromised devices and establish secure communication.

Furthermore, the use of digital surveillance technology on journalists hampers the right of the public to receive independent, diverse, and public interest information. Surveillance affects communication between individuals, limiting their ability to access opposing, critical, or dissenting information, to investigate critical issues and disseminate information freely and securely. In essence, it creates uncertainty and an erosion of trust, leading to a shrinking civic space. This might be all the more poignant for groups that have been historically marginalized or structurally disadvantaged, including women, individuals with certain attributed identities, or freelance journalists, who may lack sufficient institutional resources or support to defend themselves against the impacts of such invasive technology. This exacerbates chilling effects on media freedom and risks of self-censorship, further undermining the presence of a plurality of voices.

The proponents of digital surveillance technology oftentimes defend its application with a call on national security. This is persistently problematic, especially as there is a concerning trend of misusing the concept of national security for political reasons, leading to the securitization of human rights. This practice often benefits those in power rather than addressing genuine security threats, ultimately undermining the protection of human rights and eroding democratic societies. The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, for instance, recognized in a 2019 report that many states have misused anti-terrorism powers, leading to human rights abuses. Similar trends were witnessed in the context of crises, including the recent COVID-19 pandemic and other disasters and conflicts, where the notion of national security and countering emergencies has, in some cases, been exploited to justify actions that may infringe upon human rights.

While there are exceptional cases in which resorting to digital surveillance technology may be justified to protect the life and security of individuals and society, its utilization must adhere to international human rights law and OSCE commitments and be in line with the principles of legality, legitimacy, and necessity and proportionality. This includes the obligations for any actor to avoid unlawful, illegitimate or arbitrary surveillance, and for states generally to respect, protect, and fulfil human rights, such as the right to freedom of expression. It is clear that, for the sake of upholding freedom of expression and media freedom, the threshold for using digital surveillance technology on journalists and other media actors is again much higher.

Relevant international obligations and OSCE commitments

Aside from posing a significant challenge to the right to freedom of opinion and expression, as enshrined in Article 19 of the ICCPR, digital surveillance technology also interferes with the right to “privacy, family, home or correspondence” and the right to be free from attacks “honour and reputation”, as protected under Article 17 ICCPR.

Already in 1989, during their Third Follow up Meeting to the Helsinki Conference, the participating States recognized the importance of source protection, stating that they will ensure that "journalists, including those representing media from other participating States, are free to seek access to and maintain contacts with public and private sources of information and that their need for professional confidentiality is respected".

In their 2018 OSCE Ministerial Council Decision on the Safety of Journalists, the participating States specifically warned against the use of surveillance on journalists, as constituting a risk for their safety, and recognizing that unlawful or arbitrary surveillance undermines the enjoyment of the right to freedom of expression and protection of privacy. In this Decision, participating States agreed "to refrain from employing unlawful or arbitrary surveillance techniques, noting that such acts infringe on journalists' enjoyment of human rights and could put them at potential risk of violence and threats to their safety".

In several Joint Declarations, the OSCE Representative on Freedom of the Media (RFoM) and other free speech mandate holders addressed some of the aforementioned issues. The 2018 Joint Declaration on Media Independence and Diversity in the Digital Age identifies surveillance as a technological threat to media freedom, while the 2019 Joint Declaration on Challenges to Freedom of Expression in the Next Decade calls on states to take immediate and longer-term steps to prohibit unlawful or arbitrary surveillance and the unaccountable trafficking in tools of the commercial spyware industry, in recognition of the substantial detrimental effects these can have on the exercise of freedom of opinion and expression. The 2022 Joint Declaration on Freedom of Expression and Gender Justice recognizes the gendered nature of surveillance, calling for the elimination of online gender-based violence. Finally, the 2023 Joint Declaration on Media Freedom and Democracy calls on states to adopt comprehensive measures for protecting journalists from violence and illegitimate surveillance. It also demands states to ensure the full protection of confidentiality of journalistic sources, both in law and in practice.

Conclusions

While state authorities have the unquestionable right, and even obligation, to protect the public and society's security, it is also unequivocally clear that digital surveillance technology must be employed with much caution. For the reasons mentioned above, the bar for the use of digital surveillance technology on journalists and other media workers must be set extremely high.

For this, the implementation of a robust legal framework and strict measures is crucial. This includes requiring effective, binding prior authorization of any surveillance measure on a journalist by an independent authority under judicial control, as well as ensuring that repressive measures are restricted in time and scope and are limited to only the most serious crimes. The use of digital surveillance technology must be carefully justified and embedded in a robust rule-of-law system, accompanied by a meaningful redress mechanism.

It is strongly recommended, therefore, that the participating States refrain from using digital surveillance technology on journalists unless there is a clear and imminent danger for the security of the public. In these cases, the use of such technology on journalists must be accompanied by aforementioned strict measures, be necessary in a democratic society and proportionate to achieve the legitimate aim.

Digital technology is developing at great speed and it provides tools that are ever more intrusive, with the possibility to silently bypass encryption and take complete control of the

device it is installed on, including camera and microphone, allowing it to covertly monitor the target's entire communications, including in the physical realm. It seems very hard to imagine that the use of such extremely pervasive and intrusive spyware on journalists and other media actors can ever be considered compatible with the principles we agreed upon in the OSCE region, including the right to freedom of expression, media freedom and privacy. The participating States are therefore strongly urged to completely refrain from its use on the media in all circumstances.

In light of all the aforementioned, the participating States should acknowledge the link between the growing use of digital surveillance technology and the increasing erosion of privacy and journalists' ability to conduct their work in the digital age, as well as the need for profound encryption tools and data protection legislation.

The participating States should prioritize the protection of journalists and media workers, and allocate sufficient resources to ensure their safety, including by promoting secure communications and encryption methods, and freedom from surveillance by non-state actors.

To avoid misuse of digital surveillance tools, the participating States should establish and implement strict export controls on digital surveillance technology, requiring human rights due diligence, transparency, accountability, and democratic oversight.

Teresa Ribeiro
OSCE Representative on Freedom of the Media
Vienna, 7 September 2023