

Encryption in the age of surveillance

Opening intervention by Dunja Mijatović
Council of Europe Commissioner for Human Rights

26 September 2023

First of all, I want to thank the organisers, our partners at EDRI, for inviting me to this important event. It is a great pleasure to participate, and I want to congratulate the team for their professionalism and long-standing commitment to safeguarding human rights and freedoms in the digital space. This, increasingly, is not easy, given the profound technical and legal expertise that is required and the high level of resistance which digital rights defenders sometimes meet, from policy makers and legislators, and from the powerful industry that is behind technological progress.

We live in the age of surveillance. Even our most private moments can end up in the public eye, as human rights defenders, activists, journalists and bloggers have painfully experienced, and as, in fact, anyone may painfully experience.

So, why is encryption important? I am not a tech expert but I understood quickly that encryption is a vital human rights tool. Effective end-to-end encryption is indispensable if we want to protect the security of communications for everyone on a network. We need encryption to ensure that no-one, including the platform provider, can read or alter messages, and to preserve the confidentiality between the sender and the recipient. Encryption is therefore indispensable for the effective protection of the right to privacy, freedom of expression, and many other human rights. In fact, the security of communications often also means the security of persons. I work closely with human rights defenders across Council of Europe member states, and I know that encryption is essential for their safety, and the safety of their families, their colleagues and networks, and their beneficiaries, namely the victims of human rights violations themselves. Journalists also rely on effective end-to-end encryption to protect the confidentiality of their sources and to perform their job, which is vital for democratic societies.

The struggle over online encryption is almost as old as the Internet itself. Already 10 years ago, my Office published an [Issue Paper on the rule of law on the Internet](#), pointing to the dangers of the growing technological capabilities of electronic mass surveillance and the possibility to build flaws and backdoors into security systems to weaken encryption. If anything, the struggle over encryption has become harder and more existential since then. Public debate is dominated by narratives of national security and terror, and human rights are being “securitised”. And while Council of Europe member states have a duty to protect the security of our societies, they also have the obligation to safeguard individual rights in line with the European Convention on Human Rights. Privacy is a fundamental human right and absolutely essential if we wish to live in dignity and security. It cannot be forfeited easily. States and private companies alike must therefore be very cautious in using our data and avoid any abuse.

Any interference with our right to privacy must be subject to strict legal rules and close democratic oversight. This includes, of course, the application of automated tools that have the power to monitor private communications. While such tools can help us fight grave crimes, including the very pervasive threat of online child abuse, we need a high level of transparency and accountability around the use of such scanning technologies, to ensure that it is human rights-compliant and meets high safety, necessity,

and proportionality standards. This is especially so, because there is a high risk that these tools will be repurposed, once introduced. There must be no general and indiscriminate access to the content of personal communications, neither by state authorities nor by companies: this would undermine the very essence of digital security in terms of privacy protection and human rights safeguards.

Fighting for the right to privacy, protecting encryption as a vital tool to ensure the security of communications, and promoting transparency and rule of law standards in the digital environment, is a hard and long struggle that is fought at the frontline by civil society organisations like EDRi. I want to thank you again for your efforts - the human rights community relies on actors like yourselves. Congratulations therefore on organising this important event and I wish you very productive discussions.