

EDRi members to EU institutions and governments: mass surveillance and encryption backdoors have no future in Europe!

On 13 February, the European Court of Human Rights delivered a landmark ruling in the [Podchasov v. Russia](#) case confirming that **indiscriminate retention of content and traffic data as well as encryption backdoors impair the very essence of the right to privacy** and cannot be considered necessary in a democratic society.

The EDRi network is the key digital rights voice in Europe. We amplify the **expertise of technology and privacy professionals** as well as the **lived experiences of people in vulnerable positions** like activists, young people, racialised groups and women in the digital spaces. Based on our **20-year experience in the field**, we know that **protecting people's privacy and data protection is essential for ensuring their safety**.

However, just a week after the Court's ruling, EU institutions are holding a **public consultation meeting** to look for tools and other "potential solutions" to the issues law enforcement encounter when seeking access to electronic data. The High Level Group (HLG) "Going Dark", chaired by the European Commission and the Presidency of the Council, is tasked to draft recommendations for future EU policies and legislation to increase law enforcement access to data.

The underlying objective of the HLG to achieve higher access to data for law enforcement goes in direct conflict with people's need for privacy and data protection to ensure their safety, as numerous pointed out by tech experts like EDRi. Therefore, the HLG should be dismantled altogether. Instead, **lawmakers should invest resources in advancing and promoting people's privacy to build safer digital spaces for all**.

"We understand this "Going Dark" initiative as an attempt to launder dangerous measures that would put everyone's online privacy and safety at risk and make them look acceptable in the public eye." - Chloé Berthélémy, Senior Policy Advisor, EDRi

EDRi along with Privacy International, Statewatch, IT-Pol Denmark and other EDRi members are taking part in the consultation to caution European law enforcement representatives that **any measure that tampers with encryption would create security and privacy threats to millions of people**, public institutions and the broader digital information ecosystem.

We will also share our great concerns regarding the **growing criminalisation across Europe of the use of encryption and other privacy and data protection tools**. We have seen prosecution cases turning the use of encrypted messaging services, even mainstream ones used by government officials, into proof of criminal intent.

With regards to the obligation put on internet service providers to generally and indiscriminately



retain all their users' data, EDRi members will point out to the European Commission that **several national laws are still in contravention of the Charter of Fundamental Rights and remind it of its duty as guardian of the treaties to bring Member States' legislation into line with EU law.** We will further warn against any future EU instrument that would not respect the boundaries set by the Court of Justice of the EU for the protection of fundamental rights against mass surveillance.

"The HLG wants to explore avenues for data retention compatible with the Charter. We would like to remind the HLG that for most Member States this means repealing their existing data retention laws." – Jesper Lund, Chairman of IT-Pol Denmark

We consider **the premise upon which the HLG works rests as entirely wrong.** The group's political agenda is guided by the concept of "security by design", which seems to aim at mainstreaming law enforcement access to data in the development of all technologies. If implemented, this principle would be **tantamount to mandating backdoors in all digital systems and would go against all human rights organisations' and technical experts' recommendations.**

"It is alarming that the HLG agenda seems to disregard that tools like encryption are crucial to ensuring privacy and security in the digital age, not just for journalists or activists, but essentially for everyone." Ioannis Kouvakas, Senior Legal Officer, Privacy International

Regardless of the results of this process, **the EDRi network will continue to fight against all attempts to legalise and implement unlawful and dangerous surveillance practices,** based on our long experience of mobilisation, litigation and advocacy against abuses of power.