La Quadrature du Net

To sign this op-ed contact us at: chiffrement@laquadrature.net

Encryption protects our rights, privacy is not a crime

5 june 2023

Encryption of communications is a common practice that ensures one's correspondence is not read by third parties outside the recipients. The right to encryption is an extension of our right to privacy, articulated by Article 8 of the European Convention of Human rights which gives each and every one of us the "right to respect for private and family life, home and correspondence".

Any person who wants to protect their messages can use encrypted communications – activists, human rights defenders, investigative journalists, young people bureaucrats, parents, friends and you – all use services such as WhatsApp and Signal that integrate secure encryption in their messaging services.

Through history, people all over the world used encryption to investigate corruption, to organise and challenge oppressive regimes, to create social change and to make our world a just space for all. As of 2022, over 2 bilion people use encryption every day, all over the world. The reason is simply: privacy empowers us all.

However, end-to-end encryption is currently under attack by prosecutors and legislators in France, the EU, the UK and the US.We are asked to choose, as a society: do we accept a future in which our private mail and communication can be intercepted anytime, in which we are treated as potential suspects?

A French tragic comedy: private therefore clandestine therefore terrorist?

La Quadrature du Net has recently revealed information related to the so-called "8 December" case law, in which 7 "ultra-left" people are under investigation for "terrorist criminal association". The case shows an unprecedented police will to criminalise how a prosecuted person uses digital technologies.

Upon inspection, the documents reveal that French law enforcement in fact criminalise perfectly legal and responsible digital security practices such as the use of encryption. In the past, secure encryption has been recommended and supported by many institutions such as the United Nation, the CNIL (French data protection authority), the ANSSI (French Cybersecurity agency), the ENISA, as well as the European Commission.

Besides criminalising the use of encrypted instant messengers, French prosecutors also incriminate the use of services such as Protonmail which ensures email confidentiality, the use of tools to protect one's privacy on the internet (VPN, Tor, Tails), the use of techniques to protect against GAFAM surveillance, the encryption of digital media or even the organization of training sessions on digital protection (cryptoparties).

Criminalising the right to privacy

By criminalising encryption and other security practices, the French police aims to construct a narrative that shows the 7 prosecuted people lived in "clandestinity". In the absence of a proven terrorist project, this "clandestinity" becomes proof of the hidden existence of an unprovable project.

We, journalists, activists, tech service providers or simple citizens who care about data protection in the digital age, are deeply outraged to see the French intelligence services and anti-terrorist justice feeding such an amalgam between basic data protection and terrorism.

We are outraged that necessary measures for the protection of personal data and privacy are seen as indications of "conspiratorial actions" of people allegedly living in the "cult of secrecy". We denounce the fact that a common and benevolent digital training on Tails - an operating system open to the general public and conceived for the protection of privacy and the fight against censorship - can constitute one of the "material facts" characterizing "participation in a group formed [...] with a view to preparing acts of terrorism".

Undermining encryption beyond France

Under pretext of terrorism, the French justice system incriminates a basic security practice. But the French example is not the only effort to undermine encryption.

In Brussels, the European Commission proposed in 2022 the CSAR (Child Sexual Abuse Regulation) proposal. Under the pretext of fighting child pornography, the draft law aims to force encrypted messaging providers to scan our encrypted messages. The proposal has been criticised by many voices, amongst which over 130 NGOs, espacially due to its lack of focus on other means to tackle this horrific crime, that can be more appropriate and less right-infringing for this fight. Recent leaks from the negotiations have revealed that countries such as Spain want to simply ban end-to-end encryption technology. The British “Online Safety Bill” and US’s "EARN IT” Act add to the worrying war against encryption.

While we ourselves use data protection tools on a daily basis, for academic research, source protection, political engagement or simply to protect our private exchanges and those of our loved ones, we are extremely concerned by these attempts to criminalize widespread and beneficial practices.

As promoters and defenders of fundamental freedoms in the digital world, La Quadrature du Net and its allies will continue to use and create privacy tools. We refuse to let intelligence services, judges or police officers criminalise our activity because it is considered “suspicious”. Our vision is to build a free, decentralised and empowering Internet, that enables a more dignifying society for all. The fight for encryption is the fight for a just and fair future.