19 March 2025

Subject: Protecting digital rights and freedoms in the Draft Legislation "Sortir la France du piège du narcotrafic"

Honourable Members of France's National Assembly,

The European Union is facing numerous and ever more complex cybersecurity threats[1], impacting individuals and communities, the private sector and public authorities, including defense forces.[2] In that context, it is essential that our devices and private communications remain safe and trustworthy. In this letter we want to highlight our concerns with some of the provisions proposed as part of the forthcoming legislation against "narcotrafic" and request you to ensure that privacy, data protection and other fundamental rights are upheld.

First, we understand that proposals on the table - concerning Article 8ter - include the obligation for service providers such as messaging services, email providers or video conferencing services to

1 ENISA, ENISA Threat Landscape 2024, 19 September 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

2 Andy Greenberg, China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers, WIRED, 13 February 2025, https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/
Meredith Whittaker, Taurus leak: When it comes to privacy, it's all or nothing, Netzpolitik, 23 March 2024, https://netzpolitik.org/2024/taurus-leak-when-it-comes-to-privacy-its-all-or-nothing/

actively assist French intelligence services and law enforcement authorities by **implementing technical methods that would undermine end-to-end encryption (E2EE).**

However, there is a wide scientific consensus that giving exceptional access to end-to-end encrypted data inevitably creates vulnerabilities that criminals and repressive regimes can exploit.[3] **Any vulnerability or 'backdoor' built in France will be exploited sooner than later by malicious actors around the world.[4] The security of everybody is therefore on the line.**

These measures also pose a serious threat to online privacy and thus, to the exercise of rights and freedoms protected by European human rights laws that depend on it. Last year, the European Court of Human Rights confirmed in its Podchasov v Russia ruling the vital importance of encryption in providing a robust defense against unlawful access.[5] It asserted that the mandate to decrypt end-to-end encrypted communications is a disproportionate measure and thus unacceptable in a democratic society.

Second, Articles 15ter and 15quater suggest to authorise the remote, secret activation of devices' microphone and camera in order to spy on their users. We understand that **the same measures have previously been declared anti-constitutional by the French Constitutional Council.** It is ill-advised to attempt legalising them once again. As spyware scandals across Europe have shown, **the unfettered tapping of people's devices endangers journalists, politicians, human rights defenders and the preservation of democratic society**.[6]

We, the undersigned 22 digital rights organisations from all around Europe, therefore **call on the French National Assembly to reject those articles, and any other measures which would break or undermine encryption, which create cybersecurity risks or likely affects the essence of the right to privacy and cannot meet the legal requirements of proportionality.**

As human rights advocates with expertise in technology, we would also like to underline the inherent limitations of any technological 'solution' to complex societal problems like drug trafficking, which require a comprehensive approach. Moreover, they should not be used as a pretext to legitimise the most intrusive and far-reaching surveillance methods.

---

3 Harold Abelson and al., Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, 6 July 2015 https://dspace.mit.edu/handle/1721.1/97690
So-called "Ghost proposals" involve the modification of the encryption system to enable a third-party listener to be silently added to encrypted conversations. It requires the alteration of the key distribution process to secretly distribute illegitimate keys to an external user, as well as modifications to the notification protocols to prevent users from knowing that unauthorised third parties have been granted access to their exchanges. This amounts to a backdoor and thus, introduces systemic security vulnerabilities that can be exploited by attackers. See EDRi, State access to encrypted data, October 2022, https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf

4 Bill Goodwin, Government agencies urged to use encrypted messaging after Chinese Salt Typhoon hack, *Computer Weekly*, 5 December 2024, https://www.computerweekly.com/news/366616972/Government-agencies-urged-to-use-encrypted-messaging-after-Chinese-Salt-Typhoon-hack

5 ECtHR, CASE OF PODCHASOV v. RUSSIA, 33696/19, 13 February 2024, https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

6 European Parliament Research Service, Spyware as a threat to fundamental rights and democracy in the EU, Briefing, PE 761.472, April 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf

We hope our comments help you in the final steps of the adoption of the legislation. We are at your disposal should you need further clarification.

Sincerely,

European Digital Rights (EDRi)[7]

Access Now
Asociația pentru Tehnologie și Internet (ApTI)
Aspiration
Bits of Freedom
Danes je nov dan, Inštitut za druga vprašanja
Deutsche Vereinigung für Datenschutz e.V. (DVD)
Državljan D / Citizen D
Digital Rights Ireland
Electronic Frontier Foundation
Electronic Frontier Norway (EFN)
Electronic Privacy Information Center (EPIC)
European Sex Workers' Rights Alliance (ESWA)
Hermes Center Hacking for Human Rights
Homo Digitalis
Irish Council for Civil Liberties (ICCL)
Initiative für Netzfreiheit
IT-Pol Denmark
Politiscope
Société Numérique, Suisse
Statewatch
SUPERRR Lab

7 EDRi is the largest network in Europe of civil society organisations working to defend and promote human rights in the digital era: https://edri.org/