Civic Space & Tech Brief

What is Encryption?

Encryption is a process that protects information by making it unreadable to those for whom it is not intended. It uses mathematical algorithms to transform information so it can be accessed only by those who have the secret code, the decryption key. Online communications can be end-to-end encrypted, where only the sender and recipient have the decryption key. Sharing or storing unencrypted information online is equivalent to sending a letter without an envelope and is accessible to anyone.

ENCRYPTION IS IMPORTANT BECAUSE IT:

- ✓ **Enables people to digitally share information** about their experiences, thoughts, and identities, without fear that cybercriminals or overreaching authorities may listen in. This relates to very practical issues, such as health and financial data, as well as to information about gender identities, sexual orientation, and minority status, as well as artistic expression.
- ✓ **Is vital for groups and individuals at particular risk** (e.g. of surveillance) such as human rights defenders, doctors, lawyers, whistle-blowers and minority communities. Journalists, in particular, cannot do their work without robust encryption, which shields their sources.
- ✓ **Makes our digital infrastructure resilient against attacks** and is thus key for protecting national security and the trustworthiness of many sensitive digital services, from finance to health.

COMMON RESTRICTIONS ON ENCRYPTION:

- ⊖ Blanket bans on encryption;
- ⊖ Criminalization of the use and sale of encryption hardware and software;
- ⊖ The use of "backdoors" which allow access to encrypted communications;
- ⊖ Mandatory registration and licensing of encryption tools;
- ⊖ Traceability requirements; and
- ⊖ General monitoring obligations for digital communications providers (e.g., general client-side scanning that requires scanning of message contents, including text and images, for similarities to a database of objectionable content before sending the message to the intended recipient).

> *"Mandated client-side scanning changes the ability of people to fully control the communication devices that are intrinsically connected to all facets of their lives and to limit what information those devices share."*
>
> *HC report on the right to privacy in the digital age A/HRC/51/17, 2022*

Weakening and restricting encryption → **Reduced safety and security for everyone and exposure to harmful use of data** → **Chilling effect, where people feel less free to share through digital technology**

STAND UP FOR HUMAN RIGHTS
#STANDUP4HUMANRIGHTS

UNITED NATIONS HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Civic Space & Tech Brief

STAND UP FOR HUMAN RIGHTS
#STANDUP4HUMANRIGHTS

UNITED NATIONS HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Human rights law protects privacy

> *The right to privacy is an expression of human dignity and is linked to the protection of human autonomy and personal identity*
>
> *HC report on the right to privacy in the digital age A/HRC/48/31, 2021*

The International Covenant on Civil and Political Rights art. 17 stipulates that ***"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence [...] and everyone has the right to the protection of the law against such interference or attacks."*** Restrictions on encryption may constitute interference and therefore must be provided by law, necessary and proportionate to achieve a legitimate objective.

Blanket restrictions on encryption are neither necessary nor proportionate. While limitations on encryption are often justified as needed for conducting criminal investigations (e.g. in the context of protecting children from sexual exploitation and abuse), overbroad restrictions would not meet the proportionality threshold and rather make everyone vulnerable to unauthorized and malicious intrusions. Further, criminal investigations can rely on alternative measures including better-resourced traditional policing and metadata analysis.

Business enterprises, under the UN Guiding Principles on Business and Human Rights, **have a responsibility to respect human rights** and to prevent and mitigate adverse human rights impact in the design, development, or use of digital technologies, **including encryption technologies**. This responsibility applies throughout an enterprise's activities and relationships, including in dealings with Governments.

- **Encryption protects privacy, and the human right to privacy in turn protects encryption.** States across the world have recognized the right to privacy as part of international human rights law (IHRL). Any regulation should be anchored in IHRL and follow the three-fold test of legality, necessity and proportionality.

- Business enterprises providing communication tools have a **responsibility to equip users with safety tools** and inform them in the event of possible third-party intrusion.

- National laws should explicitly allow **individuals to protect the privacy of their digital communications by using encrypted technology,** such as VPNs and messaging applications.

- **Blanket prohibitions or criminalizing of encryption** are not necessary or proportionate and **jeopardize human rights.** Access to encrypted technology is critical in emergencies and crises.

- **Mandatory general client-scanning** should be avoided. It undermines privacy and human rights and creates vulnerabilities that third parties can exploit, weakening everyone's safety and national security.

- **Interference with encryption** of private communications of individuals **should only be carried out when authorized by an independent judicial body** on a case-by-case basis, and if strictly necessary for the investigation or the prevention of serious crimes, threats to public safety or national security.