

L'Europa alla prova del Chat Control: la cifratura end-to-end come fondamento della libertà digitale



Luca Cadonici
Firenze, 23 ottobre 2025

e-privacy XXXVII (2025)
Misurare l'Umano? Dal Vitruviano all'Algoritmo

Europol vs E2EE

21/04/2024

NEWS

European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out

Downloads ▾

Part of the EU Policy Cycle - Impact ▾



Europol vs E2EE

21/04/2024

- On **April 2024**, **Europol** and **European police chiefs** are calling for industry and governments to take urgent action to limit **end-to-end encryption (E2EE)**.
- In a joint statement release, they criticized the strict privacy measures that tech companies like **Meta** are implementing for their **messaging services**.

Joint Declaration of the European Police Chiefs

We, the European Police Chiefs, recognise that law enforcement and the technology industry have a shared duty to keep the public safe, especially children. We have a proud partnership of complementary actions towards that end. That partnership is at risk.

Two key capabilities are crucial to supporting online safety.

First, the ability of technology companies to reactively provide to law enforcement investigations – on the basis of a lawful authority with strong safeguards and oversight – the data of suspected criminals on their service. This is known as 'lawful access'.

Second, the ability of technology companies proactively to identify illegal and harmful activity on their platforms. This is especially true in regards to detecting users who have a sexual interest in children, exchange images of abuse and seek to commit contact sexual offences. The companies currently have the ability to alert the proper authorities – with the result that many thousands of children have been safeguarded, and perpetrators arrested and brought to justice.

[https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint Declaration of the European Police Chiefs.PDF](https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint%20Declaration%20of%20the%20European%20Police%20Chiefs.PDF)



What is E2EE?

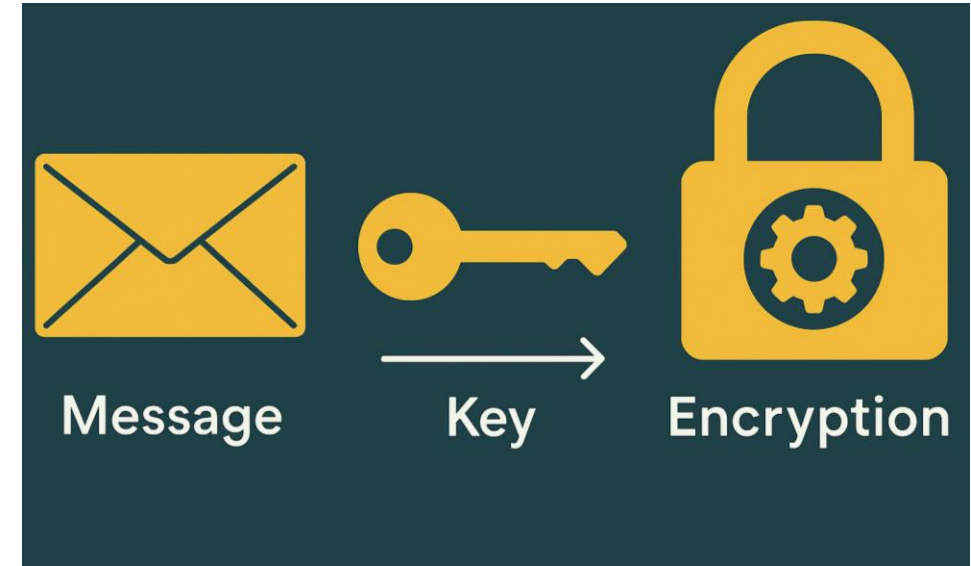
A brief overview
on encryption

Encryption

Encryption: the process of **converting data** (*plaintext*) into an unintelligible form (*cyphertext*) to prevent **unauthorized access**.

Encryption key: a piece of information used to encrypt and decrypt data during the encryption and decryption processes, respectively.

Encryption Algorithm: a mathematical or logical procedure used to encrypt and decrypt data.



Encryption

Encryption Type

aes-256-cbc

Encryption Algorithm

Hello world!

Plaintext

mobileforensics

Passphrase/encryption key

Generate passphrase

Encrypt

Your input was encrypted using aes-256-cbc and the passphrase you supplied, then base64 encoded. The result is below.

Copy

U2FsdGVkX1/Hk/tNLN+BCS08YTLcu8WzU6klrFfmuwo=

Cyphertext

Use the [decrypt tool](#) to decrypt this value, or use [OpenSSL 1.1.0](#) on your local computer.

<https://encrypt-online.com/>

End-to-End Encryption

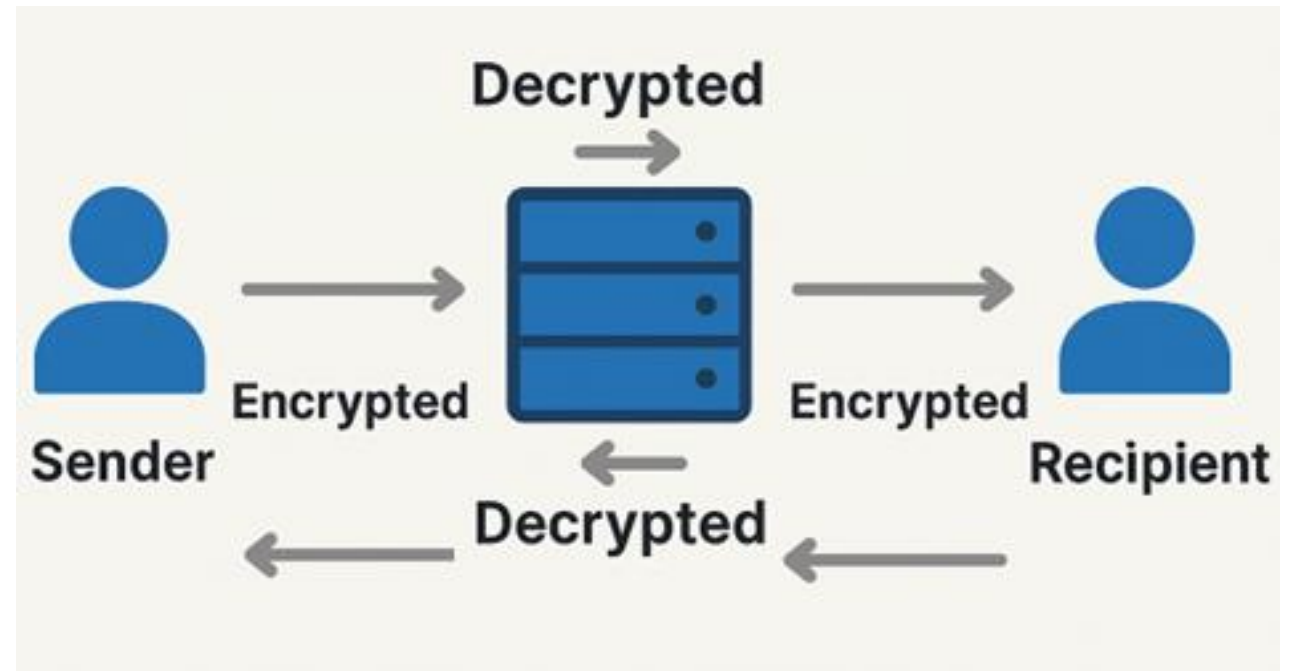
- **End-to-End Encryption (E2EE)** is an encryption mechanism that ensures data is **encrypted by the sender** and can only be **decrypted by the intended recipient**.
- This means that **no third party**—including **service providers, servers, or governments**—can **access the content of the communication**, since **only the end users hold the decryption keys**.
- Apps like **WhatsApp** and **Signal** use **E2EE** to protect **messages, calls, and files**.
- Data is encrypted on the **sender's device** and **decrypted only on the recipient's device**, making it **unreadable** even to **service providers facilitating the communication**.



Server-based encryption

Without **E2EE**, a message is typically **encrypted**:

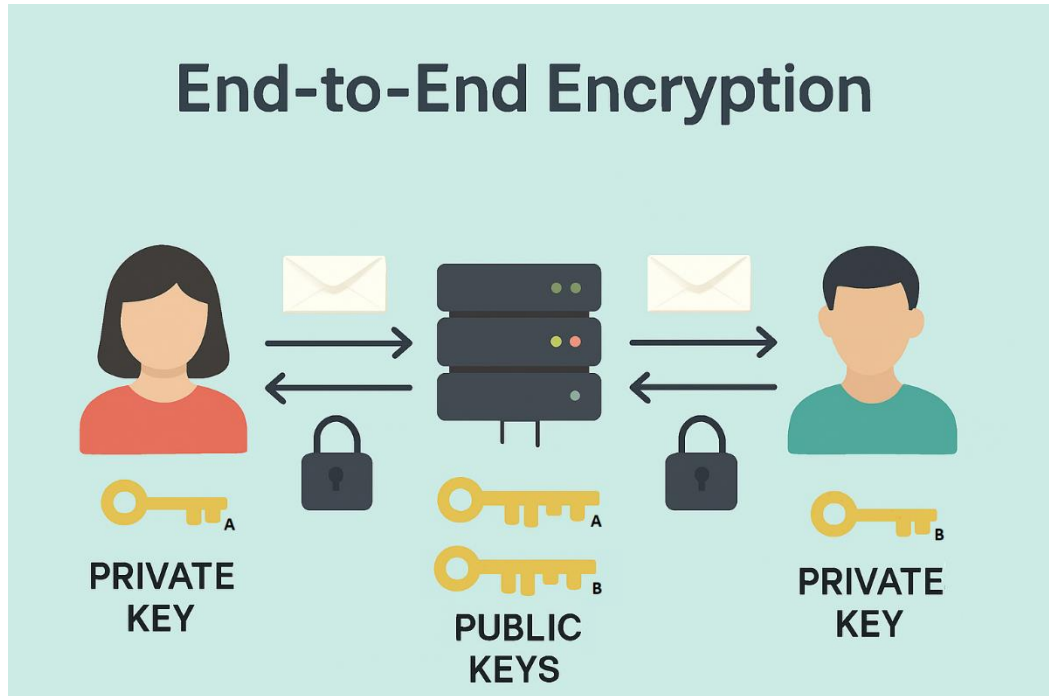
- during transmission from the **sender** to the **provider's server**
- from the **server** to the **recipient**
- However, the message is usually **decrypted** temporarily on the provider's server before being **re-encrypted** and **forwarded**.



End-to-End Encryption

E2EE is different because it is **impossible for anyone in the middle to decrypt the message**:

- **Messages are encrypted on the sender's device** using the recipient's **public key**
- They remain encrypted while in transit and are only decrypted on the recipient's device using their **private key**
- **Plaintext is never exposed to the provider's servers**



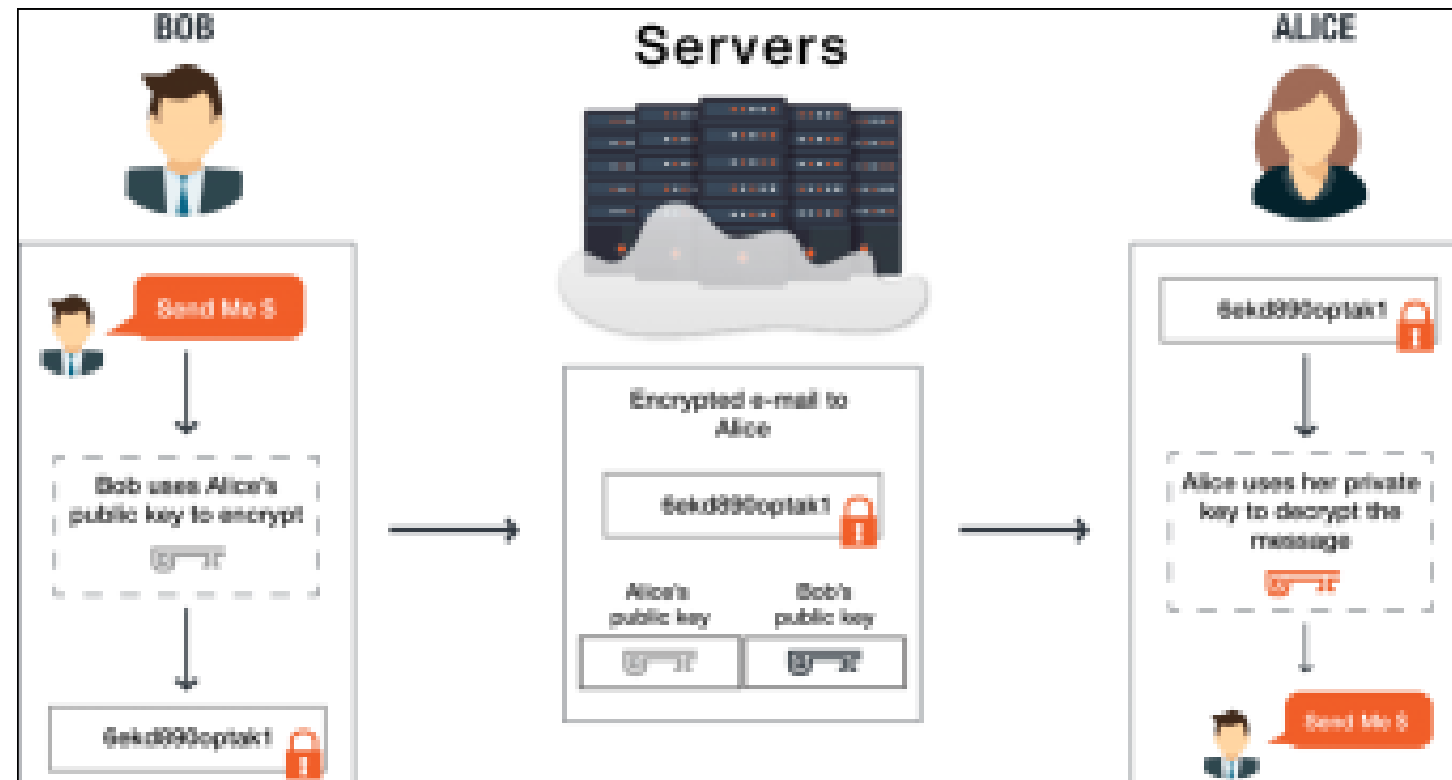
End-to-End Encryption

E2EE uses **public key cryptography**, where each user has:

- a **public key** (stored on **company servers**)
- a **private key** (kept secret on **user device**)

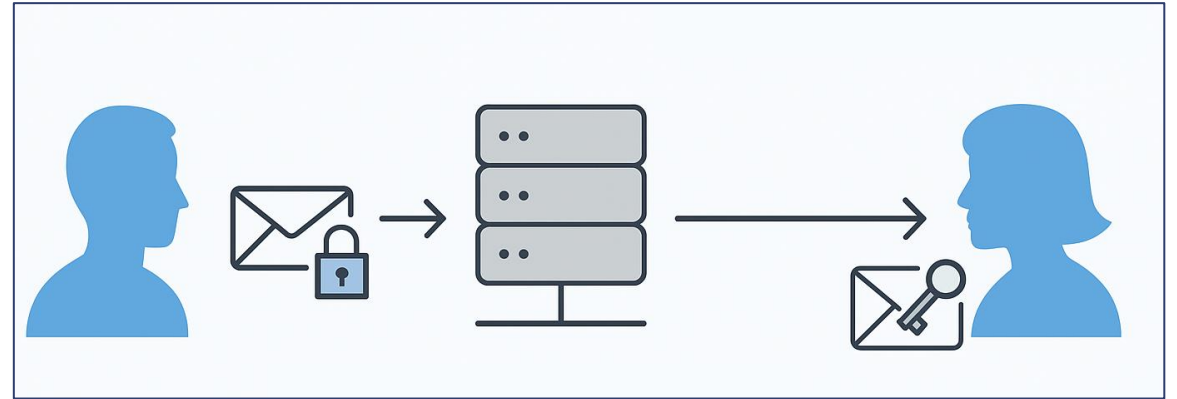
The **two keys** are mathematically linked:

anything encrypted with the public key can only be **decrypted** with the corresponding **private key**.



End-to-End Encryption

- The provider's server acts only as a **relay**, forwarding the **encrypted message (ciphertext)**.
- This ensures the data stays secure against cyberattacks targeting server
- Even if the **provider is compromised**, the data remains **protected**.
- Since only the recipient holds the private key, **service providers cannot decrypt messages**—even if requested to do so from **Governments or LEAs**.



E2EE and Lawful Access: A Structural Conflict?



E2EEE and lawful access

Legal and Ethical Tensions:

- Privacy advocates defend **E2EE** as essential for **human rights**.
- **LEAs** argues it creates “warrant-proof” **zones**.

Investigators cannot access message content from service providers.

Even with a warrant, platforms using **E2EE** could not provide **plaintext data**.

This tension has also played out in legal battles, yielding conflicting outcomes worldwide.



Facebook Messenger (Nevada - 2024)

On **December 2023** Meta has started rolling out default **end-to-end encryption** for **personal messages** and **calls** on **Messenger** and **Facebook**.

In **February 2024**, the State of **Nevada** is seeking an emergency restraining order to prevent Meta from implementing **end-to-end encryption** on **Facebook Messenger** for all **underage users** in the state.

The request for a **temporary restraining order** is part of a lawsuit filed by the **Nevada Attorney General**, who accuses Meta's products of being deceptively designed to create addiction in users.



23 MAR AT 17:04

Esatto!

Sent

🔒 Messenger upgraded the security of this chat. Messages and calls are secured with end-to-end encryption. [Learn more](#)

Facebook Messenger (Nevada - 2024)

A privacy advocacy coalition including **Signal**, and **Mozilla** filed an **amicus brief** opposing Nevada's **attempt to block end-to-end encryption** for minors:

- **End-to-end encryption** is a **fundamental tool** for protecting online privacy and security, especially for minors.
- **Blocking encryption does not eliminate abuse**; it instead exposes young people to new risks and weakens existing protections.
- **Investigations remain possible even with encryption**, through **user reports**, **access to devices**, and other data collected by **Meta**.
- A **recent study** confirms that **content-oblivious investigative methods** in **detecting online abuse** such as **user reporting** and **metadata analysis**, are often more effective.
- The **European Court of Human Rights** recently struck down a similar **Russian law**, deeming it **incompatible with human rights** (Case of Podchasov vs Russia).

BREF

CHRISTOPHER M. PETERSON, ESQ. (13932)
AMERICAN CIVIL LIBERTIES
UNION OF NEVADA
4362 W. Cheyenne Ave.
North Las Vegas, NV 89032
Telephone: (702) 366-1226
Facsimile: (725) 210-6328
Email: peterston@aclunv.org
Attorney for Amici Curiae

JENNIFER STISA GRANICK, ESQ.*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
425 California St., 7th Fl.
San Francisco, CA 94104
Telephone: 415-343-0758
Email: jgranick@aclu.org
**Pro hac vice forthcoming*

DISTRICT COURT CLARK COUNTY, NEVADA

STATE OF NEVADA,
Plaintiff,

vs.

META PLATFORMS, INC. f/k/a
FACEBOOK, INC.,
Defendant.

Case No. A-24-886110B
Dept. No. XXXI
Hearing Not Requested

Brief of Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Nevada, Electronic Frontier Foundation, Riana Pfefferkorn, Access Now, Center for Democracy and Technology, Fight for the Future, Internet Society, Mozilla Corporation, and Signal Messenger LLC, In Support of Defendant Meta Platforms.

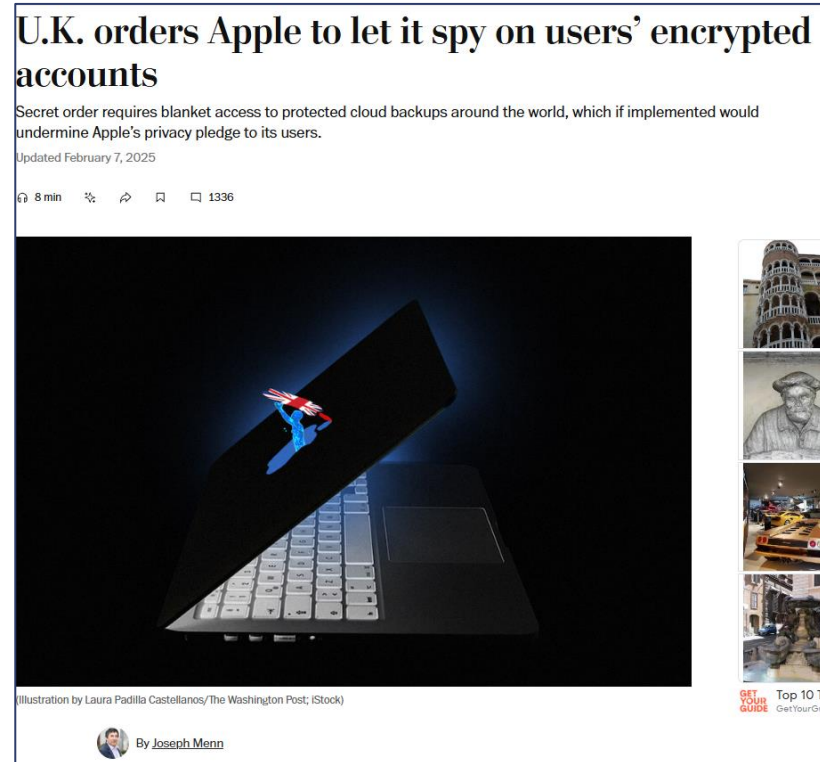
<https://www.eff.org/document/nevada-v-meta-amicus-brief>

Pfefferkorn, R. (2022). *Content-oblivious trust and safety techniques: Results from a survey of online service providers*.

Journal of Online Trust and Safety, 1(2). <https://doi.org/10.54501/jots.v1i2.14>

Apple - UK (February 2025)

- Security officials in the United Kingdom have demanded that Apple create a **backdoor** allowing them to retrieve all the **E2EE content** any **Apple user worldwide** has uploaded to the **cloud** – so not just for **U.K.** users, but for international users as well.
- Advanced Data Protection (ADP)** is an **optional Apple** feature that extends **E2EE** to data in iCloud, making it accessible only to you on your trusted devices.





Advanced Data Protection

iCloud encrypts your data to keep it secure. Advanced Data Protection uses end-to-end encryption to ensure that the iCloud data types listed here can only be decrypted on your trusted devices, protecting your information even in the case of a data breach in the cloud.

[Learn how encryption is used.](#)

Because Apple will not have the keys required to recover your data, you will be guided through verification of your recovery methods in case you ever lose access to your account.

 Device Backup

 Messages Backup

 iCloud Drive

 Notes

 Photos

 Reminders

 Safari Bookmarks

 Siri Shortcuts

 Voice Memos

 Wallet Passes

[Turn On Advanced Data Protection](#)

Some sensitive data, such as your saved passwords, and data from Health and Maps, are already protected using end-to-end encryption.

Apple - UK (February 2025)

- **Advanced Data Protection (ADP)** no longer available to new U.K. users
- Existing users will be required to disable **ADP**
- Apple: *“We have never built, and never will build, a **backdoor**”*



Apple can no longer offer Advanced Data Protection in the United Kingdom to new users

Here's what it means.

We are deeply disappointed that our customers in the UK will no longer have the option to enable Advanced Data Protection (ADP), especially given the continuing rise of data breaches and other threats to customer privacy. Apple remains committed to offering our users the highest level of security for their personal data and we are hopeful that we will be able to do so in the future in the United Kingdom.

[As we have said many times before](#), we have never built a backdoor or master key to any of our products or services and we never will.

- Withdrawing [Advanced Data Protection](#) from the UK will not affect the [14 iCloud data categories](#) that are end-to-end encrypted by default. Data like iCloud Keychain and Health remains protected with full end-to-end encryption.
- Our communication services, like iMessage and FaceTime, remain end-to-end encrypted globally, including in the UK.
- Users in the UK who have not already enabled Advanced Data Protection will no longer have the option to do so. That means the [9 iCloud data categories](#) covered by ADP will be protected by Standard Data Protection, and UK users will not have a choice to benefit from end-to-end encryption for these categories: iCloud Backup; iCloud Drive; Photos; Notes; Reminders; Safari Bookmarks; Siri Shortcuts; Voice Memos; Wallet Passes; and Freeform.
- For users in the UK who already enabled Advanced Data Protection, Apple will soon provide additional guidance. Apple cannot disable ADP automatically for these users. Instead, UK users will be given a period of time to disable the feature themselves to keep using their iCloud account.
- Advanced Data Protection continues to be available everywhere else in the world.

Published Date: February 24, 2025

<https://support.apple.com/en-us/122234>

EU Regulation on Child Sexual Abuse – CSA Regulation "Chat Control" (2022 – currently under discussion)

- **Proposed on 11 May 2022** by EU Commissioner for Home Affairs, Ylva Johansson
- **Official Objective:** Prevent and combat **child sexual abuse online** within the EU
- The goal was to **require online service providers to detect, report, and remove child sexual abuse material (CSAM)**.
- The proposal also sought to **prevent grooming practices**—the online solicitation of minors for sexual purposes.
- It further included measures to **enhance support for victims** of child sexual abuse.
- Known by critics as **“Chat Control”** because it raises significant concerns over privacy and freedom of communication.

October 2025: As member states failed to reach an agreement, the planned vote of the **Council of Europe** scheduled for **14 October 2025** will not take place. A **revised draft** may be introduced later by **Denmark** or another **Presidency**.



EU Regulation on Child Sexual Abuse – "Chat Control"

(2022 – currently under discussion)

- **The CSA Regulation** establishes the **principle of technological neutrality**, stating that no technology will be favored or excluded if it meets the legal requirements. (recital 4)
- **End-to-end encryption** is not prohibited; it is recognized as an **essential tool** for ensuring communication confidentiality. (Chapter II)
- However, a **court may issue a detection order**, requiring **service providers to implement tools** to identify abusive content. (Art. 7, 8)
- These technologies must ensure **no compromise of confidentiality** and **no potential for misuse**. (Art. 10)
- Each Member State shall designate a *Coordinating Authority* responsible for **requesting, monitoring**, and supervising **detection orders** and for cooperating with the EU Centre. (Art. 25, 26)
- To support this approach, an **EU Centre to Prevent and Counter Child Sexual Abuse will be created** to facilitate the implementation of the Regulation and **provide free detection technologies**, theoretically compliant with **EU data-protection law**. (Art. 26)

The Regulation explicitly introduces the concept of **detection orders** and **detection technologies**, defining the technical means that may be used under **judicial authorization** to identify CSAM or grooming activities. (Art. 7, 10, 12).

CSA Regulation - Detection Orders (Art. 7)

Detection orders are **binding decisions** issued by a **judicial** or **independent administrative** authority of the Member State, at the request of a **Coordinating Authority**, requiring **online service** providers to deploy technologies that detect **child sexual abuse material (CSAM)** or child solicitation on their platforms.

Preconditions:

- Coordinating Authority conducts investigations and risk assessments.
- Provider and the EU Centre are consulted before issuance.
- Provider submits an implementation plan including technologies and safeguards.

Issuance criteria:

- Significant risk that the service is used to disseminate known or new CSAM, or for child solicitation.
- Proportionality: benefits outweigh negative impacts on rights and interests.

Evidence base:

- risk assessments
- mitigation measures
- provider's implementation plan and opinions of the EU Centre and data protection authority.

Types of orders:

- Known CSAM → evidence of past or ongoing dissemination.
- New CSAM → risk and evidence within the past 12 months.
- Child solicitation → applies to interpersonal communication services with demonstrated risk.

National Coordinating Authorities (Art. 25 – CSA Regulation)

The **National Coordinating Authorities** are the cornerstone of the **CSA Regulation's governance model**, ensuring that **detection orders** and **enforcement measures** remain legally justified, proportionate, and privacy-compliant at the national level.

- Each EU Member State must designate or establish a **National Coordinating Authority** to implement the CSA Regulation. (Art. 25 §1)
- Acts as the **central contact point** for risk assessment, coordination, and cooperation with judicial or administrative bodies. (Art. 25 §1–2)
- **May request the issuance of Detection Orders** when there is a significant risk that a service is being misused for **CSAM** or **grooming**. (Art. 6–7, 25 §3)
- Ensures oversight of compliance with detection orders and protects users' privacy and data rights. (Art. 6 §3, Art. 7 §1 e)
- Operates **independently** and **impartially**, without **external** or **political interference**. (Art. 25 §2)
- Collaborates with the **EU Centre** to exchange technical data, coordinate detection efforts, and align national practices. (Art. 26)
- Must issue annual **transparency reports** on **national implementation and enforcement actions**. (Art. 25 §5)

EU Centre to Prevent and Counter Child Sexual Abuse (Art. 40)

The **EU Centre** is the **central body** responsible for supporting Member States and coordinating the EU-wide implementation of the **CSA Regulation**.

It ensures that **detection, reporting, and prevention measures** are consistent, lawful, and respectful of fundamental rights across the Union.

Central Hub: Coordinates cooperation between **National Coordinating Authorities, service providers, and EU institutions.**

Support to Enforcement: Assists national authorities in executing **Detection Orders**

Operational Coordination: Provides a platform for information exchange, best practices, and technical training.

Data Collection & Analysis: Maintains **secure databases of indicators of CSAM and grooming patterns** to assist investigations.

Databases of Indicators (Art. 44)

- The EU Centre creates, maintains, and operates three **databases of indicators** for:
 1. known CSAM
 2. new or unidentified CSAM
 3. child solicitation
- Each database contains:
 - **Relevant digital identifiers** to support detection (The Regulation does not explicitly mention “hashes”)
 - A list of uniform resource locators compiled by the **EU Centre**
 - Additional information to distinguish between **images, videos, and text**, and to identify **language patterns** linked to child solicitation.
- Indicators are generated solely from **verified material** provided by national **coordinating authorities** or courts.
- The Centre also maintains records of all **submissions** and **generation processes** for as long as related indicators remain in the databases.

Technologies, information and expertise (Art. 10, 50)

- The EU Centre makes available **technologies** that service providers can acquire, install, and operate free of charge to execute **detection orders**.
- Use may be subject to reasonable licensing conditions where relevant.
- The Centre compiles and maintains lists of such **approved technologies**.
- Technologies must comply with **Regulation requirements**, particularly Article 10(2).

Providers of hosting and communication services must execute **detection orders** by installing and operating technologies to identify known or new **CSAM** or child solicitation, using indicators from the EU Centre.

Providers may **use EU Centre technologies free of charge** but are **not obliged** to adopt specific tools as long as regulatory requirements are met.

Technologies must be:

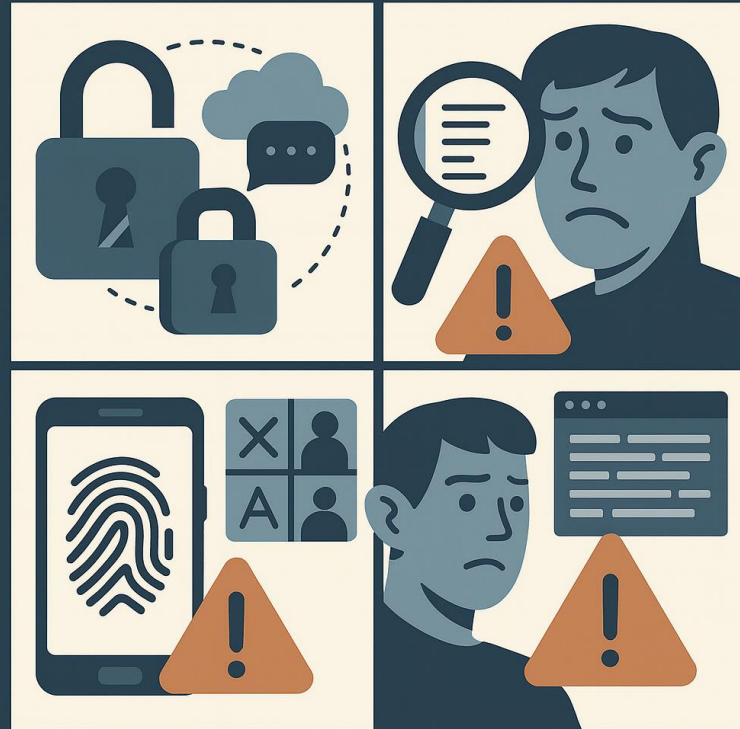
- **Effective** in detecting CSAM or solicitation
- **Minimally intrusive** and privacy-preserving
- **Accurate and reliable**, minimizing false detections

Providers must:

- Use technologies **only for detection purposes**
- Ensure **data protection and internal safeguards** against misuse
 - Maintain **human oversight** and error handling
 - Offer a **user complaint mechanism** and inform users transparently
- Notify the **Coordinating Authority** before implementation and include findings in periodic reports

User notification is allowed only when law enforcement confirms it won't interfere with investigations.

CSA Regulation: Main Risks and Concerns



CSA Regulation – Main Risks and concerns

While the goal of protecting children is legitimate, *Chat Control* risks creating a **permanent infrastructure of digital surveillance**, fundamentally altering the balance between **security and privacy** in online communication.



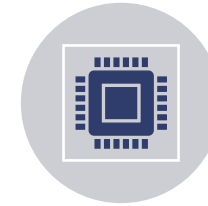
**END-TO-END ENCRYPTION
AT RISK:** ENFORCING
CONTENT DETECTION
WOULD REQUIRE **ACCESS
TO DATA BEFORE
ENCRYPTION**,
UNDERMINING ONE OF
THE CORE PILLARS OF
DIGITAL SECURITY.



**MASS SURVEILLANCE
POTENTIAL:** SYSTEMATIC
**SCANNING OF PRIVATE
COMMUNICATIONS**
COULD LEAD TO
GENERALIZED
MONITORING OF ALL
USERS.



**FALSE POSITIVES AND
ERRORS:** DETECTION
TOOLS SUCH AS HASHING,
FINGERPRINTING, AND AI
MODELS INEVITABLY
GENERATE MISTAKES
WHEN APPLIED TO
BILLIONS OF MESSAGES.



SCOPE EXPANSION: ONCE
IMPLEMENTED, SCANNING
TECHNOLOGIES COULD BE
REPURPOSED FOR OTHER
FORMS OF CONTENT
**MONITORING OR
CENSORSHIP**.

CSA Regulation - Client-side Scanning

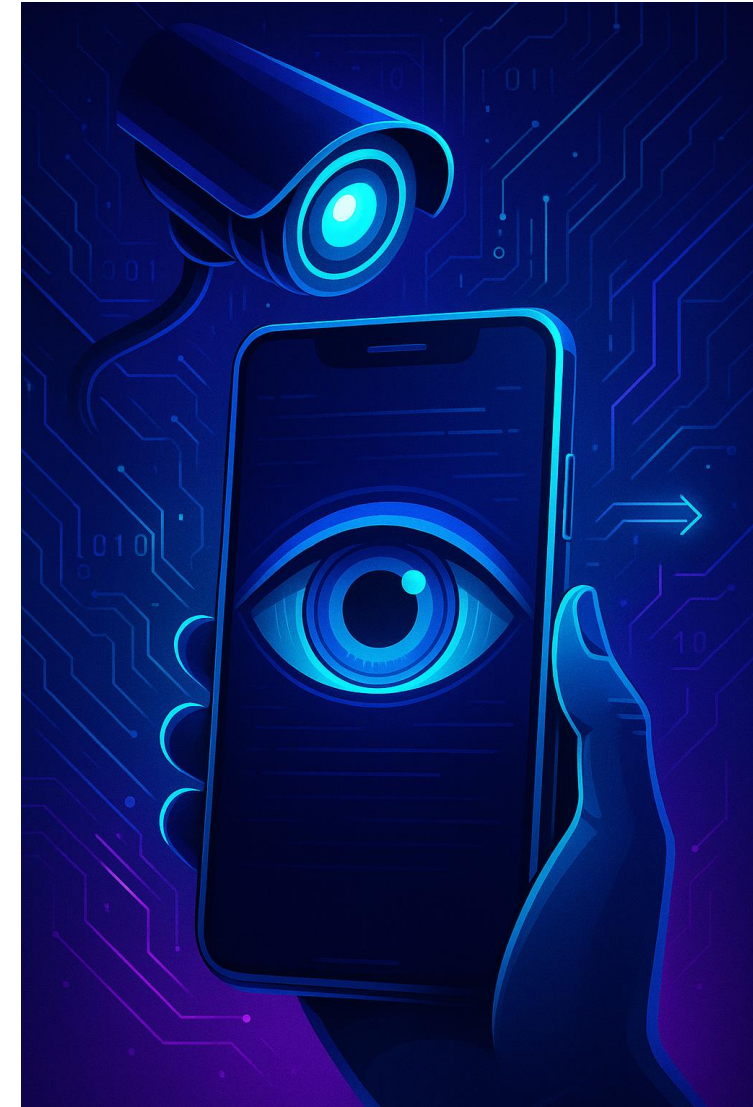
Fundamental Rights Perspective (CSA Fundamental Rights Analysis §3)

«Detecting “grooming” may have a positive impact on the rights of potential victims by preventing abuse. Yet, it is also the most intrusive detection process, since it involves automatic scanning of interpersonal communications. Such scanning is often the only possible way to detect grooming and relies on pattern recognition rather than semantic understanding. Technologies are becoming more accurate over time, but human oversight remains essential.»

- The CSA Regulation explicitly mention automatic scanning of interpersonal communications.
- Through **Articles 7 and 10**, it requires providers to **deploy detection technologies** even within **end-to-end encrypted (E2EE)** environments.

Technical Implication

- In E2EE systems, providers **cannot access message content**, as the **private key** is held exclusively by the user.
- To execute detection orders, scanning must occur **before encryption**, directly on **the user's device**
- This is achieved through **client-side scanning**, which effectively converts user devices into **monitoring endpoints**, analyzing data **prior to encryption**



EUROPEAN COURT OF HUMAN RIGHTS (ECHR)

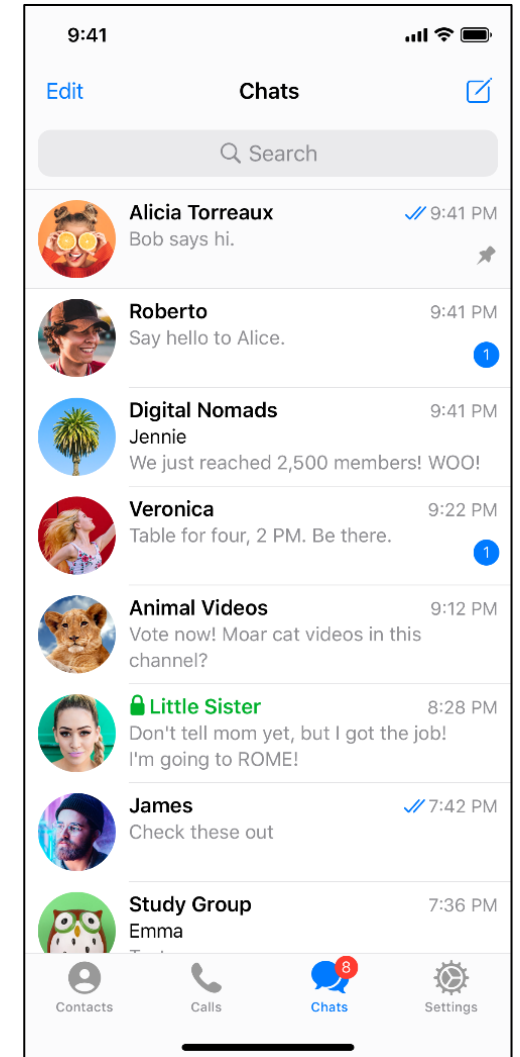
Podchasov
vs Russia



Telegram

Cloud chats:

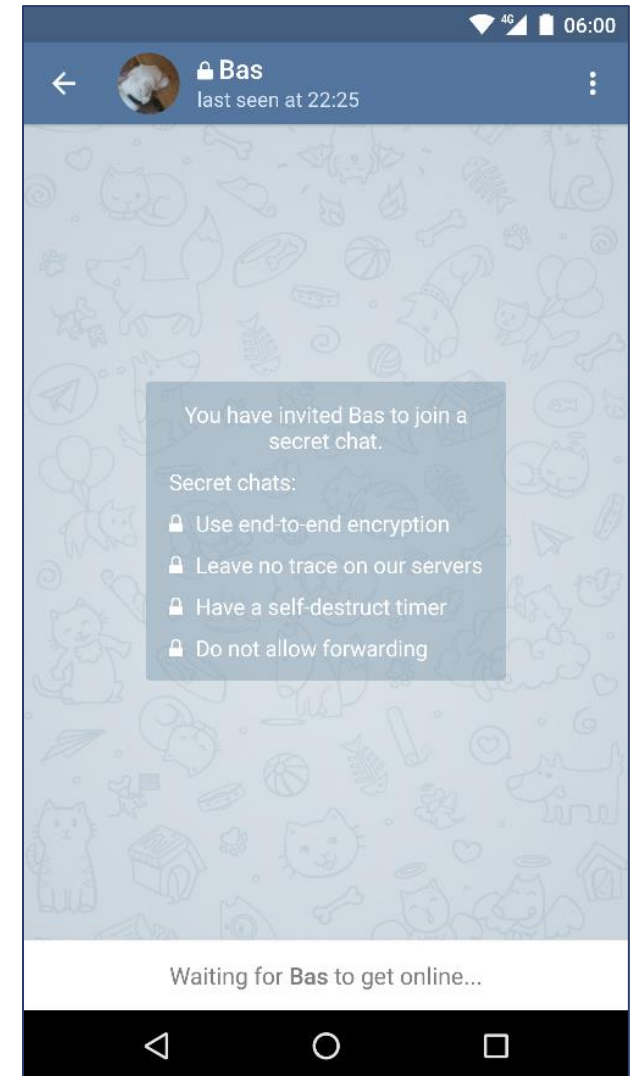
- **Single and group** chats
- **Server-client encryption** using of **MTPROTO** encryption
- **Not end-to-end encrypted**
- **Distributed infrastructure.**
- **Cloud chat** data is stored in multiple data centers around the globe.
- **Decryption keys** are split into parts and are never kept in the same place as the data they protect.



MTPROTO: security protocol developed by Telegram to ensure secure messaging over their platform by employing a sophisticated combination of symmetric and asymmetric encryption techniques, ensuring the confidentiality and integrity of transmitted data.

Telegram

- **Secret chats:**
 - **End-to-end encrypted**
 - **Chats stored only on the devices** of sender and receiver
 - Cannot be transferred to **another device.**
 - **Forwarding** is disabled
 - Have a **self-destruction timer**
- **End-to-end encryption** in Telegram is supported also for **audio** and **video** calls



ECHR – Podchasov vs Russia (March 2024)

Podchasov v. Russia (2017–2024)

- In **2017**, Russia mandated providers like **Telegram** to:
 - **Store all communication data**, including content, for **specified periods**.
 - Provide **law enforcement** with user data, message content, and **decryption capabilities**.
- The FSB ordered **Telegram** to **decrypt messages** of **six mobile numbers** using the **secret chat feature on Telegram** suspected of **terrorism**.
- **Telegram refused**, warning that such a **backdoor** would compromise encryption for all users.
- As a consequence:
 - Telegram was **fined** and its service was **blocked** in Russia.
 - Many users challenged the **disclosure orders** in **Russian courts**.

Decryption Order

Section 10.1(4.1) of the Russian Code of Criminal Procedure and the Operational-Search Activities Act, requires ICOs to provide, along with the requisite metadata and content data, any information necessary to decrypt communications. The Federal Security Service ordered Telegram to help decrypt communications for six mobile numbers, including the applicant's, by providing "data relating to the [encryption] keys." These six users were using the "secret chat" feature on Telegram, which enables E2EE protection for the messages. This order was challenged by Telegram, the applicant, and others.

<https://www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/>

- **Dmitry Podchasov**, a Russian citizen, brought the case to the **European Court of Human Rights (ECHR)**.
- He argued that forced decryption violated **Article 8 of the ECHR**:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

ECHR – Podchasov vs Russia (March 2024)

ECHR Conclusions:

- The Court held that the mandate to decrypt E2EE Telegram's *secret chats* communications risks weakening the encryption mechanism for all users, which was a disproportionate to the legitimate aims pursued.
- Encryption safeguards fundamental rights
- Encryption as a shield against abuses
- Blanket data retention interferes with the right to privacy

The ECHR conclusions stand in stark contrast to the European Commission's CSAR proposal, which would compel online services to scan private messages and compare user photos with law enforcement databases.

- The debate remains suspended between two opposing needs: protecting minors and safeguarding privacy.
- The *Podchasov* ruling and multiple security analyses reveal how the **Chat Control** approach risks being **disproportionate and counterproductive**.
- Instead of guaranteeing greater protection, it could make **European citizens more vulnerable**.
- The future of European regulation will depend on the institutions' ability to **balance security, fundamental rights, and digital trust**.



THIRD SECTION

CASE OF PODCHASOV v. RUSSIA

(Application no. [33696/19](#))

JUDGMENT

[https://hudoc.echr.coe.int/eng/#{%22itemid%22:\[%22001-230854%22\]}](https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]})



Thank you for your attention

References

<https://breakingdefense.com/2025/04/army-expands-access-to-encrypted-wickr-platform-in-aim-to-curb-insecure-comms-bolster-integration/>

<https://www.computerweekly.com/news/366632677/Chat-Control-encryption-plans-delayed-after-EU-states-fail-to-agree>

<https://dig.watch/updates/us-official-advises-encryption-amid-alleged-chinese-hacking-efforts>

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976

https://ec.europa.eu/commission/presscorner/detail/en/ip_25_920

<https://www.eff.org/deeplinks/2023/09/uk-government-knows-how-extreme-online-safety-bill>

<https://www.eff.org/deeplinks/2024/02/eff-statement-nevadas-attack-end-end-encryption>

<https://www.eff.org/deeplinks/2024/03/european-court-human-rights-confirms-undermining-encryption-violates-fundamental>

<https://www.eff.org/deeplinks/2024/10/salt-typhoon-hack-shows-theres-no-security-backdoor-thats-only-good-guys>

<https://www.eff.org/deeplinks/2025/03/win-encryption-france-rejects-backdoor-mandate>

<https://www.eff.org/press/releases/reject-nevadas-attack-encrypted-messaging-eff-tells-court>

<https://www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/>

https://www.europarl.europa.eu/doceo/document/E-10-2025-003250_EN.html

<https://getsession.org/>

[https://hudoc.echr.coe.int/eng/#%22itemid%22:\[%22001-230854%22\]](https://hudoc.echr.coe.int/eng/#%22itemid%22:[%22001-230854%22])

<https://www.reuters.com/technology/cybersecurity/chinas-harbin-says-us-launched-advanced-cyber-attacks-winter-games-2025-04-15/>

<https://support.apple.com/en-us/122234>

<https://www.theguardian.com/australia-news/2024/apr/29/australias-big-encryption-busting-laws-have-done-little-more-than-give-authorities-the-power-to-ask-nicely>

<https://www.theguardian.com/australia-news/2024/oct/11/half-of-australias-law-enforcement-agencies-have-banned-officers-using-encrypted-messaging-apps>

<https://www.theguardian.com/media/2025/mar/17/social-media-companies-fines-uk-illegal-content-online-safety-act>

<https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law>

https://www.theregister.com/2024/10/07/verizon_att_lumen_salt_typhoon/

<https://requestly.com/blog/how-whatsapp-ensures-chat-security-with-end-to-end-encryption/>

<https://therecord.media/european-commission-takes-aim-encryption-europol-fbi-proposal>

https://www.theregister.com/2024/12/05/tmobile_cso_telecom_attack/

<https://www.wati.io/blog/understanding-whatsapp-data-security-understand-end-to-end-encryption-and-backups/>

<https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>

<https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>

Pfefferkorn, R. (2022). *Content-oblivious trust and safety techniques: Results from a survey of online service providers*. Journal of Online Trust and Safety, 1(2). <https://doi.org/10.54501/jots.v1i2.14>