

Dear MEP,

Welcome back! The ECLAG coalition hopes you had a good summer break.

As we enter the fall, we'd like to bring your attention back to the child sexual abuse crisis and the stakes at hand. Every year, this issue **affects millions of children across Europe**, and the coming months will bring critical decisions in the European Parliament that will shape how the EU protects children online.

To support you and your team as you engage with this legislative agenda, the ECLAG Steering Group has prepared **a series of factsheets** covering the key issues. Each factsheet is designed to be a quick, reliable reference: it explains the core problem, summarizes the current state of play, and explores in an accessible way the technical aspects of it.

In this series, you will find factsheets on:

- What is online child sexual abuse and how it manifests
- What's the Child Sexual Abuse Regulation
- What's Child Sexual Abuse Material detection
- Detection technology
- Detection on encrypted spaces
- Why targeted detection creates significant gaps
- AI-generated CSAM

We know your time is valuable and limited, and that legislative files on this topic can be very technical and fast-moving. We hope this piece of work gives you a clearer understanding and actionable information as these debates unfold in the fall.

If you or your team have questions, or would like a briefing meeting with ECLAG, please don't hesitate to reach out to csa.euadvocacy@gmail.com.

Thank you for your continued commitment to protecting children across Europe.



Content warning: This campaign discusses child sexual abuse. Some readers may find this content distressing, particularly those who have experienced abuse or trauma themselves. Please take care while reading, and feel free to pause or stop if you need to.

WHAT IS ONLINE CHILD SEXUAL ABUSE?

Child sexual abuse is a crime. Digital technologies have made it easier for perpetrators to contact children, produce and distribute child sexual abuse material (CSAM) and reach victims across borders. The sexual abuse crisis is escalating at alarming rates. New technologies such as **generative AI** are reshaping and exacerbating online CSA. The expansion of the internet has fundamentally reshaped this crime.

WE ARE IN A CHILD SEXUAL ABUSE CRISIS

312,030

That's how many **reports** of confirmed CSAM the IWF* recorded in the last year.
↑ **7% from the year before.**

*Internet Watch Foundation

63%

of all confirmed CSAM was hosted **in the EU** in 2025 with most CSAM hosted in just a small number of jurisdictions

EVERY 1.5 SECONDS

That's how often **CSAM** was **found online** in 2025 according to NCMEC*.

*National Center for Missing and Exploited Children

Behind each photo or video there is a child who has or is still being horribly abused.
Each time the image is shared, the victim experiences the abuse all over again.

HOW DOES IT MANIFEST?

Protecting children requires understanding of how perpetrators operate online. **CSAM is not confined to the dark web**; it is openly accessible. According to the CSAM Perpetrator survey led by Protect Children:

61%

of surveyed individuals reported using **open web platforms** to view CSAM.

27%

reported searching for CSAM on search engines such as **Google, pornography sites and social media platforms.**

31%

of CSAM consumers avoid platforms with age limits and strict sign-up requirements.
20% avoid platforms without end-to-end encryption.

Technology advances faster than legislation
CHILDREN PAY THE PRICE

WHAT IS THE EU CHILD SEXUAL ABUSE REGULATION

The proposed Child Sexual Abuse Regulation is the only legal framework that can ensure to put an end to the online Child Sexual Abuse Crisis.

Child sexual abuse material (CSAM) is shared online every day and offenders actively seek out gaps in platform safety measures to target children and circulate this material with a reduced risk of detection.

Without a strong legal framework, platforms have no clear obligation - no clear legal basis - to detect, report and remove CSAM, leaving children exposed and illegal content circulating unchecked.

THE PROPOSED REGULATION

The Regulation proposed by the European Commission in May 2022 would require online platforms to:

- Assess the risk their service could be misused for child sexual abuse
- Mitigate that risk with real safety measures
- Detect, report & remove child sexual abuse material under a court-ordered, rights-balanced process
- Create an EU Centre: a hub for data, tech tools, and support for victims

THE LAW THAT CHILD RIGHTS ADVOCATES ARE ASKING FOR:

- 1 Mandates child safety by design** to ensure that platforms design their services with the rights and needs of children at the forefront, assess the risk of abuse and adopt risk mitigation measures.
- 2 Detection, reporting, and removal** of all CSAM and grooming for all online service providers and platforms that operate or have users in the EU.
- 3 A clear legal basis for voluntary detection measures by platforms**, as part of risk mitigation measures and with all necessary safeguards.
- 4 Cover all forms of threat to children online:** known CSAM, unknown CSAM and grooming to prevent harm from happening in the first place.
- 5 Strong safeguards** to avoid any misuse of detection technology and ensure the fundamental rights of adult and child users are respected, including privacy and protection.
- 6 Technology-neutral approach and future-proofing** to ensure that children are protected everywhere on the internet, including in encrypted environments, and to enable the development and deployment of technical solutions in the evolving digital environment, including gaming and the metaverse.
- 7 A new EU centre** within the existing EU and global child safety ecosystem, including a victims and survivors' council providing policy recommendations to the centre and contributing to actions taken by the Commission.

WHAT IS CSAM DETECTION?

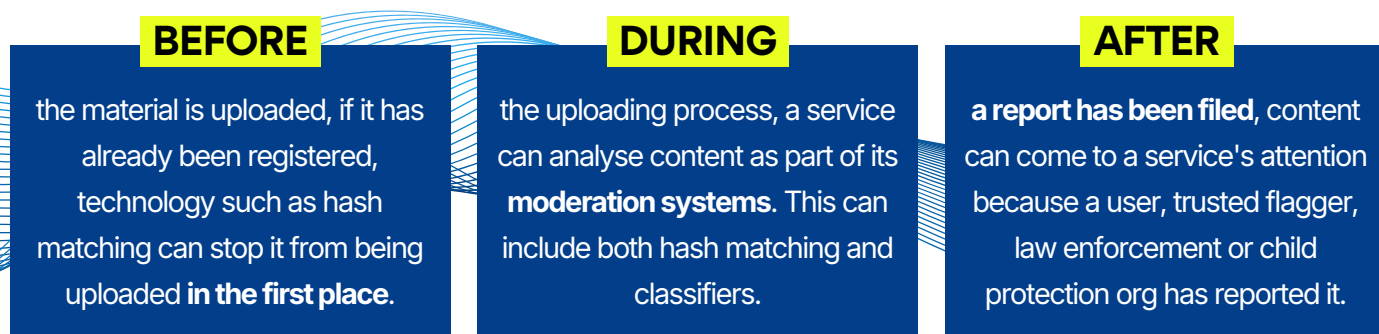
Online services use various technologies to identify child sexual abuse material (CSAM). Each is designed to address a different part of the problem. But the scale and speed at which CSAM is created and shared online means that **relying on individual reports alone will never be sufficient**.

WHAT DETECTION TECHNOLOGIES EXIST?



Different methods are layered so the limitations of one are covered by the strengths of another. **Technology does not replace human assessment**, investigation or enforcement, but can help ensure that potential CSAM is identified quickly enough for those interventions to take place.

WHEN DOES DETECTION TAKES PLACE?



FOCUS ON: HASH MATCHING

- 1 **Experts identify** an illegal image or video.
- 2 **It is turned into a hash**, a digital fingerprint.
- 3 **The hash is stored in a secure database.** The original image or video are not stored.
- 4 **If a new hash matches** that of a previously identified illegal content, action can be taken.

Caveat! It generally cannot identify previously unseen CSAM without a hash.

FOCUS ON: CLASSIFIERS

- Useful for identifying **previously unassessed CSAM** without a hash.
- They use **machine-learning** to assess CSAM by identifying patterns and assigning a probability or confidence score to content.
- **Trained using datasets** containing CSAM and legal imagery to be able to tell whether the material fits the patterns it has learned.

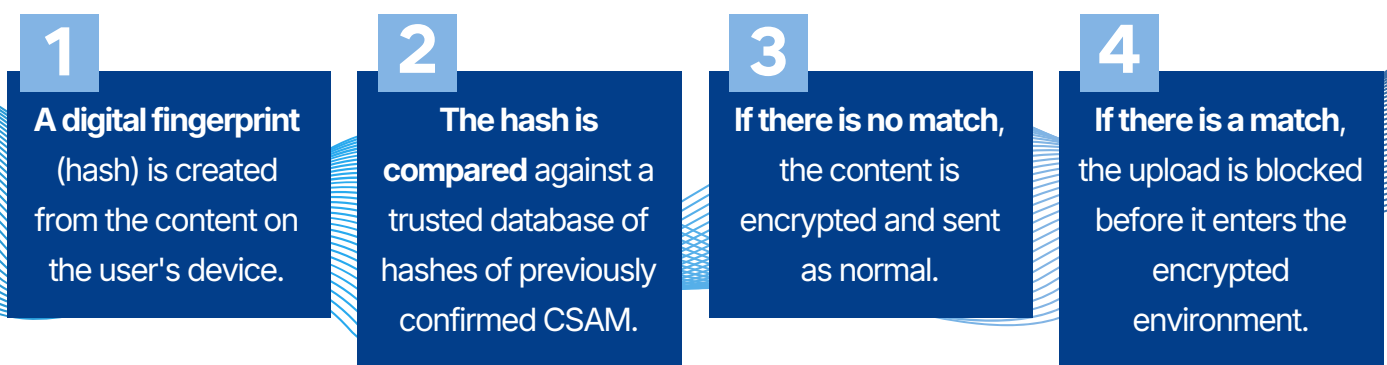
Caveat! Their outputs can require human review to confirm that the content is illegal.

PROTECTING CHILDREN **DOES NOT** REQUIRE BREAKING ENCRYPTION

Encryption is an essential security technology but without effective, privacy-preserving safety measures, offenders can exploit encrypted services to share illegal content with a reduced risk of detection, allowing known child sexual abuse material (CSAM) to continue circulating online. A common misconception is that detecting CSAM requires accessing users' private messages or weakening encryption. **This is not the case.** Modern technologies allow us to uphold strong encryption while implementing targeted measures to prevent the distribution of known CSAM.

DETECTION IS TECHNICALLY POSSIBLE WITHOUT BREAKING ENCRYPTION

Known CSAM can be detected using upload prevention before it is encrypted and transmitted:



At no stage does the platform have to decrypt messages, view communications or introduce a 'backdoor' into encryption.

PRE-ENCRYPTION SAFETY CHECKS ALREADY EXIST

Technology companies routinely perform checks before encryption to:

- **Block malware** and malicious files
- **Generate rich link previews**
- **Warn users** about suspicious links
- **Protect children** through on-device safety features such as nudity detection

These features prove that services can safely perform limited, privacy-preserving checks before encryption without compromising users' security. **Detecting CSAM uses the same principles.**

TARGETED DETECTION CREATES MAJOR GAPS

Targeted or 'suspicion-based' detection sounds straightforward: instead of skimming through a service, technology is used when there is already a reason to suspect a particular user or group of users. But, this creates a major gap:

How do you identify the people who should be targeted if you cannot find them?

Online CSA is not confined to a small, known group of offenders. People create new accounts, move between services, use different channels and share material with previously unidentified users.

Much of the CSAM detected online comes from previously unknown cases.

This makes broad detection an important source of intelligence. When a service detects and reports CSAM, that report can help identify a victim, including in urgent need of rescue, an offender, a new piece of material or a new distribution network.

Limiting detection to current suspects risks creating a self-reinforcing blind spot.

ONE LAYER OF DETECTION IS **NOT** ENOUGH

CSAM detection works more like a layered security system than a watch list:

Hash matching identifies **known material**; classifiers help identify previously unseen material; user reports surface content that automated systems miss; and human reviewers assess and act on potential abuse.

Targeting only specific suspects removes much of this coverage:

21.3 MILLION

That's how many **reports involving child sexual exploitation** the NCMEC CyberTipline received in 2025, including **61.8 million images and videos**. This shows the scale of the online material and why relying solely on people or authorities to identify suspects cannot provide comprehensive coverage.

Targeted detection cannot replace the ability to detect CSAM more widely. If detection is limited to known or suspected offenders, the system risks missing new cases and previously unseen CSAM that can be hashed and blocked using existing detection infrastructure.

If we cannot use **technology** to identify new cases, there will be **fewer** new cases that can be investigated.

FOCUS ON: AI-GENERATED CHILD SEXUAL ABUSE MATERIAL

AI-generated CSAM is increasingly difficult to distinguish from other CSAM

Largely theoretical two years ago, AI-generated child sexual abuse material (CSAM) is now being produced at scale, with more sophisticated offender communities, and growing evidence of harm to victims and child protection efforts. **Can regulation, law enforcement and industry keep pace?**

In 2025, the Internet Watch Foundation's found:

3,443

AI CSA videos identified
↑ 26,385% in one year

65%

of the videos depicted the
most severe forms of CSA
(vs 43% of non-AI videos)

NOT NICHE

AI CSAM appears both on the **dark web and mainstream platforms**, while chatbots and 'all-in-one' services combine image generation, roleplay and grooming functionality.

AI CSAM IS NOT 'VICTIMLESS'

- It is increasingly **REALISTIC** and **EXTREME**
- It is making CSAM **EASIER TO CREATE**
- It allows offenders to **GENERATE NEW CSAM** of survivors years after their abuse, often surpassing their original CSAM in volume.
- It is **NORMALISING Child Sexual Abuse**
- It **INCREASES THE PRESSURE** on law enforcement and child protection organisations by making their work more resource intensive
- It is **EXPOSING LOOPHOLES** in the legal framework

AI CHANGES THE DEBATE

Hash matching is highly effective at identifying already assessed CSAM. However, **every AI-generated image is unique so they cannot be identified using hash matching**, which allows offenders to produce an endless amount of AI-generated CSAM. By the time an image is added to a hash database **it may already have been widely shared**.

The proportion of unknown CSAM is likely to continue increasing, which makes detecting this type of content increasingly important for child protection. To act effectively against the spread of AI-generated CSAM, **regulation must allow providers to deploy technologies which are able to identify previously unknown CSAM**, such as AI classifiers.