Council of the European Union

Brussels, 28 November 2025
(OR. en)

16137/25

JAI 1814
ENFOPOL 457
CRIMORG 247
IXIM 326
DATAPROTECT 319
CYBER 356
COPEN 389
FREMP 369
TELECOM 447
COMPET 1262
MI 980
CONSOM 276
DIGIT 256

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	27 November 2025
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2025) 740 final
Subject:	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

Delegations will find attached document COM(2025) 740 final.

Encl.: COM(2025) 740 final

EUROPEAN
COMMISSION

Brussels, 27.11.2025
COM(2025) 740 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the implementation of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

CONTENTS

1. INTRODUCTION 2

2. IMPLEMENTATION MEASURES 3

2.1. Processing of personal data by providers (Article 3(1)(g)(vii)) 3

2.1.1. Type and volumes of data processed 3

2.1.2. Grounds for processing under Regulation (EU) 2016/679 4

2.1.3. Ground for transfers of personal data outside the EU 4

2.1.4. Number of cases of online CSA identified, differentiating between CSAM and solicitation of children 4

2.1.5. User redress and outcome 6

2.1.6. Number and ratios of errors (false positives) of the different technologies used 7

2.1.7. Measures applied to limit the error rate and the error rate achieved 9

2.1.8. Retention policy and data protection safeguards 9

2.1.9. Organisations acting in the public interest with which data has been shared 10

2.2. Member States' statistics (Article 8) 10

2.2.1. The total number of reports of detected online CSA 11

2.2.2. The number of children identified 20

2.2.3. The number of perpetrators convicted 25

2.3. Developments in technological progress 28

2.3.1. Detection of known CSAM 28

2.3.2. Detection of new CSAM 29

2.3.3. Detection of solicitation of children for sexual purposes 30

2.3.4. Use of generative AI for the purpose of child sexual abuse 31

3. CONCLUSIONS 32

1. INTRODUCTION

Interpersonal communication services are increasingly misused to share child sexual abuse material (CSAM) and for solicitation of children for sexual purposes ('grooming'). This has led providers of certain number-independent interpersonal communications services, such as webmail and messaging services ('providers'), to use specific technologies on a voluntary basis to detect online child sexual abuse (CSA) on their services and report it to law enforcement authorities and organisations acting in the public interest against CSA. Such voluntary activities play a valuable role in helping to identify and rescue victims, reduce child grooming and the dissemination of online CSAM, and prevent, detect, investigate and prosecute CSA offences. To enable the continuation of voluntary efforts to identify CSA, Regulation (EU) 2021/1232[1] ('the Regulation'), as amended by Regulation (EU) 2024/1307 of 29 April 2024,[2] provides for a temporary derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC[3].

Article 9 of the Regulation requires an implementation report by the Commission, based on data from providers and Member States, and considering, in particular:

(a) the conditions for the processing of relevant personal data and other data processed under the Regulation;
(b) the proportionality of the derogation provided for by the Regulation, including an assessment of the statistics submitted by the Member States pursuant to its Article 8;
(c) developments in technological progress regarding the activities covered by the Regulation, and the extent to which such developments improve accuracy and reduce the numbers and ratios of errors (false positives).

This is the second implementation report under the Regulation, following the first report adopted on 19 December 2023[4]. It builds on the data obtained since then, through reporting by providers and Member States pursuant to its Article 3(1)(g)(vii) and Article 8 respectively.

The first report brought to light significant disparities in the availability of data, the types of data collected, and therefore also the comparability of the data collected by providers and Member States. This second report shows that these issues persist. Providers did not use the

---

1 Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, (OJ L 274, 30.7.2021, p. 41-51, ELI: http://data.europa.eu/eli/reg/2021/1232/oj).

2 Regulation (EU) 2024/1307 of the European Parliament and of the Council of 29 April 2024 amending Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, (OJ L, 2024/1307, 14.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1307/oj).

3 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

4 Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, COM/2023/797 final.

standard form for reporting set out in the Commission Implementing Regulation adopted on 25 November 2024[5], as required by Article 3(4) of the Regulation, arguing that it only became available towards the end of the reporting period. They also shared different types of information which are not necessarily comparable. Many Member States provided data late and some provided only partial data or were unable to provide any data before the publication of this report. The Commission engaged in follow-up to encourage the submission of the data and enable their correct interpretation. This had a significant impact on the timing and comprehensiveness of the overall report. Despite efforts to ensure data coherence and comparability, disparities remain.

This report seeks to give a factual overview of the state of play on the implementation of the Regulation, based on the available data. The report does not contain any interpretation of the Regulation and does not take any position on the manner in which it has been interpreted and applied in practice.

2. IMPLEMENTATION MEASURES

2.1. Processing of personal data by providers (Article 3(1)(g)(vii))

Article 3(1)(g)(vii) of the Regulation lays down the conditions for providers acting under the derogation contained therein to publish and submit to the competent supervisory authority and to the Commission, by 3 February 2022, and by 31 January every year thereafter, a report on the processing of personal data under this Regulation. Google, LinkedIn, Meta, Microsoft and Yubo submitted reports, for both 2023 and 2024. This report covers the data submitted by providers for the years 2023 and 2024, while the data for 2021 and 2022 is covered under the previous report.

2.1.1. Type and volumes of data processed

Providers reported processing both content and traffic data. As regards content data processed to detect online CSA, all providers mentioned images and videos. Google also referred to the processing of other media types.

As for traffic data collected, the providers' reports varied considerably:

a) data related to the user account (Google, LinkedIn, Microsoft, Yubo), e.g. user ID, username, and IP address;
b) metadata related to content (Google, LinkedIn, Microsoft, Yubo);
c) data related to a potential victim (Google);
d) abuse operations data (Google).

LinkedIn and Microsoft provided information on the volumes of data processed under the Regulation, while the other providers did not submit data in this regard. LinkedIn reported

[5] Commission Implementing Regulation (EU) 2024/2916 of 25 November 2024 laying down a standard form for the data included in the report on the processing of personal data published and reported to the competent supervisory authority and to the Commission by service providers under Regulation (EU) 2021/1232 of the European Parliament and of the Council, (OJ L, 2024/2916, 26.11.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2916/oj).

processing over 24 million images and over 1 million videos in 2023 and over 22 million images and over 2 million videos in 2024, originating from the EU in both years. Microsoft reported processing over 11.7 billion content items globally in 2023, and 9.6 billion content items globally in 2024, without specifying the data related to the EU.

2.1.2. Grounds for processing under Regulation (EU) 2016/679

All providers reported relying on one or more of the specific grounds under Regulation (EU) 2016/679 – the General Data Protection Regulation ('the GDPR') [6]: Article 6(1)(d) (Google, Meta, Yubo), (e) (LinkedIn, Microsoft, Meta, Yubo) and (f) (Google, Meta, Yubo).

2.1.3. Ground for transfers of personal data outside the EU

All providers reported relying on data transfer mechanisms under the GDPR, including standard data protection clauses adopted by the Commission pursuant to Article 46(2)(c) of the GDPR. Google, Microsoft, LinkedIn and Yubo also reported complying with the EU-US Data Privacy Framework.

2.1.4. Number of cases of online CSA identified, differentiating between CSAM and solicitation of children

Table 1: Number of cases of online CSA identified in 2023

Provider	Number of cases	Comments
Google	1 558 content items	734 reports on CSAM sent to the National Center for Missing and Exploited Children (NCMEC). 635 Google accounts reported as sending at least one content item of CSAM.
LinkedIn	2 content items	LinkedIn identified 2 images and 0 videos constituting CSAM.
Meta	3.6 million content items	Content items constituting CSAM in relation to EU users.
Microsoft	9 000 content items	Over 32 000 content items identified as CSAM globally during the period, with over 9 000 of those content items from the EU.
Yubo	7 720 cases	Yubo suspended 7 720 accounts in the EU in 2023, 2 of which for having shared known CSAM, 938 for having shared new CSAM, and 6 780 for having solicited or sexually exploited a child.

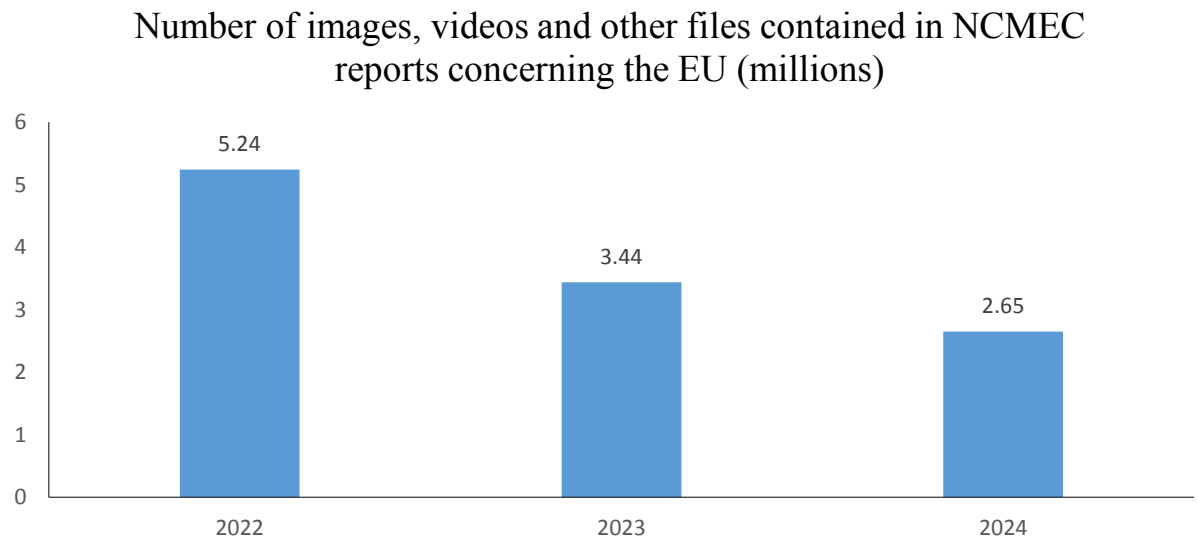
Table 2: Number of cases of online CSA identified in 2024

Provider	Number of cases	Comments
Google	1 824 content items	508 reports on CSAM sent to NCMEC. 503 Google accounts reported as sending at least one content item of CSAM.
LinkedIn	1 content item	LinkedIn identified 1 image file and 0 videos constituting CSAM.

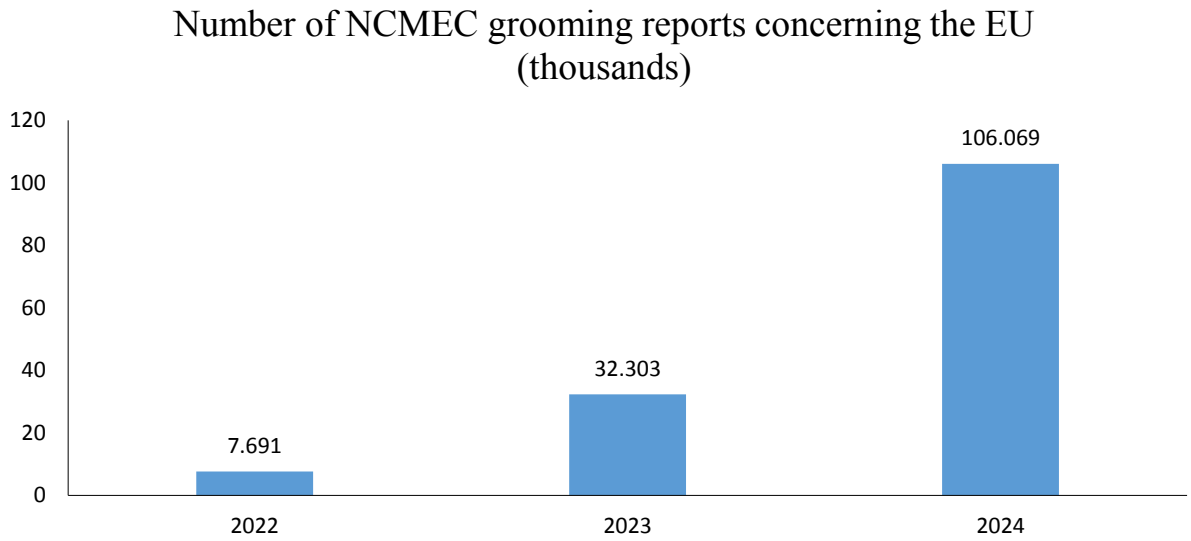
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (OJ L 119, 4.5.2016, p. 1-88, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

Meta	1.5 million content items	Content items constituting CSAM in relation to EU users.
Microsoft	More than 5 800 content items	Over 26 000 content items identified as CSAM globally, with over 5 800 of those content items from the EU[7].
Yubo	4 484 cases	Yubo identified 742 cases concerning new CSAM and 3 742 cases concerning solicitation of children.

Since all the above providers report to NCMEC in the US (see Section 2.1.9.), in addition to other providers that have not reported to the Commission, the NCMEC data provide, in principle, a more comprehensive overview of the reports of CSA in the EU. NCMEC reported having received the following numbers of content items (images, videos and other files) and cases of solicitation of children concerning the EU per year:



[7] Data reported from Microsoft show that the ratio between content items identified as child sexual abuse material and content items processed remained constant from 2023 to 2024, at 0.00027%.



2.1.5. User redress and outcome

Under Article 3(1)(g)(iv) of the Regulation, providers are to establish appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them. In addition, Article 5 sets out rules on judicial redress.

All providers reported user complaint numbers regarding matters under the scope of the Regulation within the EU, and the outcomes of such complaints. The providers referred either to complaints against the removal of content items or to complaints against the suspension of user accounts, without submitting separate information on both categories. Google and Yubo also reported separately on complaints lodged with a judiciary authority. Consequently, the tables below reflect internal redress procedures, and includes information on judicial redress in the comments where the data are available; to date, no instance of complaints to a judicial authority have been reported.

Table 3: Number of cases in which a user lodged a complaint with the internal redress mechanism or with a judicial authority and the outcome of such complaints in 2023

Provider	User complaints	Reinstated accounts	Reinstated content items	Comments
Google	297	10	n/a	The number of cases of user complaints reflects appeals against the suspension of a user account lodged with the internal redress mechanism. No user lodged a complaint with a judicial authority.
LinkedIn	0	n/a	n/a	
Meta	ca 254 500	n/a	ca 11 600	Users appealed the actions taken on around 254 500 content items. Following the appeals process, around 11 600 content items were restored and account actions reversed.

Microsoft	0	n/a	n/a	
Yubo	1159	50	n/a	Yubo estimates approximately 50 EU-based accounts were restored following such appeals. No user lodged a complaint with the judicial authority in the EU.

Table 4: Number of cases in which a user lodged a complaint with the internal redress mechanism or with a judicial authority and the outcome of such complaints in 2024

Provider	User complaints	Reinstated accounts	Reinstated content items	Comments
Google	216	19	n/a	The number of cases of user complaints reflects appeals against the suspension of a user account lodged with the internal redress mechanism. No user lodged a complaint with a judicial authority.
LinkedIn	1	n/a	n/a	
Meta	ca 76 900	n/a	ca 1 800	Users appealed the actions taken on around 76 900 content items. Following the appeals process, around 1 800 content items were restored and account actions reversed.
Microsoft	0	n/a	n/a	
Yubo	31	0	n/a	Yubo received 31 complaints against a suspension related to child safety in the EU. 0 accounts were reinstated.

2.1.6. Number and ratios of errors (false positives) of the different technologies used

In line with Article 3(1)(e) of the Regulation, providers are to ensure that the technologies used are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online CSA.

In this respect, all providers reported that they implemented a layered approach to the detection of CSA by combining different detection technologies to increase accuracy. Furthermore, there is a trade-off between false positives (i.e. when the tool flags, for example, an image as possibly constituting CSAM incorrectly) and false negatives (i.e. when the tool fails to flag, for example, CSA), since reducing one error rate typically increases the other. This means that the provider can tailor the accuracy settings to choose the appropriate balance based on the specific context and nature of the service.

Providers relied on hash-matching technology such as PhotoDNA, MD5 and CSAI Match to detect matches of previously identified CSAM. The use of artificial intelligence (AI) and machine learning classifiers to detect new CSAM was also reported (Google, Yubo). Yubo also reported detecting solicitation of children.

Providers did not submit the number and ratios of errors (false positives) for each of the different technologies used separately. Instead, they reported aggregate data for all technologies used.

The data submitted show different methods used to calculate the error rate. Some providers did not have sufficient data to calculate the error ratio (Microsoft). Others applied a calculation method based on the overall ratio of the content items restored and/or account actions reversed to the content items that were actioned, or based on the number of appeals against account restrictions (Meta, LinkedIn). Other providers (Google and Yubo) referred to the number of content items automatically flagged as constituting CSAM that were then not confirmed as CSAM upon human review (false positives), divided by the number of content items automatically flagged as constituting CSAM. The tables below therefore reflect the disparities in the sets of data presented by the providers.

To further reduce errors and false positives, providers also reported complementing these technologies with human review. This human review is not factored into the statistics below, which only take into account the accuracy of the technologies themselves.

Table 5: Number and ratios of errors in 2023 and 2024

Provider	Error ratio 2023	Error ratio 2024	Calculation method	Comments
Google	1.14% (18:1576)	0.54% (10:1834)	Ratio of the number of content items automatically flagged as CSAM that are not confirmed upon human review to the number of content items automatically flagged as CSAM	The data refer to Google's hash-matching technology.
LinkedIn	0% (0:0)	0% (0:0)	Ratio of the account actions reversed to the appeals against account restrictions	
Meta	0.32% (11 600:3.6 million)	0.12% (1 800:1.5 million)	Ratio of content items restored and account actions reversed to the actioned content items	
Microsoft	n/a	n/a	n/a	Microsoft indicated that the data was insufficient to calculate an error rate. There were reversals of initial content moderation decisions connected with 34 content items. No appeals reported.
Yubo	20%	13%	Cases automatically flagged as grooming in which moderators did not take action	The data provided by Yubo refer solely to the detection of new CSAM and grooming.

2.1.7. Measures applied to limit the error rate and the error rate achieved

Under Article 3(1)(e) of the Regulation, the technologies used must be sufficiently reliable and the consequences of any occasional errors must be rectified without delay. In addition, Article 3(1)(g)(ii) requires providers to ensure human oversight and, where necessary, human intervention.

Providers reported applying different measures and safeguards to limit and reduce the error rate in detecting online CSA. These include:

i. monitoring and quality assessment of the performance of CSA detection tools, both to fine-tune precision (that they are detecting only online CSA) and recall (that they are not missing online CSA on their platforms) (Google);
ii. application of hash verification processes in which analysts review items associated with databases of hashes and/or check the quality of existing hashes (Google, Microsoft, LinkedIn);
iii. human review and oversight: media detected as CSAM by hash-matching technologies are audited by human reviewers/trained analysts (Google, LinkedIn, Meta, Microsoft, Yubo);
iv. systematic human review of media detected as possible new CSAM prior to reporting (Google in 2023);
v. human reviewers undergoing specialised training and/or being subject to regular recertification (Google, Yubo);
vi. quality control assessments of human reviewers and the verdicts that are applied (Google, Yubo);
vii. development and regular review of policies and enforcement strategies on online CSA by trained experts (Google);
viii. regular consultations with experts to improve accuracy in identifying CSAM, including channels to receive feedback from trusted organisations that fight CSA, such as NCMEC and Thorn (Google);
ix. alert system ensuring that high volume clusters are flagged and reviewed (Meta);
x. measures to improve the quality of safety algorithms (Yubo).

2.1.8. Retention policy and data protection safeguards

Article 3(1)(h) and (i) of the Regulation require relevant personal data to be stored in a secure manner only for certain specified purposes, and to contain specifications regarding the storage period, respectively. In addition, the applicable GDPR requirements must be respected.

All providers reported having retention policies and personal data protection safeguards in place. Data retention policies vary depending on the type of data. Providers indicate that in each case the retention period is limited in time, depending on the type of data and the purpose of processing, and the data are deleted at the end of the retention period. Most providers (Google; Meta and LinkedIn for 2024) also reported applying a maximum 12-month retention policy for detected CSAM. Yubo reported that data on content moderation is usually kept for 12 months and that retention periods depend on the type of content, type of violation and

storage conditions. Meta reported, in 2024, retaining the data on users' appeals for a period of 195 days.

Data protection safeguards reported by providers include:

i. use of de-identification or pseudonymisation techniques (e.g. masking, hashing, differential privacy) (Microsoft);
ii. use of encryption of data in transit (e.g. TLS protocols) (Meta, Yubo);
iii. access controls (Meta, Yubo);
iv. implementation of data governance strategies and/or privacy programmes, ensuring that data are accessed, used or shared only in an authorised manner (Google);
v. conducting privacy reviews to identify, access and mitigate potential privacy risks from the collection, processing, storing and sharing of personal data, and review of protection practices when new system capabilities or processes are being designed (Microsoft);
vi. prompt investigation of reported incidents by the response team (Google);
vii. measures on internal redress mechanisms and information to users, including measures to ensure the right to access users' data (Google in 2024).

2.1.9. Organisations acting in the public interest with which data has been shared

All the providers reported sharing the data pursuant to this Regulation with NCMEC. All the reporting providers also communicated to the Commission, in compliance with Article 7(1) of the Regulation, that they reported online CSA under this Regulation to NCMEC [8]. Yubo also reported sharing data with the Internet Watch Foundation (IWF) in the UK and PHAROS (Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements) in France.

2.2. Member States' statistics (Article 8)

Pursuant to Article 8(1) of the Regulation, Member States must make publicly available and submit to the Commission reports with statistics on the following:

(a) the total number of reports of detected online CSA that have been submitted by providers and organisations acting in the public interest against CSA to the competent national law enforcement authorities, differentiating, where such information is available, between the absolute number of cases and those cases reported several times and the type of provider on whose service the online CSA was detected;
(b) the number of children identified through actions pursuant to Article 3, differentiated by gender;
(c) the number of perpetrators convicted.

Given that, for the previous report, some Member States reported data up to July 2022 and others for all of 2022, this report covers the full calendar years 2022, 2023 and 2024 to facilitate comparability. That said, the data reported by Member States varies greatly in terms of completeness and detail. A few Member States did not provide all the data required for each of the years in question (Belgium, Estonia, Ireland, Spain, Croatia, Portugal and Romania).

[8] The information on the organisations acting in the public interest to which providers report online CSA under this Regulation has been published at https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/legal-framework-protect-children_en, in line with the Commission's obligation under Article 7(2) of the Regulation.

2.2.1. The total number of reports of detected online CSA

Most Member States provided yearly statistics on the total number of reports of online CSA for the calendar years 2022, 2023 and 2024, pursuant to Article 8(1)(a) of the Regulation. Portugal did not provide data for any of the relevant years, while Spain did not provide data for 2023 or 2024.

Member States mostly provided the total number of reports submitted by providers or other organisations acting in the public interest against CSA to the national law enforcement authorities. Most Member States reported receiving most or all of their reports from NCMEC. Member States did not indicate the number of actionable reports (i.e. reports suitable for investigation), but some referred to the number of cases launched, which is significantly lower. Neither did Member States – with the exceptions of Finland and Denmark – differentiate between the total number of cases and cases reported several times. Only a few Member States indicated the type of providers on whose services the online CSA was detected (e.g. Belgium, Ireland, Poland and Romania). Some provided a detailed breakdown (Belgium, Czechia, France, Luxembourg, Romania and Finland).

Table 6: Total number of reports of detected CSA as reported by Member States

Country	Reports in 2022	Reports in 2023	Reports in 2024	Source of reports	Comments
AT	10 130	15 882	18 276	NCMEC[9]	
BE	19 919	11 910	4 284	Reports originating from providers (social media)	The number of providers detecting online CSA increased between 2022 and 2024. For 2024, Belgium only reported the number of actionable reports, changing the methodology used in previous years.
BG	25 303	38 026	71 187	NCMEC and INHOPE (international association of internet hotlines)	Over the three years in question, 42 596 reports were received from NCMEC and 92 010 from Safenet.
CY	2 809	3 516	5 380	NCMEC	
CZ	23 854	21 658	22 580	NCMEC, CZ.NIC (Czech association of internet service providers)	In 2024 reports were received from 57 different service providers, Instagram being the first (11 857 reports), followed by Facebook (4 461), Snapchat (3 610), Imgur (1 705), Discord (1 510), Google (1 439), Microsoft – Online operations (870), Tik Tok (825) and WhatsApp (620).
DE	136 437	180 287	205 728	NCMEC	Germany reported that it could not provide any own statistics in line with Article 8(1) of the Regulation, arguing that there is no legal basis for voluntary detection. It provided police crime statistics, highlighting that the year in which the crime was committed does not necessarily match the year in which it appears in the statistics: on sexual abuse of children and juveniles, there were 16 655 cases in 2022 and

[9] All data in this table, including where NCMEC or other external sources are listed, is reproduced as reported to the Commission by the Member States.

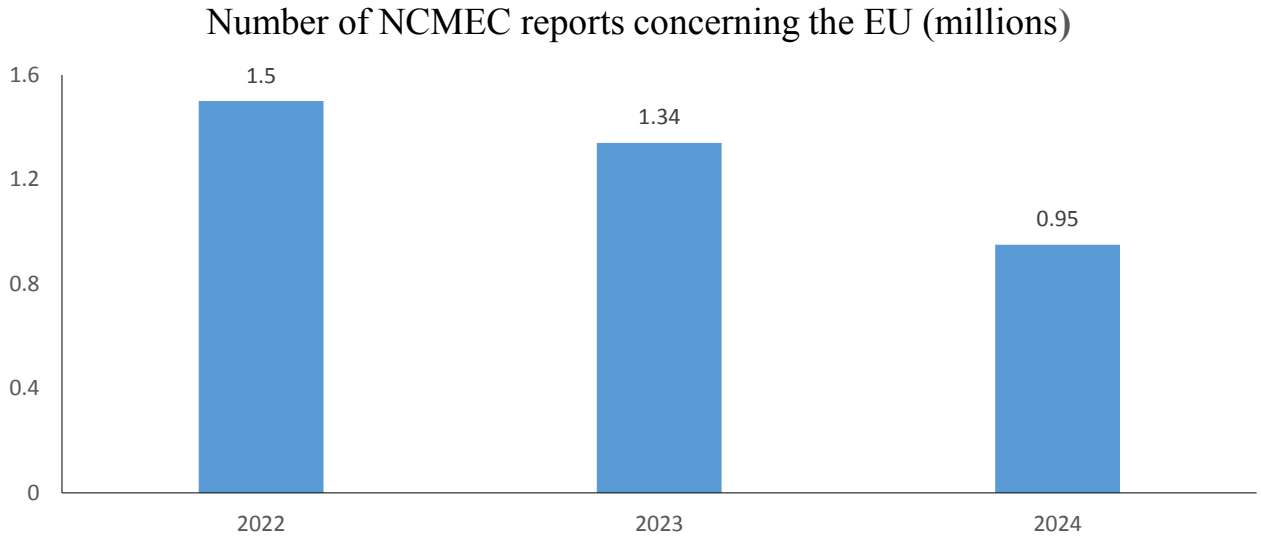
Country	Reports in 2022	Reports in 2023	Reports in 2024	Source of reports	Comments
					17 575 cases in 2023 (+6%). Concerning dissemination, acquisition and possession of child and juvenile sexual abuse material, there were 48 853 cases in 2022 and 54 042 cases in 2023 (+11%).
DK	7 556	9 938	10 918	NCMEC	2 474 cases were initiated in 2022, 2 278 in 2023, and 2 097 in 2024. 90 of the cases opened were based on CSAM reported several times in different years.
EE	250	305	274	NCMEC, Child Helpline 116 111	Estonia reported that the statistics of its Police and Border Guard, including NCMEC data, are not public. 250 non-contact sexual crimes against children were reported in 2022 and 305 in 2023. 88% of all non-contact sexual crimes in 2022 were committed in the online sphere. The data available for 2024 correspond to cases registered by the police and brought to the public's attention in the crime survey conducted by the Ministry of Justice and Digital Affairs. These statistics are derived from NCMEC and are not national statistics.
EL	121	103	123	NCMEC, Greek hotline for illegal internet content – Safeline, INTERPOL, Europol, Greek non-profit organisation – the Smile of the Child	
ES	31 474	-	-	Organisations acting in the public interest against CSA	Data not submitted for 2023 or 2024.
FI	11 248	16 781	13 954	NCMEC and other channels	For the 2024 data, the exact number of cases reported several times cannot be derived from

Country	Reports in 2022	Reports in 2023	Reports in 2024	Source of reports	Comments
					databases, but NCMEC estimates the number of these duplicate reports to be between 20 and 300. Duplicate reports appear to be most common with Snapchat. In addition to the data from NCMEC, Save the Children Finland reported on 71 domains and 439 URLs, the national initiative Sua varten somessa (For you in social media) reported 90 incidents, and other organisations/providers reported fewer than 10 incidents.
FR	227 645	335 408	164 516	NCMEC, NCECC (Canada's National Child Exploitation Crime Centre), INTERPOL National Central Bureaus, Europol secure information exchange network application (SIENA), Ministry of Interior platform – PHAROS	A total of 158 503 reports were received from NCMEC in 2024, of which 28 737 related to the financially motivated sexual extortion of minors and corruption of minors.
HR	11 693	8 010	8 900	Internet service provider	
HU	109 477	25 720	25 092	Providers and organisations acting in the public interest against CSA	There is no information available on cases reported several times or on which services the material was detected.
IE	9 168	10 785	13 334	NCMEC	Authorities do not register images or videos reported several times.
IT	4 607	7 389	9 001	Associations and providers	As not all data from 2024 have been processed yet, the numbers are not final.
LT	4 992	6 353	6 803	Not specified	
LU	789	1 641	2 112	NCMEC and BeeSecure (Luxembourg Safer Internet Centre)	Data on the breakdown of reports by NCMEC and BeeSecure for 2023 and 2024 were submitted but are unclear, as the numbers of reports by providers do not add up to the total amount indicated.

Country	Reports in 2022	Reports in 2023	Reports in 2024	Source of reports	Comments
LV	6	29	30	NCMEC, GRID COP, internet crimes against children child on-line protection system (ICACCOPS), Latvian Safer Internet Centre	The total number of reports submitted does not include reports in which criminal proceedings were not initiated after verification, because they are not counted separately. Only a portion of the reports contain indications that the offence is related to Latvia.
MT	840	1 943	272	National hotline (childwebalert.gov.mt), European network of Safer Internet Centres and hotlines managed by INSAFE and INHOPE – BeSmartOnline	
NL	36 536	70 057	70 351	Providers and organisations acting in the public interest against CSA	
PL	145	117	9 293	Providers and organisations acting in the public interest against CSA, one of them being Dyżurnet.pl	
PT	-	-	-	-	Data not submitted.
RO	5 705	1 254	13 384	Save the Children	The number of reports of online CSA, according to Romania, refers to CSA hosted by Romanian providers, but most of the clients were not from Romania.
SE	16 800	22 592	23 834	NCMEC	The total amount of incoming reports is not the same as the actual number of police reports to be investigated, because one police report can correspond to several reports by providers about the same user and because not all reports reflect crimes under Swedish criminal law. The number of police reports is considerably higher in 2023 than in 2022 and 2024. This is due to a national operation carried out in 2023, aimed at

Country	Reports in 2022	Reports in 2023	Reports in 2024	Source of reports	Comments
					dealing with all the unprioritised NCMEC reports from as far back as 2018.
SI	165	203	251	Providers and organisations acting in the public interest against CSA	Existing statistical data do not allow Slovenia to separate statistical data on offences investigated on the basis of reports submitted by providers and organisations from statistical data on other reports. There are no data available on the absolute number of cases, on the cases reported several times, or broken down by the type of provider on whose service the online CSA was detected. Additionally, the criminal offence of sexual assault on a person under 15 years of age under Article 173 of the Criminal Code was not included in the statistics provided, as in most cases this offence occurs in the physical environment, although to a lesser degree also virtually.
SK	7 628	9 601	9 017	Providers and organisations acting in the public interest against CSA	There is no information available on cases reported several times.
Total	**705 297**	**799 508**	**708 894**		

Given that NCMEC is the main source of reports, it is informative to see the number of reports concerning Member States that NCMEC received and forwarded to Member States[10]:



The breakdown per Member State of the total number of reports is as follows:

Table 7: NCMEC reports of online child sexual abuse concerning EU Member States in 2022, 2023 and 2024

Country	Total reports 2022 [11]	Total reports 2023 [12]	Total reports 2024 [13]
Austria	18 501	19 630	17 425
Belgium	50 255	41 926	26 752
Bulgaria	31 937	17 726	30 684
Croatia	11 693	16 339	8 821
Cyprus	7 361	7 564	5 750
Czechia	61 994	34 342	21 589
Denmark	30 215	12 048	10 330
Estonia	6 408	4 338	4 540
Finland	10 904	16 364	12 779
France	227 465	310 519	150 684
Germany	138 193	173 560	197 201
Greece	43 345	24 985	16 737

[10] The graph contains the total number of reports that the EU received, deduplicated, i.e. counted only once if the same report was sent to several Member States.

[11] NCMEC, '2022 CyberTipline Reports by Country', 2022, accessed on 26 May 2025.

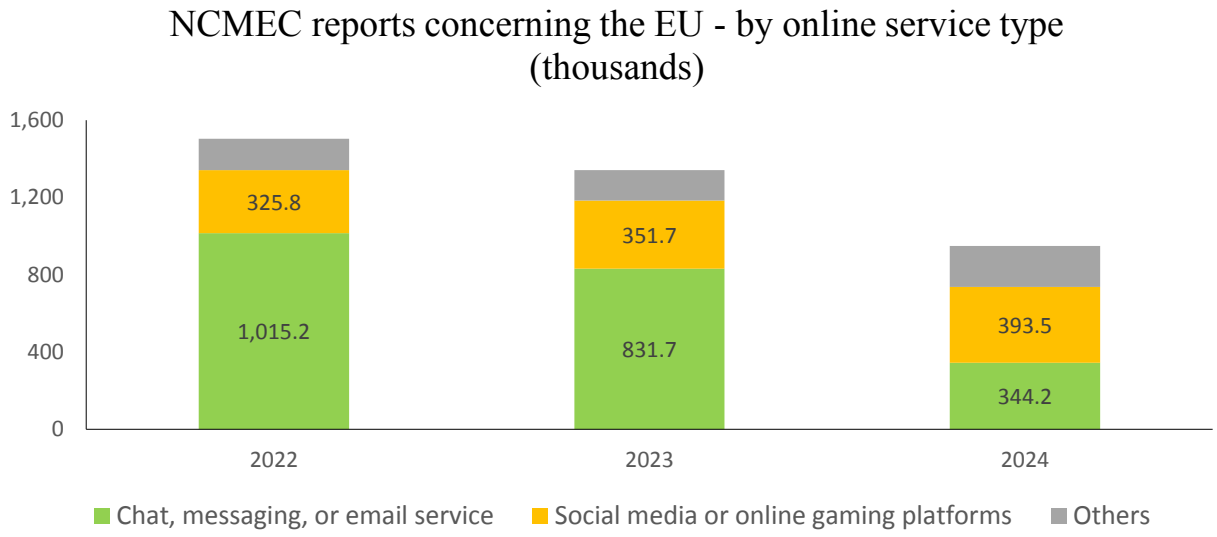
[12] NCMEC, '2023 CyberTipline Reports by Country', 2023, accessed on 26 May 2025.

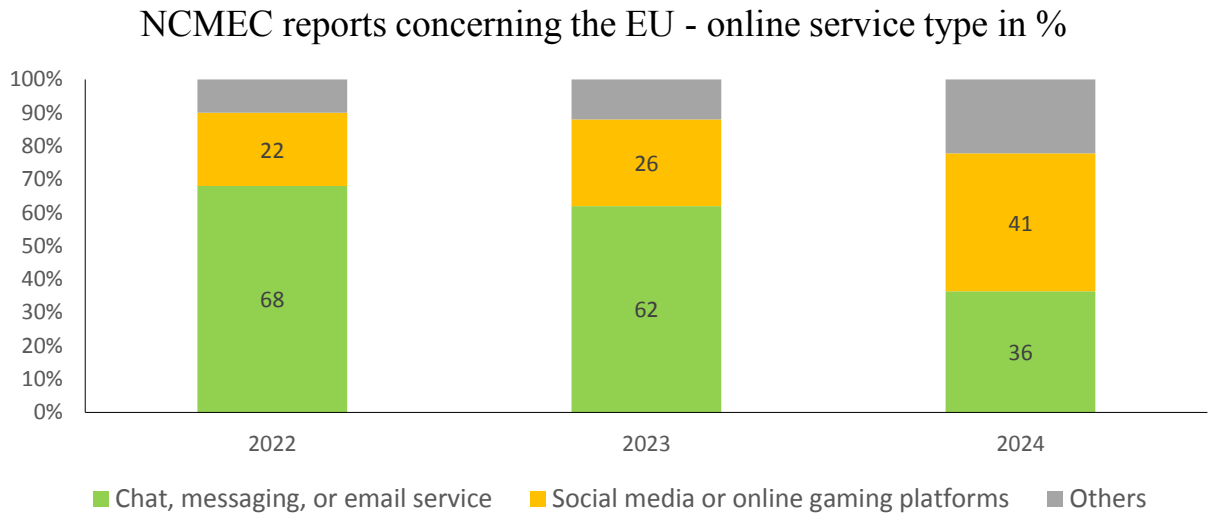
[13] NCMEC. In 2024, NCMEC started to report in its website ('2024 CyberTipline Reports by Country') the total number of referrals sent to each country. The same referral is sent to several countries, if it concerns all those countries. The data reported in table 7 for 2022, 2023 and 2024 is deduplicated reports, i.e. the same report is only counted once.

Country	Total reports 2022 [11]	Total reports 2023 [12]	Total reports 2024 [13]
Hungary	109 434	25 643	16 718
Ireland	19 770	13 265	13 604
Italy	96 512	90 424	75 274
Latvia	3 688	4 671	6 618
Lithuania	16 603	12 005	7 682
Luxembourg	2 004	3 000	2 115
Malta	4 713	1 713	1 233
Netherlands	57 012	72 913	68 611
Poland	235 310	108 800	79 174
Portugal	42 674	45 675	24 707
Romania	96 287	133 054	44 424
Slovakia	39 748	13 164	8 647
Slovenia	14 795	6 204	4 685
Spain	77 727	104 748	68 733
Sweden	48 883	29 237	25 300
Total	**1 503 431**	**1 343 857**	**950 817**

The significant disparity between the number of reports NCMEC lists as having sent to the Member State, and the number of reports the Member State lists as received suggests that the Member States' data collection and reporting is not complete.

The NCMEC statistics per Member State do not make a distinction between the source of the report, in particular whether the report stemmed from a number-independent interpersonal communications service. However, NCMEC does provide statistics about the overall number of reports concerning the EU stemming from number-independent interpersonal communications services, such as from a chat, messaging or email service. NCMEC also shared figures on reports stemming from social media or online gaming platforms, including their integrated messaging or chat services.





There is a significant drop (30%) in 2024 in the number of reports concerning the EU. This reflects a global trend, with reports reaching 31.9 million in 2022 and 35.93 million in 2023, before dropping to 19.85 million in 2024. NCMEC attributes this drop in part to a reduction of reports from interpersonal messaging services as those services move to end-to-end encryption and providers stop detection efforts.[14] The drop in share of reports from interpersonal messaging services would indeed seem to indicate that a large portion of the reduction can be attributed to less reporting from such services.

[14] Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary, 11 March 2025.

2.2.2. The number of children identified

Most Member States provided statistics on the number of children identified pursuant to Article 8(1)(b) of the Regulation. Three Member States did not provide any data (Belgium, Portugal and Romania), while others only provided data for certain years (e.g. Finland for 2023 and 2024 and Spain for 2022). Many Member States were not able to differentiate by gender.

Several Member States reported only partial statistics, pointing out, for instance, that data are not available because they are not collected as part of the national statistical data collection, or that national authorities do not record these statistics (Belgium, France and Finland), or that data are not disaggregated by gender in the national statistical data collection (Czechia, Cyprus, Lithuania, Hungary and the Netherlands). In many Member States, the data below do not differentiate between child victims of CSA online and offline, and it is therefore possible that the data do not correspond to the actual number of instances of online CSA (e.g. Germany, Cyprus and Luxembourg). The data therefore include both victims who were identified based on a report from a provider and cases where, for example, the victims themselves or a third party may have reported the criminal offence (e.g. Germany and Luxembourg). In other cases, the number of identified child victims of CSA only refers to citizens of that country or people who reside there, thus excluding children of other nationalities and unidentified children (e.g. Latvia and Lithuania).

Table 8: Number of children identified, differentiated by gender

Country	2022		2023		2024		Comments
	Female (F)/ Male(M)/ Gender not identified	Total	F/M/ Gender not identified	Total	F/M/Gender not identified	Total	
AT	4/2	6	9/4	13	3/3	6	Number of children identified on the basis of NCMEC reports.
BE	-	-	-	-	-	-	Data not available.
BG	50/12	62	25/27	52	32/28	60	
CY	-	102	-	106	-	131	Data differentiated by gender not available. The total numbers refer to victims for all child sexual exploitation cases investigated.
CZ	-	45	-	53	5/15	20	Data differentiated by gender are available only for 2024. Children accounted for in 2024 are victims of sextortion.
DE	-	18 379	14 979/ 4795	19 774	-	19 344	As the statistics do not differentiate by the reason for, or origin of, the investigations, the data may contain cases detected solely due to a provider's report as well as cases not related to the internet in any way.
DK	62/70	132	22/35	57	62/43	105	The statistics are based on numbers from the police case management system (POLSAS) and are not final, as some cases are still pending. Also, children identified through other means, including in previous cases or in an international context, are not represented in the statistics.

Country	2022		2023		2024		Comments
	Female (F)/ Male(M)/ Gender not identified	Total	F/M/ Gender not identified	Total	F/M/Gender not identified	Total	
EE	24/23	47	22/29	51	19/14	33	
EL	9/0	9	26/1	27	14/0	14	
ES	80/39	119	-	-	-	-	Data for 2023 and 2024 not submitted.
FI	-	Not available	-	526	-	1 045	The number of child victims is likely to be larger, as labelling the case as online CSA requires manual classification efforts.
FR	-	n/a	-	5	-	60	
HR	4/0	4	6/0	6	6/17	23	
HU	-	30	-	12	-	200	Data differentiated by gender not available.
IE	25/26	51	50/65	115	20/53	73	
IT	-	385	-	434	-	500	Identified cases of sextortion accounted for: 21 F and 111 M in 2022; 20 F and 117 M in 2023; 21 F and 109 M in 2024. Cases of grooming accounted for: 75 F and 46 M in 2022; 81 F and 82 M in 2023; 124 F and 11 M in 2024.
LT	-	10	-	25	-	21	The numbers refer to children identified as victims who are citizens of or reside in Lithuania. Most investigations concern unidentified children, mostly in connection with material produced in a foreign country.
LU	-	0	3/0	3	1/0	1	The numbers are not necessarily linked to online detection.

Country	2022		2023		2024		Comments
	Female (F)/ Male(M)/ Gender not identified	Total	F/M/ Gender not identified	Total	F/M/Gender not identified	Total	
LV	-	0	5/1	6	8/0	8	The numbers refer only to children who reside in Latvia.
MT	2/4	6	408/470/11	889	9/9	18	The data for 2023 refer to children identified by the Foundation for Social Welfare Services (FSWS), while the data for 2022 and 2024 refer to law enforcement statistics.
NL	-	n/a	-	676	-	359	Data differentiated by gender not available.
PL	520/82/23	566	133/34/140	307	109/25	134	
PT	-	-	-	-	-	-	Data not submitted.
RO	-	-	-	-	-	-	Data not submitted. No Romanian victims or materials produced in Romania have been identified, which RO attributes to most of the materials already being known internationally.
SE	3/0	3	16/10/2	28	53/65	118	Children identified in cases that did not result in police reports are excluded from the statistics. In some cases, even if the victim was identified, the investigation did not necessarily lead to a conviction. The number of children identified through chatlogs are included in the statistics.

Country	2022		2023		2024		Comments
	Female (F)/ Male(M)/ Gender not identified	Total	F/M/ Gender not identified	Total	F/M/Gender not identified	Total	
SI	83/15	98	121/38	159	161/30	191	The statistical data are obtained from the current database and are subject to change.
SK	11/6	17	3/2	5	7/2	9	
TOTAL		**20 071**		**23 329**		**22 473**	

As Member States mostly reported partial numbers for the periods in question or were not able to differentiate according to whether voluntary detection was at the origin of the investigation, and a few did not submit data, it is not possible to calculate the total number of children identified as victims on the basis of reports of online CSA in the EU. Nonetheless, it can be inferred from the data and the information provided by Member States that a significant number of victims have been identified with the help of voluntary reporting in line with the Regulation.

2.2.3. The number of perpetrators convicted

While most Member States complied with their obligation to provide statistics on the number of perpetrators convicted, three Member States did not provide any data pursuant to Article 8(1)(c) of the Regulation (Belgium, Cyprus and Spain). Several Member States failed to provide statistics for at least one of the years in question pursuant to Article 8(1)(c), mostly because data were not available (Belgium, Germany, Ireland, Spain, France, Cyprus, Malta, Portugal and Finland).

Member States mostly reported fragmented and incomplete data on the number of perpetrators convicted and used different criteria to record the relevant information, as shown in the table below.

Table 9: The number of perpetrators convicted

Country	Number of convictions 2022	Number of convictions 2023	Number of convictions 2024	Comments
AT	768	323	334	
BE	-	-	-	Due to technical issues, the data is not available until end of 2025.
BG	17	52	60	
CY	No convictions	Data not available	Data not available	Statistics are not available since police officers are not always informed about the outcomes of court cases.
CZ	33	25	12	
DE	1 847	1 779	Data not available	The German federal government indicated having no data on criminal proceedings, as these data were collected solely in the 16 federal states by prosecutors and courts and only delivered to the German Federal Statistical Office (*Statistisches Bundesamt* – STBA). The German federal government found figures for 2022 and 2023 on the STBA website which it reported here.
DK	318	175	44	The statistics are based on numbers from POLSAS and are not final, as some cases are still pending. They are also subject to a number of caveats based on the specificities of national data collection.
EE	1	13	4	The numbers include only convictions resulting from NCMEC reports, provided by Google, Dropbox, Facebook Messenger, Instagram Messenger, KIK Messenger, Snapchat and Twitch.
EL	10	13	18	
IE	Data not available	80	72	The figures for convicted perpetrators are still under review. The data submitted refer to the charges and summons per calendar year.
ES	Data not available	-	-	Data not submitted.
FI	Data not available	3 621	Data not available	Statistics provided for 2023 relate to the overall number of convictions for all CSA-related crimes (i.e. both online and offline). New legislation on sexual offences entered into force in 2023, but the statistics also contain the number of persons sentenced under the old Criminal Code in 2023.

Country	Number of convictions 2022	Number of convictions 2023	Number of convictions 2024	Comments
FR	1 124	1 223	Data not available	
HR	157	146	155	
HU	8	16	12	
IT	627	668	395	The data are underestimated, due to incomplete references from courts. The 2024 data covers convictions for a reduced range of offences compared with the 2022 and 2023 data.
LT	3	6	2	
LU	11	20	21	The statistics do not differentiate between offences committed online and offline. Moreover, convictions recorded for the years provided may be linked to reports made in the previous years.
LV	1	12	15	The data according to differentiation by gender are as follows: 1 male in 2022; 1 female and 11 males in 2023; 15 males in 2024.
MT	-	-	-	Data per year not available.
NL	190	240	240	The figures are indicative, rounded to tens, and the most recent numbers are still preliminary.
PL	194	144	125	
PT	3	3	Data not available	
RO	690	804	715	
SE	123	95	14	The number only concerns convictions related to NCMEC reports, and following final judgments.
SI	19	22	26	
SK	137	118	125	The statistics for 2024 are not final. The data from 2022 and 2023 do not differentiate between the number of convictions resulting from NCMEC reports and those resulting from other reports, or between offences committed online and offline.

The number of convictions is not equal to the number of perpetrators convicted, as a person might be convicted for one or more offences of online CSA. Also, the statistics on convictions reported for a certain period are not necessarily linked to the reports received in that given period (e.g. Estonia and Luxembourg). In some instances, no statistics were collected on whether reports of online CSA (e.g. via NCMEC) led to convictions, or that convictions resulted from the information provided by a provider or a public organisation. Only Estonia and Sweden explicitly confirmed that the statistics showed only convictions resulting from NCMEC reports. Many Member States reported that the numbers were not final, because investigations were still ongoing or cases were still pending or subject to appeals (Bulgaria, Denmark, Italy, the Netherlands and Slovakia). In certain instances, the data reported by the Member States do not differentiate between offences committed online and offline (Luxembourg, Slovakia, Finland and Sweden).

The way statistical data are gathered at national level does not allow for a comprehensive overview of the number of perpetrators convicted for online CSA in the EU. Nor is it currently possible, on the basis of the available data, to establish a clear link between these convictions and the reports submitted by providers and organisations acting in the public interest against CSA in given reporting periods.

2.3. Developments in technological progress

Technologies currently used to detect CSA online include technologies and tools to detect known CSAM (i.e. material previously confirmed as constituting CSAM), new CSAM (i.e. material other than known CSAM) and solicitation of children for sexual purposes (also known as 'grooming').

The non-exhaustive list of examples below includes some of the most widely used tools. Many of these tools are made available to providers, law enforcement authorities and other organisations that can prove a legitimate interest. These tools are typically combined with human review to improve accuracy.

2.3.1. Detection of known CSAM

Existing technologies to detect known CSAM rely on automatic analysis of content[15] and are typically based on hashing. Hashing technology is a type of digital fingerprinting. It creates a unique digital signature (a 'hash') of an image, which is then compared against signatures (hashes) of other photos to find copies of the same image. This technology only detects matching hashes and does not 'see' any material that does not match the hash. These hash values are also not reversible, and therefore cannot be used to recreate an image.

Many variations and implementations of hashing technology exist, including cryptographic hashing to identify exact matches, and perceptual hashing to identify visually similar content even with minor modifications (e.g. images cropped, resized or with a filter) [16]. Tools identified as being

[15] Providers do not consider metadata as an effective tool in detecting CSAM. See e.g. Pfefferkorn R.,, 'Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers' in *Journal of Online Trust and Safety*, Vol. 1, No 2, Stanford Internet Observatory, 28 February 2022.

[16] Tech Coalition, 'Annual Report 2024', 2024, p. 28.

used for detecting known CSAM include: (i) Microsoft PhotoDNA [17]; (ii) Google CSAI Match [18]; (iii) Apple NeuralHash; (iv) PDQ and TMK+PDQF [19]; (v) MD5 Hash Matching; and (vi) Safer (Thorn) [20].

The most widely used tool is Microsoft PhotoDNA, which has been in use for over 15 years. The rate of false positives is estimated, on the basis of testing, to be no more than 1 in 50 billion [21]. While the original PhotoDNA detects known CSAM in images, a version for detecting it in videos is also available [22].

The technology is continuously being improved. In May 2023, Microsoft announced the deployment of new matching capabilities that enable swifter searching (around 350 times faster), while reducing the cost of the matching process with no loss of accuracy. According to Microsoft, the new library also enables more comprehensive detection of flipped or rotated images.

2.3.2. Detection of new CSAM

Technologies currently used for the detection of new CSAM include classifiers and AI. A classifier is an algorithm that sorts data into labelled classes or categories of information through pattern recognition. Examples of classifiers include those that can detect nudity, shapes or colours. Classifiers need to be trained on data and their accuracy improves the more data they are fed.

Tools to detect new CSAM include: (i) Safer Predict (Thorn) [23]; (ii) Google Content Safety API [24]; and (iii) Facebook's AI technology [25].

For the detection of new CSAM, the accuracy rate (defined in terms of avoidance of false positives)can be set significantly above 90%. For example, Thorn indicates that its CSAM classifier can be set to a 99% precision rate (for both known and new CSAM), meaning a 0.1% false positive rate [26]. These metrics – and the corresponding false negatives rate – are likely to improve with increased usage and feedback.

---

17 Microsoft, 'PhotoDNA | Microsoft', accessed on 26 May 2025. See also Microsoft, 'How PhotoDNA for Video is being used to fight online child exploitation – On the Issues', 12 September 2018, accessed on 26 May 2025.

18 Google, 'Discover our child safety toolkit', accessed on 26 May 2025.

19 Meta, 'Open-Sourcing Photo- and Video-Matching Technology to Make the Internet Safer', 1 August 2019, accessed on 26 May 2025. See also Medium, 'Image Similarity: PDQ algorithm for real-time similarity comparison against image store | by Darwinium | Medium', 4 July 2022, accessed on 26 May 2025.

20 Safer, 'Power trust and safety with purpose-built solutions', accessed on 26 May 2025.

21 Farid H., House Committee on Energy and Commerce, Fostering a healthier Internet to protect consumers, Testimony, 16 October 2019.

22 Microsoft, 'How PhotoDNA for video is being used to fight online child exploitation', 12 September 2018, accessed on 26 May 2025.

23 Thorn, 'Introducing Safer Predict: using the power of AI to detect Child Sexual Abuse and Exploitation Online', 19 July 2024, accessed on 26 May 2025.

24 Google, 'Fighting child sexual abuse online', accessed on 26 May 2025.

25 See here and here for more information on Facebook's tool to proactively detect child nudity and previously unknown child exploitative content using artificial intelligence and machine learning.

26 Thorn, Thorn's Automated Tool to Remove Child Abuse Content at Scale Expands to More Platforms through AWS Marketplace, 24 May 2021.

The industry's capabilities to detect new CSAM are expanding: an example is the new CSAM detection tool developed by Discord using CLIP (an open-source algorithm originally created by OpenAI), trained to associate images and text, thereby allowing the tool to understand the semantic relationships between them. By applying this method to CSAM detection, the tool was able to detect both known and unknown CSAM with positive results. Discord made this technology open source to share the innovation with other companies for free and to contribute to the broader fight against CSAM online [27].

2.3.3. Detection of solicitation of children for sexual purposes

For the detection of grooming in time before the child shares CSAM, in contrast to the exchange of images or videos, text-based tools are particularly relevant. Tools to detect grooming in text-based communications detect patterns which point to grooming, without being able to deduce the substance of the content. Suspicious conversations are rated on a series of characteristics and assigned an overall probability rating, indicating the estimated probability that the conversation constitutes grooming. These ratings can serve to flag conversations for additional human review. Similar to the detection of CSAM, company can decide where to set the probability threshold, with the same consequences as outlined above when it comes to false positives or negatives: a higher probability threshold means that fewer instances that do not constitute grooming are flagged for review, but also that more instances of grooming may be missed.

Tools used for text detection operations include: (i) Microsoft's Project Artemis[28]; (ii) Amazon Rekognition[29]; (iii) Twitch's Spirit AI technology[30]; (iv) Meta's machine learning 'ranking' classifier (combining internal language analysis tech with meta data); (v) Roblox chat filtering[31]; (vi) Yubo tool for grooming detection; (vii) Safer Predict's Text Detection tool[32]; and (viii) Hive Text Moderation[33].

Yubo has reported that the accuracy rate for text-based grooming detection on its services reached 87% on average[34], meaning that, out of 100 instances of suspected grooming automatically flagged

---

27 Tech Coalition, 'Annual Report 2024', 2024, p. 28.

28 Microsoft's Project Artemis was developed in collaboration with The Meet Group, Roblox, Kik and Thorn.

29 Amazon, Amazon 'Rekognition'. See also Amazon, 'What is Amazon Rekognition?', accessed on 26 May 2025.

30 For more information see: Twitch, 'Our Ongoing Work to Combat Online Grooming', 22 November 2022, accessed on 26 May 2025.

31 Roblox filters posts and chats for players age 12 and under for inappropriate content and to prevent personal information from being posted, e.g. home addresses. This filtering system covers all areas of communication on Roblox, public and private. Roblox, 'Safety Features: Chat, Privacy & Filtering', accessed on 26 May 2025.

32 See: Safer, 'Enhancing Platform Safety: insights from Safer Predict's Text Detection Beta Period', 29 July 2024 and 'Announcing Safer Predict: AI-Driven CSAM & CSE Detection', 19 July 2024, accessed on 26 May 2025.

33 Hive Moderation, ' Automated Models with a human-level understanding of textual content' and 'Text Moderation - Overview', accessed on 26 May 2025. The text classification model is trained on a large proprietary corpus of labelled data across multiple domains (including but not limited to social media, chat, and livestreaming apps), and is able to interpret full sentences with linguistic subtleties. Pattern-matching algorithms will search sentences for a set of predefined patterns that are commonly associated with harmful content, including CSA.

34 Yubo, 'CSAM EU Reporting obligations', 31 January 2025, accessed on 26 May 2025. According to Yubo, accuracy is calculated as the number of cases automatically flagged as grooming that were confirmed as such upon human review.

to human moderators, 87 were confirmed as being grooming. Research shows that machine learning methods for detecting online grooming can reach an accuracy of 92%, excelling in capturing complex, non-linear patterns essential for analysing nuanced online interactions[35].

The Safer Predict Text Detection tool uses a machine learning text classification model to detect child sexual exploitation. It analyses text and assigns a risk score based on the content's likelihood of being associated with harmful behaviour, such as messages related to the sharing of CSAM, including self-generated content, as well as messages related to offline abuse of children and sexual extortion activities.

Other AI tools to combat online grooming are being developed. For instance, the CESAGRAM project by Missing Children Europe, which is focused on understanding and interrupting the mechanisms behind grooming, plans to produce an AI tool to help prevent grooming, through linguistic analysis to detect grooming activities based on natural language processing techniques [36].

2.3.4. Use of generative AI for the purpose of child sexual abuse

The threat landscape linked to the misuse of generative AI for CSA has rapidly evolved in recent years. The use of widely available generative AI (also 'GAI') tools can be weaponised to harm children, and the technology's use in child sexual exploitation has increased. This technology can be used to create or alter images, provide guidelines for how to groom or abuse children, or even simulate the experience of an explicit chat with a child. In 2024, NCMEC reported a 1 325% increase in reports involving generative AI: from 4 700 reports in 2023 to 67 000 in 2024[37]. Additionally, an IWF snapshot study of a dark web CSAM forum found over 20 000 AI-generated images posted in a one-month period, where more than 3 000 depicted criminal CSA activities[38].

Offenders use GAI to exploit children in a variety of ways, including those listed below.[39]

- Text to text: using text prompts to generate guides/tutorials/suggestions on how to groom and sexually abuse children.
- Text to image: entering text prompts to generate new CSAM or alter previously uploaded files to make them sexually explicit.

---

35 Leiva-Bianchi M. et al. (eds.), Effectiveness of machine learning methods in detecting grooming: a systematic meta-analytic review, in *Scientific Reports 15*, No 9008, 2025. The study presents a systematic review and meta-analysis of the use of machine learning methods for detecting online grooming. The results highlight the efficacy of certain algorithms and contribute to the identification of online predators. The study defines accuracy as the indication of the model's overall correctness in its predictions, and precision as the number of accurately detected positive instances.

36 For more information see Missing Children Europe, 'CESAGRAM', accessed on 26 May 2025.

37 NCMEC, '2024 CyberTipline Report', 2024, accessed on 26 May 2025.

38 Internet Watch Foundation, 'Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery', accessed on 26 May 2025.

39 NCMEC, Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism, 'Ending the Scourge: the need for the STOP CSAM Act', 11 March 2025, pp. 2-4.

- Image to image (altering known CSAM to create new CSAM): uploading known CSAM to generate new CSAM based on existing images, including altering or adding new abusive elements (e.g. bondage or other forms of abuse) to existing images.
- Image to image (altering an innocuous image to create an exploitative image): uploading innocuous images of a child to generate sexually explicit or exploitative images of the child (e.g. nudifying apps). GAI is also used in this manner to perpetrate financial sextortion against children.

NCMEC has flagged the lack of regulated safety protocols, the speed at which GAI tools have proliferated through apps, platforms and open-source accessibility, and the relative ease of using this technology. Moreover, the proliferation of AI-generated CSA creates new and significant challenges for law enforcement, including with respect to victim identification, due to the difficulty of determining whether the images are real or synthetic, which in turn can deviate efforts from cases involving real children in urgent need of safeguarding[40].

3. CONCLUSIONS

Implementation measures taken by providers

The providers' reporting showed that they have been detecting and reporting online CSA under the Regulation using a variety of detection technologies and processes. All the providers reported sending these reports to NCMEC. For the year 2024, the providers failed to comply with their obligation to submit the report on the processing of personal data by using the standard form set out in the Commission implementing act that was adopted on 25 November 2024. As a result, the reports submitted still have shortcomings that affect the overall comparability of the data.

Implementation measures taken by Member States

The reports submitted by Member States still have issues similar to those highlighted in the first report on the implementation of the Regulation. The data submitted by Member States appear incomplete and fragmented. It is therefore not possible to provide a comprehensive and reliable overview of the number of reports of detected online CSA, the number of children identified, and the number of perpetrators convicted. The disparities between NCMEC data and Member States' data confirm that the Member States' data collection and reporting still have significant shortcomings.

General considerations

Overall, this report shows considerable disparities in the reporting on data on combating online CSA under the Regulation, by both providers and Member States. Greater standardisation of available data and the reporting thereof.

[40] NCMEC, Testimony of Michelle DeLaune, President and CEO National Center for Missing & Exploited Children, to the United States Senate Committee on the Judiciary Subcommittee on Crime and Counterterrorism, 'Ending the Scourge: the need for the STOP CSAM Act', 11 March 2025, p. 4.

The available data show that, while materials automatically flagged as possible CSAM are overwhelmingly confirmed as such upon human review, a small fraction may turn out, upon human review, not to be CSAM. While the rate of false positives is as low as 1 in 50 billion for some tools, this fraction also depends on the provider's choice to tailor the tool's accuracy settings to minimise false negatives, with the consequent increase in false positives to subsequently filter out by human review.

The data also suggest large variations in the number of review requests and review success rates, from which it is not possible to extract conclusions, given the lack of information shared by the providers on, in particular, the scope of the review requests and the reasons for reinstatement.

As regards the requirements of Article 9(2) on the conditions for processing data, the information provided indicates that the technologies used correspond to technological applications designed for the sole purpose of detecting and removing online CSAM and reporting it to law enforcement authorities and organisations acting in the public interest against CSA. No information was submitted by the providers on whether the technologies were deployed in line with the state of the art and in the least privacy-intrusive way, or on whether a prior data protection impact assessment, as referred to in Article 35 of Regulation (EU) 2016/679, and a prior consultation procedure, as referred to in Article 36 of that Regulation, had been conducted.

On the proportionality of Regulation (EU) 2021/1232, the question is whether the Regulation achieves the balance sought between, on the one hand, achieving the general interest objective of effectively combating the extremely serious crimes at issue and the need to protect the fundamental rights of children (e.g. dignity, integrity, prohibition of inhuman or degrading treatment, private life, rights of the child, etc.) and, on the other hand, safeguarding the fundamental rights of the users of the services covered (e.g. privacy, personal data protection, freedom of expression, effective remedy, etc.). The available data are insufficient to provide a definitive answer to this question. It is not possible nor would it be appropriate to apply a numerical standard when assessing proportionality in terms of the number of children rescued, given the significant negative impact on a child's life and rights that is caused by sexual abuse. Nonetheless, in light of the above, there are no indications that the derogation is not proportionate.

While the shortcomings of the data make it not possible to have the complete picture, the data that are available show that thousands of children were identified in the reporting period and that millions of images and videos were removed from circulation, reducing secondary victimisation. Therefore, voluntary reporting in line with this Regulation appears to make a significant contribution to the protection of a large number of children, including from ongoing abuse.

At the same time, important shortcomings identified in the implementation of this Regulation, including greater standardisation of available data and reporting therefore for a better picture of the relevant activities in the fight against this crime and the use of specific indicators to detect illegal CSAM and verification of material by an independent centre, have been addressed in the Commission Proposal for a Regulation laying down rules to prevent and combat child sexual

abuse[41]. Its adoption by the co-legislators remains a priority. It is essential to ensure that no legal gaps arise between the existing and the future, improved legal framework, and that, in the meantime, the current legal framework continues to be applied in the most effective manner.

[41] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final.