EUROPESE
COMMISSIE

Brussel, 19.12.2023
COM(2023) 797 final

VERSLAG VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

over de uitvoering van Verordening (EU) 2021/1232 van het Europees Parlement en de Raad van 14 juli 2021 betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG ten aanzien van het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ten behoeve van de bestrijding van online seksueel misbruik van kinderen

INHOUD

LIJST VAN TERMEN EN ACRONIEMEN

Term/acroniem	Definitie
AI	Artificiële intelligentie
API	Application Programming Interface (applicatieprogramma-interface)
CG-CSAM	Computer-generated Child Sexual Abuse Material (met een computer gegenereerd materiaal betreffende seksueel misbruik van kinderen)
ChatGPT	ChatGPT (Chat Generative Pre-trained Transformer) is een vorm van generatieve AI. Deze chatbot is gebaseerd op een groot taalmodel en is ontwikkeld door OpenAI. Gebruikers kunnen er een gesprek mee in een bepaalde richting doen gaan qua lengte, vorm, stijl, detailniveau en taalgebruik.
Classifiers	Een algoritme dat als vorm van artificiële intelligentie gegevens onderbrengt in gelabelde klassen of categorieën
Content Safety API classifier	Deze API-classifier van Google voor de veiligheid van inhoudelijk materiaal gebruikt programmatische toegang en artificiële intelligentie om miljarden beelden te helpen classificeren en prioriteren voor onderzoek
CSA	Child Sexual Abuse (seksueel misbruik van kinderen)
CSAI Match	Een door programmeurs van YouTube ontwikkelde techniek om nieuwe uploads te herkennen van video's met eerder vastgesteld seksueel misbruik van kinderen
CSAM	Child Sexual Abuse Material (beelden en video's die seksueel misbruik van kinderen weergeven)
CSA-richtlijn	Richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van Kaderbesluit 2004/68/JBZ van de Raad (PB L 335 van 17.12.2011, blz. 1)
CSEA	Child Sexual Exploitation and Abuse (seksuele uitbuiting en seksueel misbruik van kinderen)
CSA online	De gemeenschappelijke term voor de drie in de CSA-richtlijn gedefinieerde typen seksueel misbruik van kinderen: kinderpornografie, pornografische voorstellingen en het benaderen van kinderen voor seksuele doeleinden ("grooming"), zoals gedefinieerd in artikel 2, punt 4, van de tijdelijke verordening
EU	Europese Unie
AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening

	gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1)
Grooming	Daders die vertrouwen en een relatie met een kind opbouwen om toenadering tot de minderjarige te zoeken met het oog op seksuele uitbuiting of seksueel misbruik. Formeel bekend als het benaderen van kinderen, zoals gedefinieerd in artikel 6 van de CSA-richtlijn.
Hash	Een unieke, door een wiskundig algoritme (via "hashing") gecreëerde digitale code die de handtekening of hashwaarde van het betreffende bestand wordt
Tijdelijke verordening	Verordening (EU) 2021/1232 van het Europees Parlement en de Raad van 14 juli 2021 betreffende een tijdelijke afwijking van sommige bepalingen van Richtlijn 2002/58/EG ten aanzien van het gebruik van technologieën door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten voor de verwerking van persoonsgegevens en andere gegevens ten behoeve van de bestrijding van online seksueel misbruik van kinderen (PB L 274 van 30.7.2021, blz. 41)
LLM	Een Large Language Model (groot taalmodel) is een soort model binnen de artificiële intelligentie dat met zelflerende deeplearning-algoritmen is getraind om grote hoeveelheden geschreven menselijke taal en tekstgegevens te herkennen, te genereren, te vertalen en/of samen te vatten
MD5	Een algoritme voor cryptografische berichtauthenticatiecodes voor gebruik op het internet
Meta SSN++	Een door Meta ontwikkeld AI-model dat bijna exacte kopieën kan opsporen
NCMEC	National Center for Missing and Exploited Children (nationaal centrum voor vermiste en misbruikte kinderen), een private organisatie zonder winstoogmerk in de VS waaraan onlinedienstverleners volgens de Amerikaanse wetgeving gevallen van mogelijk seksueel kindermisbruik moeten melden die zij in hun netwerken aantreffen
PDQ en TMK+PDQF	Door Facebook gebruikte instrumenten om schadelijke inhoud te herkennen. Met de PDQ-technologie kunnen foto's worden vergeleken; met de TMK+PDQF-technologie kunnen video's worden vergeleken.
PhotoDNA	Het meest gebruikte, op hashingtechnologie gebaseerde instrument. Het is gratis verkrijgbaar en is gebaseerd op een licentieovereenkomst waarmee misbruik en gebruik voor andere doeleinden dan opsporing van CSA moet worden vermeden.

1. INLEIDING

Volgens artikel 9 van de tijdelijke verordening (hierna ook “de verordening” genoemd) moet de Commissie een uitvoeringsverslag opstellen op basis van de door aanbieders van interpersoonlijke communicatiediensten (hierna “aanbieders” genoemd) ingediende verslagen over de verwerking van persoonsgegevens en op basis van de door de lidstaten verstrekte statistieken. Conform dat artikel kijkt de Commissie in het uitvoeringsverslag met name naar:

a) de voorwaarden voor de verwerking van persoonsgegevens en andere gegevens die op grond van de verordening zijn verwerkt;

b) de evenredigheid van de afwijking waarin de verordening voorziet, met inbegrip van een beoordeling van de door de lidstaten uit hoofde van artikel 8 ingediende statistieken;

c) ontwikkelingen in de technologische vooruitgang wat betreft de activiteiten die binnen het toepassingsgebied van de verordening vallen, en de mate waarin die ontwikkelingen zorgen voor meer nauwkeurigheid en voor een vermindering van het aantal fouten en de foutverhoudingen (fout-positieve resultaten).

Dit uitvoeringsverslag op grond van de tijdelijke verordening is gebaseerd op de gegevens in de verslagen van aanbieders en de lidstaten overeenkomstig respectievelijk artikel 3, lid 1, punt g), vii), en artikel 8 van de tijdelijke verordening. In die verslagen kwamen aanzienlijke verschillen aan het licht wat betreft de beschikbaarheid van gegevens, de soorten verzamelde gegevens en dus ook de vergelijkbaarheid van de gegevens die de aanbieders en de lidstaten verzamelden. Aangezien de verordening geen model voor de rapportage bevat, dienden de aanbieders verschillende soorten gegevens in die niet altijd vergelijkbaar waren. De diensten van de Commissie hebben daarop vervolgmaatregelen getroffen om te waarborgen dat de gegevens correct worden geïnterpreteerd. De meeste lidstaten konden de gegevens niet op tijd leveren en een aantal van hen konden geen gegevens leveren voor de publicatie van dit verslag. Dat heeft de tijdigheid, volledigheid en bruikbaarheid van het verslag aanzienlijk beïnvloed. Ondanks de inspanningen om de samenhang en de vergelijkbaarheid van de gegevens te waarborgen, blijven er aanzienlijke verschillen bestaan. Dat vindt zijn weerslag in de onderstaande tabellen, die niet op alle punten gegevens bevatten voor alle aanbieders of lidstaten.

Met dit uitvoeringsverslag wordt beoogd om op basis van de beschikbare gegevens een feitelijk overzicht te geven van de stand van zaken met betrekking tot de uitvoering van de tijdelijke verordening. Het verslag bevat geen interpretatie van de verordening of standpunten over de wijze waarop de verordening in de praktijk is uitgelegd en toegepast.

2. UITVOERINGSMAATREGELEN

2.1. Verwerking van persoonsgegevens door aanbieders (artikel 3, lid 1, punt g), vii))

In artikel 3, lid 1, punt g), vii), van de tijdelijke verordening zijn de voorwaarden vastgesteld waaronder aanbieders die handelen op grond van de in de verordening bepaalde afwijking, uiterlijk 3 februari 2022 en daarna elk jaar uiterlijk 31 januari een verslag moeten publiceren over de verwerking van persoonsgegevens uit hoofde van de verordening en dat verslag moeten indienen bij de bevoegde toezichthoudende autoriteit en de Commissie. Google, LinkedIn, Meta, Microsoft en X (voorheen Twitter)[1] dienden verslagen in over 2021 en 2022.

2.1.1. Type en volumes van de verwerkte gegevens

De aanbieders brachten verslag uit over de verwerking van zowel inhouds- als verkeersgegevens.

Wat betreft inhoudsgegevens die zijn verwerkt om online seksueel misbruik van kinderen op te sporen, hebben alle genoemde aanbieders beelden en video's gemeld. Ze hebben voornamelijk gebruikgemaakt van de hashmatchingtechnologieën PhotoDNA en MD5 om materiaal op te sporen dat identiek is aan al eerder herkend materiaal betreffende seksueel misbruik van kinderen (hierna "CSAM" genoemd). Het instrument CSAI Match van Google werd gebruikt om digitale vingerafdrukken van video's op platformen te maken en die te vergelijken met de bestanden in de vingerafdrukopslag van Google/YouTube (LinkedIn). Ook werd de inzet van automatische technologie (machinaal leren door artificiële intelligentie) en menselijke toetsing gemeld (bv. door Google). Google en LinkedIn bevestigden dat zij ook CSAM hebben geïdentificeerd dat niet overeenkwam met eerder herkend CSAM. Geen van de vijf aanbieders die gegevens indienden, meldde gegevens over het opsporen van het benaderen van kinderen via tekstherkenning, binnen de reikwijdte van de afwijking die deze verordening biedt.

Wat betreft de verzamelde verkeersgegevens en de respectieve volumes van de verschillende typen verwerkte inhouds- en verkeersgegevens, verschilden de verslagen van de aanbieders aanzienlijk.

De verkeersgegevens die de aanbieders verzamelden en opnamen in CyberTipline-verslagen aan het National Center for Missing and Exploited Children (nationaal centrum voor vermiste en misbruikte kinderen, hierna "NCMEC" genoemd) in de Verenigde Staten, omvatten alle of een gedeelte van de volgende gegevens:

a) Gegevens met betrekking tot gebruikers/gemelde personen/accounts (Google, LinkedIn, Microsoft, X);
b) metadata met betrekking tot inhouds-/transactiegegevens (Google, LinkedIn, Microsoft);
c) gegevens met betrekking tot een mogelijk slachtoffer (Google);
d) gegevens over misbruikhandelingen (Google).

[1] Twitter diende zijn bijdrage in vóór de naamsverandering en wordt verder in dit verslag "X" genoemd.

Wat betreft de volumes van gegevens die uit hoofde van de tijdelijke verordening zijn verwerkt, meldde LinkedIn dat het tussen 14 juli en 31 december 2021 8 miljoen beelden en video's afkomstig uit de EU heeft verwerkt, en in 2022 21 miljoen beelden en 63 000 video's afkomstig uit de EU. Microsoft meldde dat het voor de toepassing van de verordening tussen juli en december 2021 wereldwijd 8,9 miljard beelden en video's heeft verwerkt en in 2022 12,3 miljard inhoudelijke elementen. Er waren geen cijfers voor de EU beschikbaar, zodat er voor dit verslag geen conclusies konden worden getrokken. De andere aanbieders verstrekten geen informatie over het volume van de verwerkte gegevens. Van de vijf aanbieders die gegevens indienden, was er dus maar één die gegevens op het vereiste detailniveau verstrekte.

Ter illustratie van de algemene context: het NCMEC meldde dat het in 2022 in totaal 87,2 miljoen beelden en video's wereldwijd en 5,1 miljoen beelden en video's betreffende de EU heeft ontvangen, en in 2021 84,8 miljoen beelden en video's wereldwijd en 1,8 miljoen beelden en video's betreffende de EU. Het gaat uitsluitend om materiaal dat door een aanbieder als mogelijk CSAM is aangemerkt; het kan dus geen indicatie vormen voor het totale volume aan gegevens die uit hoofde van de tijdelijke verordening zijn verwerkt.

2.1.2. Gronden voor verwerking overeenkomstig Verordening (EU) 2016/679

De aanbieders meldden de volgende gronden voor verwerking overeenkomstig Verordening (EU) 2016/679 (hierna "AVG" genoemd):

- artikel 6, lid 1, punt d), AVG, d.w.z. verwerking die noodzakelijk is om de vitale belangen te beschermen van kinderen en personen die slachtoffer zijn van online seksueel misbruik van kinderen (Google, Meta, X[2]);
- artikel 6, lid 1, punt e), AVG, namelijk verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang (LinkedIn, Microsoft, Meta, X[3]);
- artikel 6, lid 1, punt f), AVG, namelijk verwerking die noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van:
    i. de aanbieders om online seksueel misbruik van kinderen op hun diensten op te sporen, te voorkomen of op andere wijze aan te pakken en om andere gebruikers, klanten, partners en het publiek te beschermen tegen die vorm van illegale inhoud (Google, Meta);
    ii. slachtoffers van seksueel misbruik van kinderen en de organisatie waarbij de aanbieder online seksueel misbruik van kinderen meldt (bv. NCMEC) om online seksueel misbruik van kinderen op te sporen, te voorkomen en van zijn diensten te verwijderen (Google).

[2] Meta en X hebben het concrete artikel niet expliciet vermeld.
[3] Meta en X hebben het concrete artikel niet expliciet vermeld.

2.1.3. Grond voor doorgifte van persoonsgegevens aan landen buiten de Unie overeenkomstig hoofdstuk V van de AVG, indien van toepassing

Alle aanbieders meldden dat zij gebruikmaken van standaardcontractbepalingen die door de Commissie op grond van artikel 46, lid 2, punt c), AVG zijn vastgesteld. Wat betreft de doorgifte van persoonsgegevens aan het NCMEC meldde LinkedIn ook dat het, voor zover van toepassing, gebruikmaakte van de afwijking die is toegestaan volgens artikel 49, lid 1, AVG.

2.1.4. Aantal geconstateerde gevallen van online seksueel misbruik van kinderen, waarbij een onderscheid wordt gemaakt tussen online CSAM en het benaderen van kinderen

Tabel 1: Aantal in 2021 geconstateerde gevallen van online seksueel misbruik van kinderen

Aanbieder	Aantal in 2021 geconstateerde gevallen van CSAM	Opmerkingen
Google	33 Google Chat-accounts	Dit betreft het aantal Google Chat-accounts van EU-gebruikers waarin met geautomatiseerde technologie online seksueel misbruik van kinderen werd vastgesteld tussen 2 augustus 2021 en 31 december 2021. Er werden geen gegevens verstrekt over het aantal geconstateerde inhoudelijke elementen.
LinkedIn	31 inhoudelijke elementen	Via handmatige toetsing werden 31 inhoudelijke elementen bevestigd als CSAM en aan het NCMEC gemeld; 6 items waren bekend CSAM en 25 items onbekend CSAM.
Meta	340 000 accounts	Aantal accounts waarvan tussen 8 november 2021 en 31 december 2021 is vastgesteld dat ze ten minste één media-element met CSAM hebben verzonden in berichtenthreads waarbij een gebruiker uit de EU betrokken was.
Microsoft	6 600 inhoudelijke elementen	6 600 inhoudelijke elementen (afzonderlijke beelden of video's) bevestigd als zijnde CSAM uit de Europese Unie, van de meer dan 20 000 inhoudelijke elementen die tussen juli 2021 en december 2021 wereldwijd werden geconstateerd.
X (voorheen Twitter)	532 898 accounts	Accounts (onduidelijk of die zich uitsluitend in de EU dan wel in de hele wereld bevonden) die tussen 2 augustus 2021 en 31 december 2021 buiten werking zijn gesteld wegens schending van het beleid van X inzake seksueel misbruik van kinderen.

In het geval van X blijkt uit de verstrekte gegevens niet of die uitsluitend betrekking hebben op diensten die binnen de werkingssfeer van de tijdelijke verordening vallen (nummeronafhankelijke interpersoonlijke communicatiediensten) dan wel of dat aantal ook betrekking heeft op andere diensten (zoals diensten van de informatiemaatschappij). Dat geldt voor alle gegevens betreffende X in dit verslag.

Tabel 2: Aantal in 2022 geconstateerde gevallen van online seksueel misbruik van kinderen

Aanbieder	Aantal in 2022 geconstateerde gevallen van CSAM	Opmerkingen
Google	2 045 inhoudelijke elementen	Aantal inhoudelijke elementen die in 752 Google-accounts van EU-gebruikers zijn vastgesteld met geautomatiseerde technologie en zijn gemeld aan het NCMEC.
LinkedIn	2 inhoudelijke elementen	LinkedIn heeft 2 afbeeldingen en 0 video's bevestigd als zijnde CSAM.
Meta	6,6 miljoen	Media-elementen die CSAM vormen, die zijn opgespoord

	inhoudelijke elementen	door de mediaherkenningstechnologie van Meta en waartegen actie is ondernomen, in berichtenthreads waarbij een gebruiker uit de EU betrokken was.
Microsoft	12 800 inhoudelijke elementen	12 800 inhoudelijke elementen (afzonderlijke beelden of video's) bevestigd als zijnde CSAM uit de EU, van de meer dan 50 000 inhoudelijke elementen die wereldwijd werden geconstateerd in 2022.
X (voorheen Twitter)	2 348 712 accounts	Accounts (onduidelijk of die zich uitsluitend in de EU dan wel in de hele wereld bevonden) die buiten werking zijn gesteld wegens schending van het beleid van X inzake seksueel misbruik van kinderen.

2.1.5. Verhaal van gebruikers en uitkomsten

Overeenkomstig artikel 3, lid 1, punt g), iv), van de tijdelijke verordening moeten aanbieders passende procedures en verhaalmechanismen instellen om ervoor te zorgen dat gebruikers bij hen een klacht kunnen indienen. Artikel 5 bevat daarnaast regels over een voorziening in rechte.

De aanbieders meldden dat zij dergelijke interne verhaalprocedures en -mechanismen hebben ingesteld voor gebruikers van wie de account is beperkt wegens het delen van CSAM en/of van wie inhoud is verwijderd omdat die als CSAM is aangemerkt, zodat die gebruikers bezwaar kunnen maken tegen die beperking/verwijdering en kunnen laten toetsen of er fouten zijn gemaakt.

Zij meldden gevallen waarin een gebruiker een klacht heeft ingediend bij het interne verhaalmechanisme of een gerechtelijke autoriteit over zaken die binnen de werkingssfeer van de verordening vielen en zich in de EU hebben voorgedaan, en verschaften tevens informatie over de uitkomst van die klachten. Met uitzondering van Microsoft (dat over 2021 en 2022 geen klachten meldde in beide kanalen) hebben de aanbieders niet afzonderlijk gerapporteerd over intern verhaal en beroepen in rechte; de onderstaande tabellen hebben dus betrekking op zowel interne als rechterlijke procedures voor verhaal.

Tabel 3: Aantal gevallen in 2021 waarin een gebruiker een klacht heeft ingediend via het interne verhaalmechanisme of bij een gerechtelijke autoriteit, en de uitkomst van die klachten

Aanbieder	**Aantal klachten van gebruikers**	**Aantal heropende accounts**	**Aantal teruggeplaatste inhoudelijke elementen**	**Opmerkingen**
Google	8	0	Niet beschikbaar	Google Chat-accounts die wegens online seksueel misbruik van kinderen buiten werking waren gesteld en waarbij de gebruiker bezwaar maakte: 8. Geen van de accounts werd

				heropend.
LinkedIn	0	Niet beschikbaar	Niet beschikbaar	
Meta	4 900	Niet beschikbaar	207	4 900 gebruikers maakten bezwaar. Na de bezwaarprocedures werd van 207 gebruikers de inhoud teruggeplaatst en werden ingrepen op het account teruggedraaid.
Microsoft	0	Niet beschikbaar	Niet beschikbaar	
X (voorheen Twitter)	Ca. 90 000	Ca. 3 000	Niet beschikbaar	Ca. 90 000 bezwaarprocedures. X heeft ca. 3 000 accounts heropend.

Tabel 4: Aantal gevallen in 2022 waarin een gebruiker een klacht heeft ingediend via het interne verhaalmechanisme of bij een gerechtelijke autoriteit, en de uitkomst van die klachten.

Aanbieder	**Aantal klachten van gebruikers**	**Aantal heropende accounts**	**Aantal teruggeplaatste inhoudelijke elementen**	**Opmerkingen**
Google	378	0	Niet beschikbaar	Google-accounts die wegens online seksueel misbruik van kinderen buiten werking waren gesteld en waarbij de gebruiker bezwaar maakte: 378. Geen van de accounts is heropend.
LinkedIn	0	Niet beschikbaar	Niet beschikbaar	
Meta	29 000	Niet beschikbaar	3 700	Gebruikers maakten bezwaar tegen maatregelen ten opzichte van 29 000 van hun gedeelde media-elementen. Na de bezwaarprocedures werden ongeveer 3 700 inhoudelijke elementen teruggeplaatst en ingrepen op het account teruggedraaid.
Microsoft	0	Niet beschikbaar	Niet beschikbaar	
X (voorheen Twitter)	Ca. 430 000	Ca. 4 000	Niet beschikbaar	Ca. 430 000 bezwaarprocedures. X heeft ongeveer 4 000 accounts heropend.

2.1.6. Aantal fouten en de foutverhoudingen (fout-positieve resultaten) van de verschillende gebruikte technologieën

Overeenkomstig artikel 3, lid 1, punt e), van de tijdelijke verordening moeten de aanbieders ervoor zorgen dat de gebruikte technologieën voldoende betrouwbaar zijn, in die zin dat het foutenpercentage met betrekking tot het opsporen van inhoud die seksueel online misbruik van kinderen omvat, zo veel mogelijk wordt beperkt.

Op dat punt hebben de aanbieders gemeld dat zij de verschillende technologieën om online CSA op te sporen niet geïsoleerd gebruiken. Zij hanteren daarentegen een gelaagde benadering voor de opsporing van online CSA, waarbij zij verschillende opsporingstechnologieën inzetten om de nauwkeurigheid te verhogen. Alle aanbieders maken daarnaast gebruik van toetsing door mensen om fouten of fout-positieve resultaten te verminderen. In plaats van het aantal fouten en de foutverhoudingen (fout-positieve resultaten) voor elk van de gebruikte technologieën afzonderlijk, hebben de aanbieders geaggregeerde gegevens verstrekt voor alle gebruikte technologieën.

De meeste aanbieders meten het aantal fouten en de foutverhoudingen in de vorm van terugdraaiingen van handhavingsbeslissingen, dus de totale verhouding tussen enerzijds klachten en anderzijds maatregelen zoals het heropenen van accounts of terugplaatsen van inhoud. De benadering van de aanbieders weerspiegelt niet noodzakelijkerwijs de statistische definitie van fout-positieve resultaten.

De volgende verhoudingen tussen klachten en terugdraaiingen van maatregelen zijn gemeld:

Tabel 5: Verhoudingen tussen klachten en het terugdraaien van maatregelen

	2021*		2022		
Aanbieder	**% heropende accounts t.o.v. aantal klachten**	**% heropende t.o.v. opgeschorte accounts**	**% heropende accounts t.o.v. aantal klachten**	**% heropende t.o.v. opgeschorte accounts**	**Opmerkingen**
Google	0 % (0 t.o.v. 8)	0 % (0 t.o.v. 33)	0 % (0 t.o.v. 378)	0 % (zie opmerkingen)	Voor 2022 is het aantal opgeschorte accounts niet verstrekt. In plaats daarvan is het aantal inhoudelijke elementen verstrekt dat is opgespoord en aan het NCMEC is gemeld, namelijk 2045. Er zijn geen accounts heropend naar aanleiding van klachten.
LinkedIn	0 %	0 %	0 %	0 %	Geen klachten. Over de periode tussen 13 juli 2021 en 31 december 2021 meldde LinkedIn ook dat van de 75 bestanden die als mogelijk CSAM uit de EU waren gecontroleerd, bij toetsing door mensen 31 bestanden werden bevestigd als CSAM. LinkedIn heeft deze gegevens niet verstrekt over 2022.
Meta	4,22 % (207 t.o.v. 4 900)	0,06 % (207 t.o.v. 340 000)	Zie opmerkingen	Zie opmerkingen	Er is geen informatie verstrekt waaruit de reikwijdte en de inhoud van de klachten en de redenen voor heropening nauwkeurig konden worden opgemaakt. Voor 2022 hadden de verstrekte gegevens betrekking op inhoudelijke elementen, niet op accounts: - Aantal geschorste inhoudelijke elementen (“waarop is ingegrepen”): 6,6 miljoen - Aantal geschorste inhoudelijke elementen waarover een klacht is ingediend: 29 000 - Aantal geschorste inhoudelijke elementen dat is teruggeplaatst: 3 700

					Dit geeft: - % teruggeplaatste inhoudelijke elementen t.o.v. het aantal klachten: 12,8 % (3 700 t.o.v. 29 000); - % teruggeplaatste inhoudelijke elementen t.o.v. het aantal opgeschorte inhoudelijke elementen: 0,06 % (3 700 t.o.v. 6,6 miljoen)
Microsoft	0 %	—	—	—	Onvoldoende gegevens om de verhouding tussen klachten en teruggedraaide maatregelen te kunnen berekenen. Over 2022 zijn in totaal 17 terugdraaiingen van aanvankelijke beslissingen door de inhoudsmoderatie gemeld, maar zonder cijfers over het totaal aantal klachten.
X (voorheen Twitter)	1,43 % (100 t.o.v. 7 000)	0,06 % (100 t.o.v. 166 000)	2,17 % (500 t.o.v. 23 000)	0,10 % (500 t.o.v. 501 000)	Over de tweede helft van 2021 hebben geautomatiseerde mechanismen ongeveer 166 000 gebruikers geschorst wegens CSA. Van die gebruikers hebben er ongeveer 7 000 een klacht ingediend, waarna de beslissing in ongeveer 100 gevallen is teruggedraaid. Over 2022 hebben geautomatiseerde mechanismen 501 000 gebruikers geschorst wegens CSA. Van die gebruikers hebben er ongeveer 23 000 een klacht ingediend, waarna de beslissing in ongeveer 500 gevallen is teruggedraaid.

* De verslagperioden in 2021 verschillen per aanbieder.

2.1.7. Maatregelen die zijn toegepast om het foutenpercentage te beperken, en het bereikte foutenpercentage

Overeenkomstig artikel 3, lid 1, punt e), van de tijdelijke verordening moeten de gebruikte technologieën voldoende betrouwbaar zijn en moeten de gevolgen van incidentele fouten onverwijld worden gecorrigeerd. Daarnaast worden in artikel 3, lid 1, punt g), ii), menselijk toezicht en waar nodig menselijke tussenkomst verplicht gesteld.

Alle aanbieders meldden dat zij de verspreiding van online CSA met een gelaagde aanpak opsporen en bestrijden. Die aanpak omvat het gebruik van hashmatchingtechnologieën (waaronder PhotoDNA) om CSAM op te sporen, in combinatie met toetsing door mensen om te bevestigen of een mediabestand (beeld en video) CSAM bevat, en toezicht door mensen op de CSAM-verwerking.

Volgens de aanbieders hebben zij verschillende maatregelen en waarborgen toegepast om het foutenpercentage bij het opsporen, melden en verwijderen van online CSA te beperken en terug te dringen. Het gaat onder andere om[4]:

i. bewaking en kwaliteitsbeoordeling van de prestaties van CSA-opsporingsinstrumenten, om zowel de nauwkeurigheid (zodat ze uitsluitend online seksueel misbruik van kinderen opsporen) als de trefkans (zodat ze geen online seksueel misbruik van kinderen op hun platforms over het hoofd zien) precies af te stemmen (Google, X);
ii. toetsing en toezicht door mensen: steekproeven van media die met hashmatchingtechnologie als CSAM zijn aangemerkt, worden gecontroleerd door menselijke toetsers/getrainde analisten (Google, LinkedIn, Meta, Microsoft);
iii. signaleren en toetsen van clusters met een hoog volume (Meta);
iv. inzetten van verdere handmatige toetsingsprocessen als doorlopende hashkwaliteitscontroles (LinkedIn, Microsoft);
v. menselijke toetsers krijgen onder deskundige begeleiding een intensieve, specialistische training over het herkennen van CSAM-materiaal, om de nauwkeurigheid van de toetsing door mensen te waarborgen (Google);
vi. periodieke beoordeling van de controle die wordt uitgevoerd ten aanzien van de kwaliteit van de menselijke toetsers en de conclusies die zij trekken (Google, X);
vii. andere kwaliteitscontroleprocessen om fouten te verminderen en onmiddellijk te corrigeren, zoals onafhankelijke hashverificatie (Google, LinkedIn), of menselijke toetsing van elk nog niet eerder aangetroffen geval van CSAM voordat het wordt gemeld (Google);
viii. ontwikkeling en regelmatige evaluatie van beleid en handhavingsstrategieën door getrainde deskundigen op het gebied van online CSA (Google);

[4] De aanbieders tussen haakjes hebben de betreffende maatregelen specifiek gemeld. Indien een aanbieder niet vermeld staat bij een maatregel betekent dat niet dat de aanbieder die achterwege laat, maar alleen dat hij die niet in zijn verslag heeft vermeld.

ix. samenwerking met de CyberTipline van het NCMEC voor het rapporteren over de kwaliteit en eventuele fout-positieve meldingen (Google, LinkedIn, Meta, Microsoft, X).

2.1.8. Bewaringsbeleid en toegepaste waarborgen inzake gegevensbescherming overeenkomstig de AVG

Volgens artikel 3, lid 1, punt h), van de tijdelijke verordening moeten persoonsgegevens op een veilige manier en enkel en alleen voor bepaalde precies omschreven doeleinden worden opgeslagen; punt i) bevat aanwijzingen voor de bewaartermijn. Verder moet aan de toepasselijke eisen van de AVG worden voldaan.

De aanbieders meldden dat ze robuuste beleidsmaatregelen hebben getroffen voor de bewaring en de bescherming van persoonsgegevens. Het bewaringsbeleid hangt af van het type gegevens. Volgens de aanbieders wordt de bewaartermijn in elk geval beperkt in de tijd, zoals passend wordt geacht voor het type gegevens en het doel van de gegevensverwerking, en worden de gegevens aan het einde van de bewaartermijn gewist. De aanbieders hebben meer gedetailleerde informatie over hun werkwijze bij het bewaren van gegevens opgenomen in hun beleid of verklaringen inzake privacy en hun dienstverlenings- of gebruikersovereenkomsten.

De meeste aanbieders (LinkedIn, Meta, Microsoft) hanteren een bewaartermijn van 90 dagen voor media waarvan is bevestigd dat ze CSAM bevatten binnen de werkingssfeer van de verordening. Binnen die termijn wordt de als CSAM bevestigde inhoud opgeslagen in een aparte, beveiligde CSAM-opslag die wordt beheerd door gespecialiseerde teams (zoals het team voor wetshandhaving en nationale veiligheid van Microsoft). Het opgeslagen CSAM wordt na 90 dagen automatisch door die opslagsystemen gewist, tenzij de bewaartermijn wordt verlengd na ontvangst van een rechtmatig verzoek tot verwerking, dat gewoonlijk verband houdt met het optreden van rechtshandhavingsinstanties naar aanleiding van meldingen door het NCMEC.

Google meldde dat binnen de werkingssfeer van de verordening aangetroffen CSAM niet langer wordt bewaard dan strikt noodzakelijk is voor de relevante doeleinden op grond van de verordening en hoe dan ook niet langer dan 12 maanden vanaf het moment waarop het CSAM is aangetroffen en gemeld; die termijn kan worden verlengd op basis van een geldig wettelijk verzoek tot bewaring.

X (voorheen Twitter) meldde dat het profielgegevens en inhoud bewaart zolang het gebruikersaccount bestaat, en dat het persoonsgegevens van gebruikers van X gedurende maximaal 18 maanden bewaart. Als een account door de gebruiker wordt gedeactiveerd, bewaart X de gegevens gewoonlijk nog 30 dagen, waarna de account wordt verwijderd. Gebruikersgegevens in verband met klachten en inbreuken op het beleid, inclusief de accountgegevens van overtreders (zoals de identificatiegegevens die zijn gebruikt om het account aan te maken: e-mailadres of telefoonnummer), worden onbeperkt bewaard om te voorkomen dat overtreders van het beleid een nieuw account maken en te zorgen dat overtreders van het beleid van X niet simpelweg wachten tot het einde van de verwijderingsperiode en dan het beleid opnieuw overtreden[5].

[5] Privacybeleid van X, punt 4. Hoelang we informatie bewaren. Zie: https://twitter.com/nl/privacy.

Door de aanbieders toegepaste waarborgen ter bescherming van persoonsgegevens omvatten alle of een selectie van de standaardmaatregelen voor de sector, zoals (niet-uitputtende lijst)[6]:

i. gebruik van anonimiserings- of pseudonimiseringstechnieken en anonimisering van gegevens (bijvoorbeeld door maskering, hashing of differentiële privacy) (Google, LinkedIn, Meta, Microsoft);
ii. verstrekking van uitsluitend hashwaarden aan derden ten behoeve van CSAM-opsporing (Google, LinkedIn);
iii. gebruik van standaard in de sector toegepaste encryptie (algoritmen en protocollen) voor gegevens die van particuliere infrastructuur naar openbare netwerken worden verzonden (Meta);
iv. invoering van gegevensbeheerstrategieën/uitgebreide privacyprogramma's (X, voorheen Twitter, Google) en strenge interne beperkingen voor de toegang tot gegevens (Meta) (bv. voor werknemers, aannemers en agenten die de gegevens nodig hebben voor verwerking), gebruik van Access Control Lists (toegangscontrolelijsten) voor alle toetsingsinstrumenten voor CSAM en hashuitsluitingen (Meta) en strikte, contractuele vertrouwelijkheidsverplichtingen voor degenen die toegang hebben;
v. beoordeling van strategieën voor anonimisering en gegevensbeheer, in de vorm van privacybeoordelingen voor het herkennen van, toegang krijgen tot en tegengaan van mogelijke privacyrisico's door het verzamelen, verwerken, opslaan en verspreiden van persoonsgegevens, en beoordeling van beschermingspraktijken (Microsoft);
vi. beschikken over responsplannen in het geval van veiligheidsincidenten voor het bewaken, opsporen en oplossen van alle mogelijke kwetsbaarheden en incidenten op het vlak van veiligheid in de gehele infrastructuur (Google, Meta).

2.1.9. Namen van de in het algemeen belang tegen seksueel misbruik van kinderen optredende organisaties waarmee uit hoofde van deze verordening gegevens zijn gedeeld

In beide verslagperioden (juli/augustus 2021 tot december 2021 en januari 2022 tot december 2022) hebben alle aanbieders gemeld dat zij de gegevens die uit hoofde van deze verordening zijn verwerkt, hebben gedeeld met het NCMEC. Alle aanbieders die verslag hebben uitgebracht, hebben de Commissie overeenkomstig artikel 7, lid 1, van de tijdelijke verordening tevens meegedeeld dat zij online seksueel misbruik van kinderen uit hoofde van deze verordening hebben gemeld aan het NCMEC[7].

[6] De aanbieders tussen haakjes hebben de betreffende maatregelen specifiek gemeld. Als een aanbieder niet vermeld staat bij een maatregel, betekent dat niet dat de aanbieder die achterwege laat, maar alleen dat hij die niet in zijn verslag heeft vermeld.

[7] De informatie over de in het algemeen belang optredende organisaties waaraan de aanbieders online seksueel misbruik van kinderen melden op grond van deze verordening, is overeenkomstig de verplichtingen van de Commissie uit hoofde van artikel 8, lid 2, van de tijdelijke verordening gepubliceerd op https://home-affairs.ec.europa.eu/policies/internal-security/child-sexual-abuse/legal-framework-protect-children_en

2.2. Statistieken van de lidstaten (artikel 8)

De lidstaten zijn op grond van artikel 8, lid 1, van de tijdelijke verordening verplicht om statistieken te verstrekken over:

(a) het totaal aantal meldingen van opgespoord online seksueel misbruik van kinderen die door aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen zijn gedaan bij de bevoegde nationale rechtshandhavingsinstanties, waarbij (als dergelijke informatie beschikbaar is) een onderscheid wordt gemaakt tussen het absolute aantal gevallen en de gevallen die meermalen zijn gemeld, en het type aanbieder op wiens dienst het online seksueel misbruik van kinderen is ontdekt;
(b) het aantal kinderen dat is geïdentificeerd via maatregelen uit hoofde van artikel 3, uitgesplitst naar geslacht;
(c) het aantal veroordeelde daders.

De meeste lidstaten hebben de gegevens ten minste gedeeltelijk verstrekt, maar in veel lidstaten waren geen systemen opgezet voor de verzameling en rapportage van de relevante gegevens. Daardoor hebben de aangeleverde statistieken betrekking op zeer uiteenlopende verslagperioden en verschillen ze aanzienlijk op het punt van detailniveau. Sommige lidstaten hebben jaarstatistieken ingediend vanaf de datum van inwerkingtreding van de verordening. De meeste rapporteerden per kalenderjaar, omdat zij misschien niet over de technische mogelijkheden beschikken om een onderscheid te maken tussen de gevraagde jaarlijkse statistieken vanaf de datum van inwerkingtreding van de verordening. Enkele lidstaten hebben helemaal geen gegevens verstrekt.

Verder moet worden vermeld dat de statistische gegevens in sommige gevallen zijn verkregen uit zogenoemde levende databanken of journaliserings- en zaakbeheersystemen, dus geen echte statistische systemen. Soms zijn de cijfers gebaseerd op dynamische gegevens, wat betekent dat de gegevens niet definitief zijn en dus nog kunnen worden gewijzigd. Gegevens veranderen bijvoorbeeld naargelang de tijd van extractie (zoals in Slovenië en Denemarken), omdat er meer onderzoeken en rechtszaken worden afgerond.

In verschillende lidstaten richten de bevoegde autoriteiten nieuwe afdelingen op voor onderzoeken naar misdrijven in verband met online seksueel misbruik van kinderen, en voeren ze centrale rapportage in voor online seksueel misbruik van kinderen (Letland, Tsjechië). In de toekomst zouden de statistieken daardoor nauwkeuriger moeten worden.

Duitsland verklaarde dat het geen statistieken kon verstrekken op grond van artikel 8, lid 1, van de tijdelijke verordening, omdat het naar eigen zeggen geen rechtsgrondslag had voor vrijwillige opsporing[8]. De Duitse federale recherche (Bundeskriminalamt) vermeldt op haar website echter

[8] Het door Duitsland conform artikel 8 van Verordening (EU) 2021/1232 ingediende verslag is ontvangen op 18 oktober 2022. Het NCMEC publiceert alle gegevens over ontvangen meldingen in verband met de EU-lidstaten, waaronder Duitsland, in hun CyberTipline-verslagen per land. Zie: NCMEC, 2021 CyberTipline Reports by

dat zij in 2022 89 844 meldingen van het NCMEC heeft ontvangen, en het NCMEC zegt dat het 138 193 meldingen heeft doorgestuurd naar de Duitse autoriteiten[9]. Drie lidstaten hebben geen gegevens aangeleverd, noch een reden aangevoerd waarom zij op grond van deze bepaling niet hebben gerapporteerd (Malta, Portugal en Roemenië).

2.2.1. Totaal aantal meldingen van opgespoord online seksueel misbruik van kinderen

De meeste lidstaten verstrekten op grond van artikel 8, lid 1, punt a), van de tijdelijke verordening enkele statistieken over het totale aantal meldingen van online seksueel misbruik van kinderen. De lidstaten verstrekten gegevens over verschillende verslagperioden, zodat het totaal aantal meldingen van opgespoord online seksueel misbruik van kinderen in de EU niet kon worden berekend per periode, zoals het tijdvak waarin de verordening werd uitgevoerd.

Meestal verstrekten de lidstaten het totale aantal meldingen dat ze hadden ontvangen van aanbieders of van andere organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen, aan de nationale rechtshandhavingsinstanties. Aangezien de meeste in de VS gevestigde aanbieders aan het NCMEC rapporteren, gaven de meeste lidstaten aan dat zij de meeste of al hun meldingen van het NCMEC ontvangen. De lidstaten vermeldden niet het aantal meldingen waarnaar een onderzoek kan worden ingesteld, maar sommige lidstaten vermeldden het aantal geopende onderzoeken, dat significant lager is. Het verschil tussen ontvangen meldingen en geopende onderzoeken werd toegeschreven aan verschillende redenen, bv. dat de melding wel CSAM betrof maar onvoldoende informatie bevatte om een onderzoek te openen; dat meerdere meldingen over één verdachte werden samengevoegd; of dat het materiaal wel situaties van uitbuiting toonde, maar volgens het nationaal recht niet als strafbaar werd aangemerkt. Daarnaast maakten de lidstaten meestal geen onderscheid tussen het absolute aantal gevallen en gevallen die meerdere malen werden gemeld. In de van het NCMEC ontvangen meldingen, waren de van aanbieders ontvangen meldingen door het NCMEC al uitgesplitst naar “te onderzoeken” en “ter informatie”. Het NCMEC definieert een te onderzoeken melding als een melding die voldoende informatie bevat om een onderzoek te starten. Die informatie omvat gewoonlijk gebruikersgegevens, beeldmateriaal en een mogelijke locatie. De melding wordt onder “ter informatie” ingedeeld als ze niet genoeg informatie bevat of als de beelden als viraal worden beschouwd en veelvuldig zijn gemeld. In 2022 heeft het NCMEC 49 % van de meldingen aangemerkt als “te onderzoeken” en 51 % als “ter informatie”.

Slechts zeer weinig lidstaten gaven aan bij welk type aanbieder het online seksueel misbruik van kinderen was aangetroffen (bv. België, Tsjechië, Estland, Frankrijk en Polen) en slechts één lidstaat verstrekte een gedetailleerde uitsplitsing (België).

Country, geraadpleegd in juli 2023; NCMEC, 2022 CyberTipline Reports by Country, geraadpleegd in juli 2023.

9 https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/230623_Mindestspeicherfristen_IP-Adressen.html

Slovenië gaf aan dat het geen cijfers kon geven over uitsluitend feiten waarnaar een onderzoek was ingesteld naar aanleiding van meldingen van aanbieders en organisaties, maar dat het slechts cijfers kon verstrekken over alle onderzoeken naar online seksueel misbruik van kinderen, ongeacht de informatiebron die tot de start van het onderzoek had geleid.

Tabel 6: Totaal aantal meldingen door de lidstaten van opgespoord online seksueel misbruik van kinderen

Land	Rapportageperiode	Totaal aantal meldingen van online seksueel misbruik van kinderen	Bron van de meldingen	Opmerkingen
Oostenrijk	2021 en 2022	16 311	NCMEC	
België	1 augustus 2021 tot en met 31 juli 2022	26226	Meldingen door aanbieders (sociale media) en de hotline van Childfocus	
Bulgarije	2021 en 2022	9 120	Aanbieders en de hotline van INHOPE via "Safenet" en andere	Daarvan betroffen 9 112 meldingen webpagina's met CSAM die door Bulgaarse aanbieders werden gehost.
Kroatië	1 januari 2021 tot en met 31 oktober 2022	9 044	NCMEC	
Cyprus	1 juli 2021 tot en met 31 december 2022	3 570	NCMEC	
Tsjechië	1 januari 2022 tot en met 31 juli 2022	13 279	NCMEC	
Denemarken	2 augustus 2021 tot en met 20 januari 2023	10 744	NCMEC	
Estland	—	—	NCMEC, Child Helpline 116 111	Estland meldde dat de statistieken van de politie en douane, waaronder NCMEC-statistieken, niet openbaar zijn. Over 2021 meldde het 360 strafbare seksuele feiten zonder contact tegen kinderen. Verder was 86 % van alle strafbare seksuele feiten zonder contact gepleegd via het

				internet of met IT-instrumenten.
Finland	2022	25 000	NCMEC en Save the Children	
Frankrijk	1 augustus 2021 tot en met 1 augustus 2022	120 000	NCMEC	
Duitsland	—	—	—	Gegevens niet beschikbaar/niet gemeld.
Griekenland	2021 en 2022	142	NCMEC, Griekse hotline voor illegale inhoud op internet — Safeline, nationale commissie voor telecommunicatie en posterijen, nationale SOS-lijn 1056 — Glimlach van een kind, Griekse ombudsman	
Hongarije	2022	0	De aanbieders hebben geen meldingen verzonden uit hoofde van de tijdelijke verordening.	
Ierland	2021 en 2022	15 355	NCMEC	
Italië	2022	4 607	Niet gespecificeerd	
Letland	1 augustus 2022 tot en met 6 maart 2023	Maandelijks ongeveer 115 tot 220 meldingen	Van aanbieders en in het algemeen belang tegen seksueel misbruik van kinderen optredende organisaties buiten Letland (voornamelijk het NCMEC) en Letse aanbieders en organisaties (voornamelijk het Letse centrum voor een veiliger internet)	
Litouwen	1 januari 2021 tot en met 30 juni 2022	4 142	Niet gespecificeerd	
Luxemburg	2021 en 2022	2 491	Niet gespecificeerd	

Malta	—	—	—	Gegevens niet ingediend/niet gemeld.
Nederland	2021	36 537	Aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen	
Polen	3 augustus 2021 tot en met 3 augustus 2023	227	Aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen	Voor de periode van 3 augustus 2022 tot en met 3 augustus 2023 meldde Polen 1 geval van het benaderen van kinderen voor seksuele doeleinden en 105 gevallen van CSAM.
Portugal	—	—	—	Gegevens niet ingediend/niet gemeld.
Roemenië	—	—	—	Gegevens niet ingediend/niet gemeld.
Slowakije	1 augustus 2021 tot en met 31 juli 2022	7 206	Aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen	
Slovenië	1 januari 2021 tot en met 14 juli 2023	452	Dit cijfer slaat op strafbare feiten in verband met internetactiviteiten. Op dit moment kan Slovenië op basis van de bestaande statistische gegevens geen onderscheid maken tussen statistische gegevens over strafbare feiten die worden onderzocht naar aanleiding van meldingen door aanbieders en organisaties, en statistische gegevens over andere meldingen.	
Spanje	2022	31 474	Organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen	

Zweden	Augustus 2021 tot en met 31 december 2022	32 830	Voornamelijk NCMEC	

Aangezien het NCMEC de belangrijkste bron van de meldingen is, is het leerzaam de cijfers over door de lidstaten ontvangen meldingen te vergelijken met de cijfers die het NCMEC heeft verstrekt over naar de lidstaten verzonden meldingen. Het NCMEC ontving in 2021 wereldwijd in totaal 29 397 681 meldingen uit de sector, waarvan 99,7 % (29 309 106) een of meer beelden of video's van seksueel misbruik van kinderen bevatten, 0,15 % (44 155) verband hielden met grooming en 0,05 % (16 032) verband hielden met kinderhandel voor seksuele doeleinden. In 2022 ontving het NCMEC in totaal 32 059 029 meldingen, waarvan 99,5 % (31 901 234) beelden of video's van seksueel misbruik van kinderen betroffen, 0,25 % (80 524) verband hielden met grooming en 0,06 % (18 336) verband hielden met kinderhandel voor seksuele doeleinden. Voor de EU kunnen die cijfers als volgt worden uitgesplitst:

Tabel 7: In 2021 en 2022 aan EU-lidstaten verstrekte NCMEC-meldingen inzake verdenking van online seksueel misbruik van kinderen

Land	**Totaal aantal meldingen in 2021[10]**	**% van het EU-totaal in 2021**	**Totaal aantal meldingen in 2022[11]**	**% van het EU-totaal in 2022**	**% van de EU-bevolking**
Oostenrijk	7580	1,36 %	18501	1,23 %	2,00 %
België	15762	2,84 %	50255	3,34 %	2,60 %
Bulgarije	13584	2,44 %	31937	2,12 %	1,53 %
Kroatië	4744	0,85 %	11693	0,78 %	0,86 %
Cyprus	2657	0,48 %	7361	0,49 %	0,20 %
Tsjechië	15004	2,70 %	61994	4,12 %	2,36 %
Denemarken	5891	1,06 %	30215	2,01 %	1,31 %
Estland	2729	0,49 %	6408	0,43 %	0,30 %
Finland	6079	1,09 %	10904	0,73 %	1,24 %
Frankrijk	98233	17,67 %	227465	15,13 %	15,16 %
Duitsland	79701	14,34 %	138193	9,19 %	18,59 %
Griekenland	14616	2,63 %	43345	2,88 %	2,37 %
Hongarije	31710	5,70 %	109434	7,28 %	2,16 %
Ierland	7327	1,32 %	19770	1,31 %	1,13 %
Italië	37480	6,74 %	96512	6,42 %	13,32 %
Letland	1537	0,28 %	3688	0,25 %	0,42 %
Litouwen	3509	0,63 %	16603	1,10 %	0,63 %
Luxemburg	2005	0,36 %	2004	0,13 %	0,14 %
Malta	750	0,13 %	4713	0,31 %	0,12 %
Nederland	36790	6,62 %	57012	3,79 %	3,96 %
Polen	37758	6,79 %	235310	15,65 %	8,41 %
Portugal	34415	6,19 %	42674	2,84 %	2,31 %

[10] NCMEC, 2021 CyberTipline Reports by Country, geraadpleegd in november 2023.
[11] NCMEC, 2022 CyberTipline Reports by Country, geraadpleegd in november 2023.

Roemenië	32765	5,89 %	96287	6,40 %	4,25 %
Slowakije	7275	1,31 %	39748	2,64 %	1,21 %
Slovenië	3162	0,57 %	14795	0,98 %	0,47 %
Spanje	33136	5,96 %	77727	5,17 %	10,60 %
Zweden	19635	3,53 %	48883	3,25 %	2,33 %
Totaal	555834		1503431		

De significante verschillen tussen het aantal meldingen in 2021 en 2022, met een grote stijging in 2022, zijn grotendeels veroorzaakt door de daling van vrijwillige opsporing tussen januari en augustus 2021, toen de tijdelijke verordening nog niet van toepassing was.

Het NCMEC heeft in zijn statistieken geen uitsplitsing per EU-lidstaat gemaakt op basis van de bron van de melding, met name of die afkomstig was van een nummeronafhankelijke interpersoonlijke communicatiedienst. Het NCMEC geeft echter wel statistieken over het totale aantal meldingen met betrekking tot de EU die afkomstig zijn van nummeronafhankelijke interpersoonlijke communicatiediensten. In 2021 waren 283 265 meldingen betreffende lidstaten afkomstig van een chat-, berichten- of e-maildienst, dat is 51 % van het totaal aantal meldingen betreffende de EU. Verder waren 164 645 meldingen (30 % van het totaal) afkomstig van platforms voor sociale media of online gaming, die mogelijk ook berichten- of chatdiensten omvatten. In 2021 hadden 3 565 meldingen betreffende de EU betrekking op grooming. In 2022 waren 1 015 231 meldingen betreffende lidstaten afkomstig van een chat-, berichten- of e-maildienst, dat is 68 % van het totaal aantal meldingen betreffende de EU. Verder waren 325 847 meldingen (22 % van het totaal) afkomstig van platforms voor sociale media of online gaming, die mogelijk ook berichten- of chatdiensten omvatten. In 2022 hadden 7 561 meldingen betreffende de EU betrekking op grooming. De verschillen tussen het aantal meldingen van nummeronafhankelijke interpersoonlijke communicatiediensten in 2021 en 2022 worden nogmaals veroorzaakt door de daling van vrijwillige opsporing tussen januari en augustus 2021, toen de tijdelijke verordening nog niet van toepassing was.

Het aandeel meldingen per lidstaat komt in veel gevallen grofweg overeen met het aandeel van de bevolking van de lidstaten ten opzichte van de gehele EU-bevolking, wat kan wijzen op een vergelijkbare incidentie van online seksueel misbruik van kinderen in alle lidstaten. Wat Spanje en Italië betreft, zijn er opmerkelijke afwijkingen zichtbaar: daar zijn de percentages in beide jaren laag in vergelijking met de gehele EU-bevolking, terwijl het aandeel meldingen van andere lidstaten aanzienlijk fluctueert (bv. voor Duitsland, Polen, Nederland en Slowakije). Die veranderingen worden niet als zodanig weergegeven in verslagen over aantallen gevallen, zodat het ook hier moeilijk is om conclusies te trekken over de correlatie tussen meldingen en onderzoeken.

Gezien de uiteenlopende verslagperioden kan er geen rechtstreeks verband worden gelegd. Er zijn echter significante verschillen tussen de statistieken van het NCMEC en de cijfers die door de lidstaten zijn gemeld. Evenmin kunnen de cijfers van het NCMEC betreffende de lidstaten volledig worden vergeleken met de cijfers afkomstig van de sector in het vorige punt. Hoewel sommige verschillen mogelijk worden veroorzaakt door meldingen van online seksueel misbruik

van kinderen uit andere bronnen dan interpersoonlijke communicatie, is daarvoor een verdere analyse nodig omdat het, gezien de lijst van aanbieders die aan het NCMEC rapporteren[12], mogelijk is dat ook andere aanbieders dan degenen die tot nu toe aan de Commissie verslag hebben uitgebracht, vrijwillige opsporingsmaatregelen treffen met betrekking tot de EU. Niettemin wijst het feit dat er betreffende de meeste lidstaten een significant verschil lijkt te bestaan tussen het aantal meldingen dat volgens het NCMEC naar de lidstaten is gezonden en het aantal meldingen dat volgens de lidstaten is ontvangen, erop dat de verzameling van en rapportering over gegevens door de lidstaten onvolledig is.

Voor elk van de hierboven aangegeven NCMEC-meldingen zijn de bijbehorende beelden en video's van seksueel misbruik van kinderen verwijderd en uit de circulatie genomen. Dat is met name van belang voor hen die slachtoffers van seksueel misbruik van kinderen zijn of zijn geweest. Uit onderzoek blijkt dat bij voortgezette circulatie van beelden en video's van het misbruik, het vermogen van slachtoffers wordt beperkt om de psychologische gevolgen van dat misbruik te boven te komen en er een secondaire vorm van victimisatie ontstaat.

2.2.2. Aantal geïdentificeerde kinderen

De meeste lidstaten verstrekten op grond van artikel 8, lid 1, punt b), van de tijdelijke verordening volledige of gedeeltelijke statistieken over het aantal geïdentificeerde kinderen, uitgesplitst per geslacht. Verschillende lidstaten hebben echter geen gegevens verstrekt, noch een reden aangevoerd waarom ze niet hebben gerapporteerd op grond van die bepaling.

Een aantal lidstaten heeft geen of slechts gedeeltelijke statistieken over de rapportageperiode verstrekt, maar heeft daar redenen voor opgegeven. Die redenen zijn onder meer:

- kinderslachtoffers van online CSA kunnen niet worden geteld (Frankrijk);
- er zijn geen gegevens beschikbaar omdat die niet worden verzameld als onderdeel van de nationale verzameling van statistische gegevens, of de nationale autoriteiten hebben die statistieken niet geregistreerd (Denemarken, Litouwen);
- in de nationale verzameling van statistische gegevens zijn die gegevens niet uitgesplitst naar geslacht (België, Cyprus, Tsjechië, Griekenland, Ierland, Italië, Litouwen, Nederland);
- in de bestaande informatiesystemen is geen informatie met het gevraagde detailniveau beschikbaar (Finland);
- de informatie wordt niet verzameld (Duitsland).

Sommige van de lidstaten die hebben aangegeven dat zij geen statistieken konden aanleveren, bevestigden dat hun nationale autoriteiten was verzocht om hun registratieprocedure voor vrijwillige meldingen en onderzoeken en het verzamelen van statistieken te wijzigen (Denemarken), en/of voeren nieuwe informatiesystemen in waarmee voldoende gedetailleerd kan worden gerapporteerd (Finland).

[12] De gegevens van het NCMEC zijn hier te raadplegen.

In één lidstaat (Hongarije) werd in de onderstaande gegevens geen onderscheid gemaakt tussen kinderslachtoffers van online en offline CSA. In sommige gevallen omvatten de statistieken ook kinderen die dit materiaal zelf hadden gemaakt en geüpload (zelfgemaakt materiaal, voornamelijk video) (Tsjechië, Estland).

Aangezien de lidstaten meestal over uiteenlopende perioden rapporteerden, kon geen berekening worden gemaakt van het totaal aantal kinderen dat per jaar en/of per rapportageperiode werd geïdentificeerd als slachtoffers van online seksueel misbruik van kinderen.

Tabel 8: Aantal geïdentificeerde kinderen, uitgesplitst naar geslacht

Land	Verslagperiode	Meisjes	Jongens	Totaal	Opmerkingen
Oostenrijk	2021 en 2022	11	6	17	
België	2021 en 2022	—	—	63	Naar geslacht uitgesplitste gegevens niet beschikbaar.
Bulgarije	2022	50	12	62	
Kroatië	1 januari 2021 tot en met 31 oktober 2022	20	0	20	
Cyprus	2022	—	—	102	Naar geslacht uitgesplitste gegevens niet beschikbaar.
Tsjechië	2022	—	—	30	Naar geslacht uitgesplitste gegevens niet beschikbaar.
Denemarken	—	—	—	—	Gegevens niet beschikbaar.
Estland	2021	6	12	18	
Finland	—	—	—	—	Gegevens niet beschikbaar.
Frankrijk	—	—	—	—	Gegevens niet beschikbaar.
Duitsland	—	—	—	—	Gegevens niet beschikbaar.
Griekenland	2021 en 2022	—	—	4	Naar geslacht uitgesplitste gegevens niet beschikbaar.
Hongarije	2021 en 2022	379	47	426	Onderscheid tussen slachtoffers van online en offline CSA niet mogelijk. Uitsluitend betreffende kinderen onder 16 jaar.
Ierland	2021 en 2022	—	—	101	Gegevens over 2021 (50 slachtoffers) konden niet worden uitgesplitst naar geslacht. Over 2022 zijn de naar geslacht uitgesplitste gegevens: 25 meisjes en 26 jongens geïdentificeerd.
Italië	2022	—	—	385	Naar geslacht uitgesplitste gegevens niet beschikbaar.

Letland	1 augustus 2022 tot en met 6 maart 2023	1	—	1	
Litouwen	—	—	—	—	Gegevens niet beschikbaar.
Luxemburg	2021 en 2022	0	0	0	
Malta	—	—	—	—	Gegevens niet ingediend/niet gemeld.
Nederland	2021	—	—	222	Naar geslacht uitgesplitste gegevens niet beschikbaar.
Polen	2022	2 368	487	3 014	In 2022 heeft het Poolse nationale politie-informatiesysteem de gegevens verstrekt van 3 014 slachtoffers van aan CSA gerelateerde strafbare feiten (2 368 meisjes, 487 jongens en 159 zonder vermeld geslacht).
Portugal	—	—	—	—	Gegevens niet ingediend/niet gemeld.
Roemenië	—	—	—	—	Gegevens niet ingediend/niet gemeld.
Slowakije	Augustus 2021 tot en met juli 2022	13	8	21	
Slovenië	1 januari 2021 tot en met 14 juli 2023	220	85	305	
Spanje	2022	80	39	119	
Zweden	2022	8	4	12	
TOTAAL VOOR ALLE LIDSTATEN	**1 januari 2021 tot en met 6 maart 2023**	**3 156**	**700**	**4 922**	

Bij de bovenstaande gegevens moet een voorbehoud worden gemaakt. Aan de hand van de bestaande statistische gegevens kunnen de lidstaten niet altijd een onderscheid maken tussen gegevens over slachtoffers die zijn geïdentificeerd op basis van een melding van een aanbieder en meldingen die zijn gedaan door bijvoorbeeld het slachtoffer van het strafbare feit zelf of iemand die het slachtoffer kende of het strafbare feit heeft ontdekt (zoals vermeld door Slovenië). Zweden meldde dat ook kinderen worden gemeld die zijn geïdentificeerd op basis van chatlogbestanden, hoewel er nooit foto's of video's van het misbruik zijn gevonden of tot het betreffende slachtoffer zijn herleid.

Over het algemeen komen de gegevens in tabel 8 niet noodzakelijkerwijs overeen met de rapportageverplichtingen in de tijdelijke verordening, waarin uitsluitend slachtoffers worden bedoeld die zijn gered dankzij de meldingen van aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen uit hoofde van de verordening. De gerapporteerde gegevens omvatten in sommige gevallen slachtoffers die om andere redenen of met andere middelen zijn geïdentificeerd.

Aan de hand van de gegevens kan dus geen volledig overzicht worden gemaakt van het aantal kinderen in de EU dat is geïdentificeerd als slachtoffers van online seksueel misbruik.

Zelfs als een slachtoffer werd geïdentificeerd, betekende dat bovendien niet noodzakelijkerwijs dat die identificatie gekoppeld is aan een veroordeling. In sommige gevallen werd het slachtoffer geïdentificeerd maar leverde het onderzoek geen verdachte of veroordeling op (Zweden).

Niettemin kan uit de gegevens worden afgeleid dat een aanzienlijk aantal slachtoffers is geïdentificeerd met behulp van vrijwillige rapportage overeenkomstig de tijdelijke verordening. Dat wordt bevestigd door rapportages van rechtshandhavingsinstanties over zaken die vaak uitsluitend worden geopend na een vrijwillige melding[13].

2.2.3. Aantal veroordeelde daders

De meeste lidstaten hebben aan hun verplichtingen voldaan, maar twee lidstaten hebben geen gegevens verstrekt of een reden opgegeven voor het uitblijven van hun verslag uit hoofde van artikel 8, lid 1, punt c), van de tijdelijke verordening.

Verschillende lidstaten hebben geen statistieken over de rapportageperiode uit hoofde van die bepaling verstrekt en gaven daarvoor de volgende redenen:

- de gegevens waren nog niet beschikbaar (België en Spanje);
- de centrale databank die wordt gebruikt voor het registreren van strafbare feiten, vereist niet dat de aard van de oorspronkelijke verwijzing wordt vermeld (Ierland);
- de informatie wordt niet verzameld (Duitsland).

De lidstaten rapporteerden zeer uiteenlopende gegevens over het aantal veroordeelde daders, en de bestreken rapportageperioden vertoonden geen samenhang, zoals blijkt uit tabel 9.

Tabel 9: Aantal veroordeelde daders

Land	**Verslagperiode**	**Aantal veroordelingen**	**Opmerkingen**
Oostenrijk	2021	850	In de gegevens wordt geen onderscheid gemaakt tussen online en offline gepleegde

[13] Zie bijvoorbeeld een lijst van voorbeeldzaken uit de gehele EU, die zijn geopend dankzij vrijwillige meldingen door de ondernemingen in de effectbeoordeling bij het voorstel voor een verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen (zie met name bijlage 7).

			feiten.
België	—	—	Gegevens niet beschikbaar.
Bulgarije	2021 en 2022	52	
Kroatië	—	—	Gegevens niet beschikbaar.
Cyprus	2022	0	Tot nu toe geen veroordelingen.
Tsjechië	1 januari 2022 tot en met 31 juli 2022	20	
Denemarken	2 augustus 2021 tot en met 20 januari 2023	224	
Estland	2021	2	Omvat uitsluitend veroordelingen als gevolg van NCMEC-meldingen.
Finland	2021	240	
Frankrijk	4 augustus 2021 tot en met 3 augustus 2022	820	
Duitsland	—	—	Gegevens niet beschikbaar.
Griekenland	2021 en 2022	62	
Hongarije	2021 en 2022	126	
Ierland	—	—	Gegevens niet beschikbaar.
Italië	2021 en 2022	5 835	In de gegevens wordt geen onderscheid gemaakt tussen online en offline gepleegde feiten.
Letland	2021 en 2022	33	In de gegevens wordt geen onderscheid gemaakt tussen online en offline gepleegde feiten.
Litouwen	1 januari 2021 tot en met 30 juni 2022	10	
Luxemburg	2022	11	In de gegevens wordt geen onderscheid gemaakt tussen online en offline gepleegde feiten.
Malta	—	—	Gegevens niet ingediend/niet gemeld.
Nederland	2021	217	
Polen	Tweede helft van 2021 tot en met de eerste helft van 2022/2022/eerste helft van 2023	185/194/81	
Portugal	—	—	Gegevens niet ingediend/niet gemeld.
Roemenië	—	—	Gegevens niet ingediend/niet gemeld.
Slowakije	2021	10	
Slovenië	2021 en 2022	45	

Spanje	2022	—	Gegevens niet beschikbaar.
Zweden	2022	55	

Er moet worden opgemerkt dat het aantal veroordelingen niet gelijk is aan het aantal veroordeelde daders, omdat een persoon voor een of meer feiten van online seksueel misbruik van kinderen kan worden veroordeeld.

Bovendien zijn de statistieken over in een bepaalde periode gemelde veroordelingen niet noodzakelijkerwijs gekoppeld aan de meldingen die in diezelfde periode zijn ontvangen (een veroordeling in 2022 kan bijvoorbeeld voortvloeien uit een melding uit 2021 of 2020 en een melding uit 2022 leidt mogelijk pas in 2023 of later tot een veroordeling). Verschillende lidstaten (Ierland, Luxemburg, Zweden) wijzen daar uitdrukkelijk op in hun verslagen.

In sommige gevallen werden er geen statistieken verzameld over de vraag of meldingen van verdachte activiteiten (bv. via het NCMEC) tot veroordelingen leidden of, met andere woorden, de vraag of die veroordelingen het gevolg waren van de gegevens die door een aanbieder of een organisatie van algemeen belang werden verstrekt (Oostenrijk, Letland). Alleen Estland bevestigde uitdrukkelijk dat de statistieken uitsluitend veroordelingen tonen die voortkomen uit NCMEC-meldingen. Meldingen kunnen ook leiden naar andere daders die in de loop van een onderzoek worden onderzocht en veroordeeld (Oostenrijk).

Er wordt grotendeels aangenomen dat het aantal gemelde veroordelingen slaat op zaken die zijn afgerond nadat er vermoedelijk beroep is aangetekend binnen het gerechtelijk stelsel. In één lidstaat (Denemarken), waar de aantallen worden samengesteld op grond van de laatste beslissing, zijn die aantallen niet definitief omdat naderhand beroep kan zijn aangetekend tegen de beslissingen.

In bepaalde gevallen wordt in de gegevens uit de nationale IT-systemen die door de lidstaten zijn doorgegeven, geen onderscheid gemaakt tussen online en offline gepleegde strafbare feiten (Oostenrijk, Luxemburg, Letland).

Vanwege de zeer uiteenlopende verslagen die de lidstaten hebben ingediend en de wijze waarop statistische gegevens op nationaal niveau worden verzameld, kan er dus geen totaaloverzicht worden opgesteld van het aantal daders dat in de EU is veroordeeld voor online seksueel misbruik van kinderen. Momenteel is het met de beschikbare gegevens evenmin mogelijk om veroordelingen binnen concrete verslagperioden duidelijk te koppelen aan overeenkomstig deze verordening gedane meldingen door aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen.

2.3. Ontwikkelingen in de technologische vooruitgang

De technologieën die momenteel worden gebruikt om online seksueel misbruik van kinderen op te sporen, zijn onder andere technologieën en instrumenten die “bekend” (d.w.z. eerder opgespoord) CSAM, “nieuw” (nog niet eerder opgespoord) CSAM en het benaderen van kinderen voor seksuele doeleinden (“grooming”) kunnen herkennen.

De onderstaande voorbeelden omvatten een aantal van de meest gebruikte instrumenten, maar vormen geen uitputtende lijst. Veel van die instrumenten worden beschikbaar gesteld aan aanbieders, rechtshandhavingsinstanties en andere organisaties die een legitiem belang kunnen aantonen. Meestal worden die instrumenten voor maximale nauwkeurigheid gecombineerd met toetsing door mensen.

Dit punt omvat ook nieuwe technologische ontwikkelingen in verband met artificiële intelligentie.

2.3.1. Opsporing van bekend CSAM

De bestaande technologieën om bekend CSAM op te sporen maken uitsluitend gebruik van automatische inhoudelijke analyse[14] en zijn meestal gebaseerd op hashing. Hashingtechnologie is een soort digitale vingerafdruk. Van een afbeelding wordt een unieke digitale handtekening ("hash") gemaakt, die vervolgens wordt vergeleken met handtekeningen (hashes) van andere foto's om kopieën te zoeken van dezelfde afbeelding. Met die technologie kunnen alleen overeenkomende hashes worden gevonden en kan geen materiaal worden "bekeken" waarvan de hash niet overeenstemt. Ook zijn hashwaarden niet omkeerbaar, zodat ze niet kunnen worden gebruikt om een afbeelding opnieuw te creëren.

Er zijn vele varianten en uitvoeringen van hashingtechnologie. Instrumenten voor de opsporing van bekend CSAM zijn onder andere: i) Microsoft PhotoDNA; ii) Google CSAI Match; iii) Apple NeuralHash + Private Set Intersection; iv) Meta SSN++; v) PDQ en TMK+PDQF; vi) MD5 Hash generator (Skype); vii) Safer (Thorn).

Het meest gebruikte instrument is Microsoft PhotoDNA, dat door meer dan 150 organisaties wordt gebruikt[15]. PhotoDNA wordt al meer dan 10 jaar gebruikt en is zeer nauwkeurig. Op basis van tests wordt het aandeel fout-positieve resultaten geschat op slechts 1 per 50 miljard[16]. Het foutenpercentage van PhotoDNA blijft zeer laag vanwege de aard van de technologie. Die technologie herkent uitsluitend kopieën van eerder geïdentificeerd materiaal. De oorspronkelijke versie van PhotoDNA spoort bekend CSAM op in afbeeldingen, maar er is ook een versie voor het opsporen van CSAM in video's beschikbaar.

De technologie wordt voortdurend ontwikkeld en verbeterd. In mei 2023 kondigde Microsoft aan dat nieuwe vergelijkingscapaciteit zou worden ingevoerd om sneller te kunnen zoeken (ongeveer 350 keer sneller) en de kosten van het vergelijkingsproces te verlagen zonder aan nauwkeurigheid in te boeten. Volgens Microsoft is met de nieuwe "library" ook een bredere

---

[14] Aanbieders beschouwen metadata niet als een doeltreffend instrument voor het opsporen van CSAM. Zie in het bijzonder Pfefferkorn, R., Stanford Internet Observatory, "Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers", blz. 10 en 11, 9 september 2021.

[15] Microsoft, Digital Crimes Unit.

[16] Verklaring van Hany Farid, ontwikkelaar van PhotoDNA, voor de Commissie betreffende energie en handel ter bevordering van een gezonder internet om consumenten te beschermen van het Amerikaanse Huis van Afgevaardigden, 16 oktober 2019.

detectie van omgekeerde of gedraaide afbeeldingen mogelijk. Daarnaast heeft de Internet Watch Foundation (IWF) gemeld dat zij onlangs haar hashingtechnologie heeft verbeterd[17].

2.3.2. Opsporing van nieuw CSAM

Technologieën die momenteel voor de opsporing van nieuw CSAM worden gebruikt, zijn onder meer classifiers en artificiële intelligentie (AI) die door analyse van beelden en video's inhoudelijke patronen proberen op te sporen die overeenkomen met patronen die zijn gegenereerd op basis van eerder geïdentificeerd materiaal betreffende seksueel misbruik van kinderen. Een classifier is een algoritme dat gegevens door middel van patroonherkenning in gelabelde klassen of categorieën van informatie plaatst. Classifiers hebben trainingsgegevens nodig en worden nauwkeuriger naarmate zij meer gegevens te verwerken krijgen.

Instrumenten voor het opsporen van nieuw CSAM zijn onder andere: i) Safer (Thorn); ii) Google Content Safety API; iii) AI-technologie van Facebook[18]; iv) Amazon Rekognition; v) Hive AI voor visueel materiaal.

Uit onderzoek blijkt dat geautomatiseerde instrumenten en systemen zoals classifiers de nuttigste middelen zijn om CSAM op te sporen[19]. Wat de opsporing van nieuw CSAM betreft, ligt de nauwkeurigheidsgraad momenteel aanzienlijk boven 90 %. Thorn geeft bijvoorbeeld aan dat haar CSAM-classifier kan worden ingesteld op een nauwkeurigheidsgraad van 99 % (voor zowel bekend als nieuw CSAM), met derhalve 0,1 % fout-positieve resultaten[20]. Die cijfers zullen waarschijnlijk verbeteren naarmate het gebruik en de feedback toenemen.

2.3.3. Opsporen van grooming

Instrumenten voor de opsporing van grooming (het benaderen van kinderen voor seksuele doeleinden) in tekstcommunicatie maken uitsluitend gebruik van technologie om patronen op te sporen die wijzen op mogelijke concrete elementen voor de verdenking van online seksueel misbruik van kinderen, zonder dat de aard van het materiaal kan worden afgeleid. Die techniek wordt toegepast op tekstgebaseerde chatgesprekken. De gesprekken worden ingedeeld volgens een serie kenmerken en krijgen een percentage voor de geschatte waarschijnlijkheid dat het om grooming gaat. Op basis van die indeling wordt door individuele ondernemingen bepaald of de gesprekken verder moeten worden getoetst door mensen.

---

17 Internet Watch Foundation (IWF), jaarverslag 2022, blz. 129-133.

18 Zie hier en hier voor meer informatie over het instrument van Facebook voor het proactief opsporen van kindernaakt en nog onbekende inhoud met betrekking tot de uitbuiting van kinderen, door middel van artificiële intelligentie en machinaal leren.

19 Pfefferkorn, R., "Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers", *Journal of Online Trust and Safety*, februari 2022, blz. 1-38.

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

Voor tekst worden onder andere de volgende instrumenten gebruikt: i) Project Artemis van Microsoft[21]; ii) Amazon Rekognition; iii) de Spirit AI-technologie van Twitch (op basis van NLP en tekstclassifiers)[22]; iv) een door Meta zelf ontwikkelde rangschikkende classifier op basis van machinaal leren (waarbij interne technologie voor taalanalyse wordt gecombineerd met metadata); v) Roblox-chatfiltering[23]; vi) de technische oplossing van Thorn en de Tech Coalition op basis van machinaal leren en classifiers[24].

Net als bij de identificatie van nieuw CSAM moet de technologie voor het vaststellen van grooming worden getraind met gelijkaardig materiaal. Toegang tot dergelijke trainingsgegevens blijft het grootste probleem voor de ontwikkeling en verbetering van die technologieën.

Thorn is met de Tech Coalition en haar leden als partners een nieuw initiatief begonnen om een technische oplossing te ontwikkelen voor het herkennen en aanpakken van pogingen tot online grooming, die nuttig en bruikbaar zal zijn voor uiteenlopende platforms die tekstcommunicatie aanbieden. Die oplossing wordt gebaseerd op de werkzaamheden van een team van Thorn aan een NLP-classifier (natuurlijke-taalverwerking) of een model voor machinaal leren, waarmee online materiaal of gedrag dat onder gedefinieerde “klassen” met betrekking tot grooming valt (zoals blootstelling aan seksueel materiaal of het aansturen op een persoonlijke ontmoeting met een minderjarige) wordt opgespoord en gecategoriseerd en een totaalscore wordt gegeven voor het verband tussen een gesprek en grooming[25].

2.3.4. Nieuwe uitdagingen door chatbots en generatoren van illustraties/beelden met AI

De ontwikkeling en het uitbrengen van AI-chatbots zoals ChatGPT (een groot taalmodel, LLM, ontwikkeld door OpenAI) en generatoren van illustraties/beelden zoals DALL-E[26] en Midjourney[27] heeft grote aandacht van het publiek gekregen, met name omdat ze snel pasklare antwoorden geven of realistische beelden maken die kunnen worden toegepast op een groot aantal verschillende contexten. Deze instrumenten zijn binnen korte tijd populair geworden en worden veel gebruikt. De bekendste producten worden gefinancierd en ontwikkeld door technologiebedrijven zoals Microsoft en Google, de nieuwe technologieën worden verfijnd en er worden regelmatig nieuwe versies ingevoerd.

---

21 Project Artemis van Microsoft is ontwikkeld in samenwerking met The Meet Group, Roblox, Kik en Thorn.

22 Zie voor meer informatie: https://safety.twitch.tv/s/article/Our-Work-to-Combat-Online-Grooming?language=en_US

23 Roblox filtert berichten en chats voor spelers tot en met 12 jaar op ongepaste inhoud, en om te voorkomen dat persoonsgegevens zoals adressen worden gepost in berichten. Het filtersysteem bestrijkt alle openbare en privécommunicatie op Roblox. Roblox, Safety Features: Chat, Privacy & Filtering, geraadpleegd in juli 2023.

24 Tech Coalition, New Technology to Help Companies Keep Young People Safe, 20 juni 2023.

25 Tech Coalition, New Technology to Help Companies Keep Young People Safe, 20 juni 2023.

26 DALL-E is een AI-systeem dat realistische beelden en illustraties kan maken op basis van een beschrijving in natuurlijke taal.

27 Midjourney is een programma en dienst met generatieve artificiële intelligentie waarmee beelden worden gemaakt op basis van beschrijvingen in een natuurlijke taal.

Deze technologieën bieden grote kansen voor het bedrijfsleven en het publiek, maar kunnen ook een risico inhouden. Er is onder meer de bezorgdheid dat criminelen die producten willen gebruiken voor kwade doeleinden, waaronder seksuele uitbuiting van kinderen.

Europol meldt dat alle door ChatGPT verstrekte informatie weliswaar vrij op internet beschikbaar is, maar dat dit instrument het voor kwaadwillende actoren aanzienlijk gemakkelijker maakt "om zonder voorkennis informatie te krijgen over een groot aantal mogelijke misdaadgebieden, van inbraak tot terrorisme, cybercriminaliteit en seksueel misbruik van kinderen". De genoemde personen kunnen die vormen van criminaliteit beter begrijpen en dus beter plegen[28].

ChatGPT wordt door de regels van OpenAI beperkt in zijn antwoorden op vragen naar seksueel, haatzaaiend of gewelddadig materiaal, of materiaal dat zelfbeschadiging bevordert. Die beveiliging kan echter vrij gemakkelijk worden omzeild door de instructies aan te passen (prompt engineering)[29]. De recente invoering van AI-chatbots (bv. door Snapchat) laat zien hoe die de grens van kwetsende of gevaarlijke interacties kunnen overschrijden, onder andere richting seksueel misbruik van kinderen[30]. Nu meer bedrijven overwegen om AI-chatbots te testen op hun platforms (Instagram, eventueel WhatsApp en Messenger), moet het effect op gebruikers zorgvuldig worden beoordeeld, in het bijzonder voor kinderen en jongeren.

Deze nieuwe instrumenten moeten op passende wijze worden beveiligd, zodat zij niet worden misbruikt om met behulp van AI gegenereerd realistisch ogend (deepfake) materiaal te produceren dat seksueel misbruik van kinderen inhoudt[31]. Gezien de snelheid waarmee AI-instrumenten worden ontwikkeld, zal het waarschijnlijk al snel eenvoudiger worden om beelden te genereren die niet van echt kunnen worden onderscheiden. Dat zorgt voor verschillende grote uitdagingen op het vlak van bestrijding van CSA, omdat het onderzoeken en vervolgen van CSAM-zaken door wetshandhavingsinstanties en het identificeren van echte slachtoffers ernstig kunnen worden belemmerd als er online grote hoeveelheden zeer realistisch, door de computer gegenereerd CSAM aanwezig is[32].

Uit onderzoek blijkt dat het bekijken van materiaal betreffende seksueel misbruik van kinderen vaak de eerste stap is richting fysiek misbruik, ongeacht of dat materiaal echt of realistisch ogend

---

28 Europol, ChatGPT — The Impact of Large Language Models on Law Enforcement, 2023, ISBN 978-92-95220-57-7, blz. 7.

29 Swanson, S. M., ChatGPT Generated Child Sex Abuse When Asked to Write BDSM Scenarios, Vice, 6 maart 2023; Mitchell, A., ChatGPT gives sick child sex abuse answer, breaking its rules, New York Post, 24 juli 2023; Europol, ChatGPT — The Impact of Large Language Models on Law Enforcement, 2023, ISBN 978-92-95220-57-7, blz. 5.

30 Fowler, G.A., Snapchat tried to make a safe AI. It chats with me about booze and sex, The Washington Post, 14 maart 2023; Vincent, J., Instagram is apparently testing an AI chatbot that lets you choose from 30 personalities, The Verge, 7 juli 2023.

31 Crawford, A., Smith, T., Illegal trade in AI child sex abuse images exposed, BBC, 27 juni 2023.

32 Thiel, D., Stroebel, M. en Portnoff, R., Generative ML and CSAM: Implications and Mitigations. Stanford Digital Repository, 2023. Te raadplegen op https://purl.stanford.edu/jv206yg3793, https://doi.org/10.25740/jv206yg3793, blz. 2.

misbruik en uitbuiting weergeeft[33]. Daarom is het voor de preventie van daderschap cruciaal om de verspreiding van met AI gegenereerd realistisch ogend materiaal betreffende seksueel misbruik van kinderen te beperken. Een ander belangrijk punt van zorg is dat personen die kinderen benaderen voor seksuele doeleinden, de geavanceerde tekstgeneratiemogelijkheden van ChatGPT en de gratis AI-diensten voor het genereren van beelden op basis van tekst gebruiken om snel en gemakkelijk materiaal te maken voor valse profielen en plausibele gesprekken met jongeren, om kinderen online te benaderen. "ChatGPT zelf zal mensen niet aanmoedigen om kinderen te benaderen voor seksuele doeleinden, maar geeft iedereen wel de mogelijkheid om in zijn online gesprekken met kinderen AI-technologie te gebruiken om overtuigender en geloofwaardiger over te komen bij zijn slachtoffer, wat manipulatie in de hand werkt."[34] Generatieve AI kan potentieel bijdragen aan een toename van het online benaderen van kinderen voor seksueel misbruik en zelfs tot "de grootschalige automatisering"[35] daarvan.

3. CONCLUSIES

Door aanbieders genomen uitvoeringsmaatregelen

Uit de verslaglegging van aanbieders blijkt dat zij online seksueel misbruik van kinderen uit hoofde van de tijdelijke verordening opsporen en melden met behulp van uiteenlopende opsporingstechnologieën en -processen. Alle aanbieders lieten weten dat zij die meldingen naar het NCMEC zenden. Wat het soort en de volumes persoonsgegevens betreft dat door de aanbieders wordt verwerkt, bevat de verslaglegging een verscheidenheid aan verzamelde verkeersgegevens en uiteenlopende detailniveaus van de verwerkte gegevensvolumes, zodat de Commissie op EU-niveau geen eenvormige gegevens in verband met aanbieders kan verkrijgen over de betreffende rapportageperiode (juli 2021 tot en met 31 januari 2023).

De aanbieders verstrekten niet het aantal fouten en de foutverhoudingen (fout-positieve resultaten) per verschillende gebruikte technologie, maar gaven aan dat zij online CSA opsporen met een gelaagde benadering en die aanvullen met toetsing door mensen. Zij maken tevens gebruik van een brede verscheidenheid aan (veiligheids)maatregelen om het foutenpercentage in hun opsporing te beperken en te verminderen. Verder meldden de aanbieders dat zij beleid en maatregelen hebben ingevoerd voor gegevensbewaring en -bescherming, die zijn omschreven in hun privacybeleid of -verklaring en die worden ondersteund door in de sector gebruikelijke beveiligingsmaatregelen.

---

[33] Protect Children, Protect Children's research in the dark web is revealing unprecedented data on CSAM users, 6 juni 2021; RAINN, What is Child Sexual Abuse Material (CSAM), 25augustus 2022.

[34] Breck Foundation, Is artificial intelligence putting children at risk?, 9 februari 2023, bijgewerkt op 3 april 2023.

[35] Butler, J., AI tools could be used by predators to 'automate child grooming', eSafety commissioner warns, The Guardian, 19 mei 2023.

Door de lidstaten genomen uitvoeringsmaatregelen

Bij artikel 8 van de tijdelijke verordening worden ook de lidstaten verplicht om essentiële statistieken te verstrekken over gevallen van online seksueel misbruik van kinderen die zij hebben opgespoord en gemeld aan hun rechtshandhavingsinstanties, het aantal geïdentificeerde kinderslachtoffers en het aantal veroordeelde daders. Aangezien de rapportageperioden waarover de lidstaten gegevens hebben verstrekt meestal uiteenliepen, kon uit de verstrekte gegevens het totale aantal ontvangen meldingen van online seksueel misbruik van kinderen op EU-niveau niet worden berekend. Daarnaast verschilt het aantal meldingen die de lidstaten hebben ontvangen en doorgegeven, wellicht van het aantal te onderzoeken meldingen, d.w.z. meldingen die kunnen worden gebruikt voor een onderzoek, of het aantal gemelde zaken. Slechts enkele lidstaten gaven het type aan van de aanbieders op wiens diensten online seksueel misbruik van kinderen was aangetroffen. In sommige gevallen wordt in de nationale statistische gegevens geen onderscheid gemaakt tussen strafbare feiten die worden onderzocht naar aanleiding van meldingen door aanbieders en andere organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen, en strafbare feiten die worden onderzocht naar aanleiding van andere meldingen.

Daardoor kon uit de ontvangen meldingen niet het totaal aantal kinderen worden afgeleid dat is geïdentificeerd als slachtoffer van online seksueel misbruik van kinderen in de EU, uitgesplitst naar geslacht. De oorzaken zijn onder meer dat: de gemelde gegevens verschillende perioden beslaan; voor de definitie van kinderslachtoffers van online CSA verschillende leeftijdsgrenzen worden gebruikt; op nationaal niveau geen statistieken op dergelijk detailniveau worden verzameld vanwege technische of andere beperkingen; geen onderscheid wordt gemaakt tussen online en offline kinderslachtoffers van CSA enz. Sommige lidstaten nemen in hun statistieken ook kinderen op die zelf materiaal hebben geproduceerd. Van groter belang is dat de statistieken vaak geen onderscheid maken tussen slachtoffers die zijn geïdentificeerd op basis van meldingen uit hoofde van de verordening door aanbieders en organisaties die in het algemeen belang optreden tegen seksueel misbruik van kinderen, en slachtoffers die zijn geïdentificeerd op basis van andere gronden en met andere middelen.

Ook het overzicht van de aantallen veroordeelde daders is gefragmenteerd. In bepaalde gevallen zijn die gegevens niet beschikbaar omdat de bron van de oorspronkelijke melding niet in de databank is vastgelegd, zodat in de gegevens geen onderscheid wordt gemaakt tussen daders die zijn veroordeeld naar aanleiding van meldingen die zijn verstrekt uit hoofde van de verordening en daders die naar aanleiding van andere meldingen zijn veroordeeld. In sommige gevallen zijn de gegevens van het nationale IT-systeem ook niet uitgesplitst naar online en offline gepleegde strafbare feiten. Bovendien zijn de statistieken over gemelde veroordelingen in een bepaalde periode niet noodzakelijkerwijs gekoppeld aan de meldingen die in die periode zijn ontvangen, maar kunnen zij betrekking hebben op meldingen uit eerdere perioden. De verzamelde statistieken over het aantal veroordelingen kan ook afwijken van het aantal veroordeelde daders (omdat een dader meermalen kan zijn veroordeeld).

Door de heterogene statistieken die zijn verstrekt door de lidstaten, die de gegevens niet altijd systematisch en correct lijken te verzamelen, en alle hierboven genoemde factoren is het dus onmogelijk om uit hoofde van de verordening een totaalbeeld te verkrijgen over de ontvangen

meldingen inzake online CSA, het aantal kinderen dat is geïdentificeerd als slachtoffer van dit strafbare feit of het aantal daders dat in de EU is veroordeeld. Het feit dat er voor de meeste lidstaten een significant verschil lijkt te bestaan tussen het aantal meldingen dat volgens het NCMEC naar de lidstaten is gezonden en het aantal meldingen dat volgens de lidstaten is ontvangen, wijst erop dat de verzameling van en rapportering over gegevens onvolledig is. Sommige lidstaten bevestigden dat hun bevoegde autoriteiten structurele veranderingen of reorganisaties ondergaan in verband met het opzetten van nieuwe afdelingen die verantwoordelijk zijn voor het onderzoeken van strafbare feiten in verband met online seksueel misbruik van kinderen. Ook worden er nieuwe IT-systemen ingevoerd en in sommige lidstaten is de nationale autoriteiten verzocht hun registratieprocedures en statistieken te wijzigen. Dat moet gunstige voorwaarden scheppen om in de toekomst nauwkeuriger statistieken uit de lidstaten te krijgen. Hoe dan ook zal de Commissie haar bevoegdheden uit hoofde van de Verdragen waar nodig inzetten om te waarborgen dat de lidstaten voldoen aan hun rapportageverplichtingen uit hoofde van de tijdelijke verordening.

Algemene overwegingen

Al met al laat dit verslag aanzienlijke verschillen zien in het rapporteren over gegevens over de bestrijding van online CSA uit hoofde van de tijdelijke verordening, zowel door aanbieders als door lidstaten. Een grotere standaardisatie van de beschikbare gegevens en de rapportage daarvan, zoals die in het voorstel voor een verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen[36], zou bijdragen aan een beter beeld van de relevante activiteiten in de bestrijding van deze misdaad. Meer inspanningen van aanbieders en lidstaten lijken nodig om te waarborgen dat de gegevensverzameling en de rapportage voldoen aan de eisen van de tijdelijke verordening.

De beschikbare gegevens laten zien dat het onder het huidige vrijwillige opsporings- en meldingssysteem mogelijk is dat materiaal dat automatisch is aangemerkt als mogelijk CSAM, na toetsing door mensen geen CSAM blijkt te zijn. Dat kan te wijten zijn aan het ontbreken van een gemeenschappelijke verzameling hashes en andere indicatoren voor de opsporing van in de EU als illegaal beoordeeld CSAM, of aan uiteenlopende wettelijke normen in de verschillende rechtsgebieden, met name in de EU en de VS, vooral wat de definities betreft. De gegevens wijzen ook in de richting van grote verschillen in het aantal toetsingsverzoeken en de slaagkans van deze verzoeken, met als gevolg dat geen conclusies kunnen worden getrokken omdat er onvoldoende informatie is over met name de strekking van de verzoeken en de redenen om verwijderingen terug te draaien.

Wat betreft de vereisten van artikel 9, lid 2, voor de voorwaarden voor verwerking, blijkt uit de verstrekte informatie dat de gebruikte technologieën overeenkomen met technologische toepassingen die uitsluitend zijn ontworpen voor de opsporing en verwijdering van online materiaal betreffende seksueel misbruik van kinderen en het melden daarvan aan de rechtshandhavingsinstanties en aan organisaties die in het algemeen belang optreden tegen

[36] Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, COM/2022/209 final.

seksueel misbruik van kinderen. Er werd geen informatie verstrekt over de vraag of die technologieën werden ingevoerd volgens de nieuwste ontwikkelingen in de technische vooruitgang en met de minst mogelijke inbreuk op de privacy, en over de vraag of er eerder een gegevensbeschermingseffectbeoordeling volgens artikel 35 van Verordening (EU) 2016/679 en een voorafgaande raadplegingsprocedure volgens artikel 36 van diezelfde verordening zijn uitgevoerd.

Wat de evenredigheid van de tijdelijke verordening betreft, is de centrale vraag of ze tot het evenwicht komt dat de EU-wetgever wilde bereiken tussen enerzijds het behalen van de doelstelling van algemeen belang om de desbetreffende, zeer ernstige misdaden doeltreffend te bestrijden en de behoefte om de grondrechten van kinderen (waardigheid, integriteit, verbod op onmenselijke of vernederende behandeling, persoonlijke levenssfeer, rechten van het kind) te beschermen, en anderzijds het beschermen van de grondrechten van de gebruikers van de betreffende diensten (persoonlijke levenssfeer, bescherming van persoonsgegevens, vrijheid van meningsuiting, doeltreffende voorziening in rechte). Er zijn onvoldoende gegevens beschikbaar om over dit punt definitieve conclusies te trekken. Het is niet mogelijk en het zou ook niet passend zijn om een getalsmatige norm toe te passen bij de beoordeling van de evenredigheid in termen van het aantal geredde kinderen, gezien het significante negatieve effect van seksueel misbruik op het leven en de rechten van een kind. Niettemin zijn er in het licht van het bovenstaande geen aanwijzingen dat de afwijking onevenredig is.

Ondanks de tekortkomingen van de beschikbare gegevens, waardoor in een significant aantal lidstaten geen inzicht kan worden verkregen in het gebruik van vrijwillige meldingen, blijkt uit de beschikbare gegevens duidelijk dat in de rapportageperiode duizenden kinderen zijn geïdentificeerd, meer dan tweeduizend veroordelingen zijn verkregen en miljoenen afbeeldingen en video’s uit omloop zijn gehaald, waardoor secundaire victimisatie werd beperkt. Er kan dus worden geconcludeerd dat vrijwillige meldingen significant hebben bijgedragen aan de bescherming van een groot aantal kinderen, ook tegen lopend misbruik, en dat de tijdelijke verordening doeltreffend lijkt te zijn.