EDPB-EDPS

Gezamenlijk advies 4/2022 over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen

Vastgesteld op 28 juli 2022

Translations proofread by EDPB Members.

This language version has not yet been proofread.

INHOUDSOPGAVE

Samenvatting

De Europese Commissie heeft op 11 mei 2022 een voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen gepubliceerd.

Op grond van het voorstel zouden aanbieders van hostingdiensten, interpersoonlijke communicatiediensten en andere diensten gekwalificeerde verplichtingen worden opgelegd inzake het opsporen, melden, verwijderen en blokkeren van bekend en nieuw onlinemateriaal over seksueel misbruik van kinderen, alsook van het benaderen van kinderen. Het voorstel voorziet ook in de oprichting van een nieuw gedecentraliseerd EU-agentschap (het 'EU-centrum') en een netwerk van nationale coördinerende autoriteiten voor kwesties inzake seksueel misbruik van kinderen om de voorgestelde verordening te kunnen uitvoeren. Zoals in de toelichting bij het voorstel wordt erkend, zouden de in het voorstel vervatte maatregelen van invloed zijn op de uitoefening van de grondrechten van de gebruikers van de betrokken diensten.

Seksueel misbruik van kinderen is een bijzonder ernstig en gruwelijk misdrijf en de doelstelling om doeltreffend te kunnen optreden, is een door de Unie erkende doelstelling van algemeen belang en beoogt de rechten en vrijheden van slachtoffers te beschermen. Tegelijkertijd herinneren het EDPB en de EDPS eraan dat beperkingen van de grondrechten, zoals die waarin het voorstel voorziet, moeten voldoen aan de voorschriften van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie.

Het EDPB en de EDPS benadrukken dat het voorstel aanleiding geeft tot ernstige bezorgdheid over de evenredigheid van de beoogde inmenging en beperkingen op de bescherming van de grondrechten op privacy en de bescherming van persoonsgegevens. In dat verband wijzen het EDPB en de EDPS erop dat procedurele waarborgen nooit volledig in de plaats kunnen komen van materiële waarborgen. Een complex systeem voor escalatie van risicobeoordeling en risicobeperkende maatregelen naar een opsporingsbevel kan niet in de plaats komen van de vereiste duidelijkheid van de materiële verplichtingen.

Het EDPB en de EDPS zijn van mening dat het voorstel niet duidelijk is over belangrijke elementen, zoals het concept 'significant risico'. Bovendien beschikken de entiteiten die belast zijn met de toepassing van deze waarborgen, van particuliere marktdeelnemers tot administratieve en/of gerechtelijke autoriteiten, over een zeer ruime beoordelingsmarge; dit leidt tot rechtsonzekerheid over de vraag hoe de betrokken rechten in elk individueel geval met elkaar in evenwicht kunnen worden gebracht. Het EDPB en de EDPS benadrukken dat de wetgever, wanneer hij bijzonder ernstige inmenging in de grondrechten toestaat, juridische duidelijkheid moet verschaffen over wanneer en waar inmenging is toegestaan. Hoewel het EDPB en de EDPS erkennen dat de wetgeving niet te prescriptief mag zijn en enige flexibiliteit moet bieden bij de praktische toepassing ervan, zijn zij van mening dat het voorstel te veel ruimte laat voor mogelijk misbruik als gevolg van het ontbreken van duidelijke materiële normen.

Wat de noodzaak en evenredigheid van de beoogde opsporingsmaatregelen betreft, maken het EDPB en de EDPS zich met name zorgen over de voorgenomen maatregelen voor de opsporing van onbekend materiaal van seksueel misbruik van kinderen en van het benaderen van kinderen ('grooming') via interpersoonlijke communicatiediensten. Gezien hun indringendheid, hun probabilistische aard en de foutenpercentages in verband met dergelijke technologieën, zijn het EDPB en de EDPS van mening dat de inmenging die deze maatregelen meebrengen, verder gaat dan wat noodzakelijk en evenredig is. Bovendien kunnen maatregelen op grond waarvan de overheidsinstanties op algemene basis toegang krijgen tot de inhoud van een mededeling om het benaderen van kinderen op te sporen, de wezenlijke inhoud van de in de artikelen 7

en 8 van het Handvest gewaarborgde rechten eerder aantasten. Daarom moeten de relevante bepalingen met betrekking tot grooming uit het voorstel worden gehaald. Bovendien wordt in het voorstel het scannen van audiocommunicatie niet van het toepassingsgebied uitgesloten. Het EDPB en de EDPS zijn van mening dat het scannen van audiocommunicatie bijzonder indringend is en als zodanig buiten het toepassingsgebied van de opsporingsverplichtingen van de voorgestelde verordening moet blijven, zowel wat spraakberichten als livecommunicatie betreft.

Het EDPB en de EDPS hebben ook twijfels over de doeltreffendheid van blokkeringsmaatregelen en zijn van mening dat het onevenredig zou zijn om aanbieders van internetdiensten te verplichten onlinecommunicatie te decoderen om het betreffende materiaal van seksueel misbruik van kinderen te blokkeren.

Voorts wijzen het EDPB en de EDPS erop dat versleutelingstechnologieën op fundamentele wijze bijdragen tot de eerbiediging van het privéleven en de vertrouwelijkheid van communicatie, de vrijheid van meningsuiting, alsook tot innovatie en de groei van de digitale economie, die afhankelijk is van de hoge mate van vertrouwen die dergelijke technologieën bieden. In overweging 26 van het voorstel wordt niet alleen bij de keuze van opsporingstechnologieën, maar ook bij die van de technische maatregelen ter bescherming van de vertrouwelijkheid van communicatie, zoals versleuteling, de kanttekening geplaatst dat deze technologische keuze moet voldoen aan de voorschriften van de voorgestelde verordening, dat wil zeggen dat zij opsporing mogelijk moet maken. Dit schraagt de uit artikel 8, lid 3, en artikel 10, lid 2, van het voorstel voortvloeiende gedachte dat een aanbieder de uitvoering van een opsporingsbevel niet kan weigeren op grond van technische onmogelijkheid. Het EDPB en de EDPS zijn van mening dat er een beter evenwicht moet zijn tussen de maatschappelijke behoefte aan veilige en particuliere communicatiekanalen en de bestrijding van misbruik ervan. In het voorstel moet duidelijk worden gesteld dat niets in de voorgestelde verordening mag worden uitgelegd als een verbod op of een verzwakking van de versleuteling.

Hoewel het EDPB en de EDPS ingenomen zijn met de verklaring in het voorstel dat het geen afbreuk doet aan de bevoegdheden en competenties van de gegevensbeschermingsautoriteiten uit hoofde van de AVG, zijn het EDPB en de EDPS van mening dat de verhouding tussen de taken van coördinerende autoriteiten en die van gegevensbeschermingsautoriteiten niettemin beter moet worden geregeld. In dit verband waarderen het EDPB en de EDPS de rol die in het voorstel aan het EDPB wordt toegekend waarbij om zijn betrokkenheid bij de praktische uitvoering van het voorstel wordt verzocht; met name zou het EDPB advies dienen uit te brengen over de technologieën die het EU-centrum beschikbaar zou stellen om opsporingsbevelen uit te voeren. Er moet echter worden verduidelijkt wat het doel van het advies zou zijn en hoe het EU-centrum zou handelen nadat het een advies van het EDPB zou hebben ontvangen.

Tot slot merken het EDPB en de EDPS op dat het voorstel voorziet in nauwe samenwerking tussen het EU-centrum en Europol, die elkaar “van een zo volledig mogelijke toegang tot relevante informatie en informatiesystemen” moeten voorzien. Hoewel het EDPB en de EDPS in beginsel de samenwerking tussen de twee agentschappen steunen (aangezien het EU-centrum geen rechtshandhavingsinstantie is), doen het EDPB en de EDPS nog steeds meerdere aanbevelingen ter verbetering van de desbetreffende bepalingen; zoals het alleen per geval doorgeven van persoonsgegevens tussen het EU-centrum en Europol, na een naar behoren beoordeeld verzoek, via een communicatie-instrument voor beveiligde uitwisseling, zoals Siena.

Het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming

Gezien artikel 42, lid 2, van Verordening 2018/1725 van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG ('EUDPR')[1],

Gezien de EER-overeenkomst en met name bijlage XI en Protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[2],

Gezien het verzoek van de Europese Commissie van 12 mei 2022 om een gezamenlijk advies van het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen[3],

HEBBEN HET VOLGENDE GEZAMENLIJK ADVIES VASTGESTELD

1. ACHTERGROND

1. Op 11 mei 2022 heeft de Europese Commissie ('de Commissie') een voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen (het 'voorstel' of de 'voorgestelde verordening') gepubliceerd[4].

2. Het voorstel is ingediend na de vaststelling van Verordening (EU) 2021/1232 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 (de 'tijdelijke verordening')[5]. De tijdelijke verordening verplicht de betrokken dienstenaanbieders niet om maatregelen te treffen om materiaal van seksueel misbruik van kinderen (zoals foto's, video's, enz.) of van het benaderen van kinderen (ook bekend als 'grooming') via hun diensten op te sporen. Zij staat deze aanbieders echter toe dit op vrijwillige basis te doen, in overeenstemming met de voorwaarden van die verordening[6].

---

[1] PB L 295 van 21.11.2018, blz. 39.
[2] Alle verwijzingen in dit document naar 'lidstaten' moeten worden gelezen als verwijzingen naar 'EER-lidstaten'.
[3] 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.
[4] Ibid.
[5] 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 [2021] L 274/41).
[6] Zie ook advies 7/2020 van de EDPS over het voorstel voor tijdelijke afwijkingen van Richtlijn 2002/58/EG met het oog op de bestrijding van online seksueel misbruik van kinderen (10 november 2020).

3. Het voorstel bestaat uit twee belangrijke bouwstenen. Ten eerste legt zij aanbieders van hostingdiensten, interpersoonlijke communicatiediensten en andere diensten gekwalificeerde verplichtingen op inzake het opsporen, melden, verwijderen en blokkeren van bekend en nieuw onlinemateriaal van seksueel misbruik van kinderen, alsook van het benaderen van kinderen. Ten tweede voorziet het voorstel in de oprichting van een nieuw gedecentraliseerd EU-agentschap ('EU-centrum inzake seksueel misbruik van kinderen' of 'EU-centrum') en een netwerk van nationale coördinerende autoriteiten voor kwesties inzake seksueel misbruik van kinderen om de voorgestelde verordening te kunnen uitvoeren[7].

4. Zoals in de toelichting bij het voorstel wordt erkend, zouden de in het voorstel vervatte maatregelen van invloed zijn op de uitoefening van de grondrechten van de gebruikers van de betrokken diensten. Deze rechten omvatten met name het grondrecht op eerbiediging van de privacy (met inbegrip van de vertrouwelijkheid van communicatie, als onderdeel van het ruimere recht op eerbiediging van het privéleven en van het familie- en gezinsleven), op bescherming van persoonsgegevens en op vrijheid van meningsuiting en van informatie[8].

5. Bovendien zijn dergelijke voorgestelde maatregelen bedoeld om voort te bouwen op de bestaande EU-wetgeving inzake gegevensbescherming en privacy en deze tot op zekere hoogte aan te vullen. In dit verband wordt in de toelichting het volgende opgemerkt:

> "Het voorstel bouwt voort op de algemene verordening gegevensbescherming (AVG). In de praktijk beroepen aanbieders zich vaak op verschillende verwerkingsgronden waarin de AVG voorziet om de verwerking van persoonsgegevens in het kader van de vrijwillige opsporing en melding van online seksueel misbruik van kinderen uit te voeren. Het voorstel voorziet in een systeem van gerichte opsporingsbevelen en preciseert de opsporingsvoorwaarden, zodat meer rechtszekerheid wordt geboden voor deze activiteiten. Wat betreft de verplichte opsporingsactiviteiten waarbij persoonsgegevens worden verwerkt, wordt in het voorstel, en met name in de opsporingsbevelen die op basis daarvan worden uitgevaardigd, aldus de grond voor een dergelijke verwerking vastgesteld als bedoeld in artikel 6, lid 1, punt c, van de AVG, dat voorziet in de verwerking van persoonsgegevens die noodzakelijk is om te voldoen aan een wettelijke verplichting uit hoofde van het recht van de Unie of van de lidstaat waaraan de verwerkingsverantwoordelijke onderworpen is.
>
> Het voorstel heeft onder meer betrekking op aanbieders die interpersoonlijke elektronischecommunicatiediensten aanbieden en bijgevolg onderworpen zijn aan nationale bepalingen ter uitvoering van de e-privacyrichtlijn en de voorgestelde herziening ervan waarover momenteel wordt onderhandeld. De in het voorstel opgenomen maatregelen beperken in sommige opzichten de reikwijdte van de rechten en plichten uit hoofde van de desbetreffende bepalingen van die richtlijn, namelijk met betrekking tot activiteiten die strikt noodzakelijk zijn voor de uitvoering van opsporingsbevelen. In dit opzicht heeft het voorstel betrekking op de toepassing, naar analogie, van artikel 15, lid 1, van die richtlijn."[9]

6. Gezien de ernst van de beoogde inmenging in de grondrechten is het voorstel van bijzonder belang voor de bescherming van de rechten en vrijheden van personen in verband met de verwerking van persoonsgegevens. Zo heeft de Commissie op 12 mei 2022 besloten het Europees Comité voor

[7] COM(2022) 209 final, blz. 17.
[8] COM(2022) 209 final, blz. 12.
[9] COM(2022) 209 final, blz. 4-5.

gegevensbescherming ('EDPB') en de Europese Toezichthouder voor gegevensbescherming ('EDPS') te raadplegen overeenkomstig artikel 42, lid 2, van de EUDPR.

2. DRAAGWIJDTE VAN HET ADVIES

7. In dit gezamenlijk advies worden de gemeenschappelijke standpunten van het EDPB en de EDPS over het voorstel uiteengezet. Het is beperkt tot de aspecten van het voorstel die betrekking hebben op de bescherming van privacy en persoonsgegevens. In het gezamenlijk advies wordt met name gewezen op de gebieden waar het voorstel onvoldoende bescherming van de grondrechten op privacy en gegevensbescherming waarborgt of waar verdere aanpassing aan het EU-rechtskader inzake de bescherming van privacy en persoonsgegevens is vereist.

8. Zoals in dit gezamenlijk advies nader wordt toegelicht, geeft het voorstel aanleiding tot ernstige bezorgdheid over de noodzaak en evenredigheid van de beoogde inmenging en beperkingen op de bescherming van de grondrechten op privacy en de bescherming van persoonsgegevens. Het doel van dit gezamenlijk advies is echter noch om een uitputtende lijst te geven van alle in het voorstel aan de orde gestelde kwesties op het gebied van privacy en gegevensbescherming, noch om specifieke suggesties te doen om de formulering van het voorstel te verbeteren. In plaats daarvan bevat dit gezamenlijk advies opmerkingen op hoog niveau over de belangrijkste punten van zorg in het voorstel die door het EDPB en de EDPS zijn geïdentificeerd. Niettemin blijven het EDPB en de EDPS beschikbaar om tijdens het wetgevingsproces met betrekking tot het voorstel verdere opmerkingen en aanbevelingen aan de medewetgevers te formuleren.

3. ALGEMENE OPMERKINGEN OVER HET RECHT OP VERTROUWELIJKHEID VAN COMMUNICATIE EN OP BESCHERMING VAN PERSOONSGEGEVENS

9. Vertrouwelijkheid van communicatie is een wezenlijk onderdeel van het grondrecht op eerbiediging van het privéleven en het familie- en gezinsleven, dat is neergelegd in artikel 7 van het Handvest van de grondrechten van de Europese Unie (het 'Handvest')[10]. Bovendien wordt in artikel 8 van het Handvest een grondrecht op bescherming van persoonsgegevens erkend. Het recht op vertrouwelijkheid van communicatie en het recht op eerbiediging van het privéleven en het familie- en gezinsleven zijn ook gewaarborgd in artikel 8 van het Europees Verdrag voor de rechten van de mens ('EVRM') en maken deel uit van de gemeenschappelijke constitutionele tradities van de lidstaten[11].

10. Het EDPB en de EDPS herinneren eraan dat de in de artikelen 7 en 8 van het Handvest verankerde rechten geen absolute rechten zijn, maar moeten worden beschouwd in relatie tot hun functie in de

[10] Zie bijvoorbeeld de verklaring van het EDPB over de herziening van de e-privacyverordening en de gevolgen daarvan voor de bescherming van personen in verband met de privacy en de vertrouwelijkheid van hun communicatie (25 mei 2018).

[11] Bijna alle Europese grondwetten bevatten een recht ter bescherming van de vertrouwelijkheid van communicatie. Zie bijvoorbeeld artikel 15 van de grondwet van de Italiaanse Republiek, artikel 10 van de grondwet van de Bondsrepubliek Duitsland, artikel 22 van de Belgische Grondwet en artikel 13 van de Grondwet van het Koninkrijk der Nederlanden.

samenleving[12]. Seksueel misbruik van kinderen is een bijzonder ernstig en gruwelijk misdrijf en de doelstelling om doeltreffend te kunnen optreden, is een door de Unie erkende doelstelling van algemeen belang en beoogt de rechten en vrijheden van slachtoffers te beschermen. Wat de doeltreffend optreden ter bestrijding van strafbare feiten jegens minderjarigen en andere kwetsbare personen betreft, heeft het Hof van Justitie van de Europese Unie ('HvJ-EU') erop gewezen dat positieve verplichtingen uit artikel 7 van het Handvest kunnen voortvloeien; op grond daarvan kunnen overheidsinstanties worden verplicht wettelijke maatregelen te nemen ter bescherming van het privé-leven, het familie- en gezinsleven, de woning en de communicatie. Dergelijke verplichtingen kunnen ook voortvloeien uit de artikelen 3 en 4 van het Handvest, wat betreft de bescherming van de lichamelijke en geestelijke integriteit van een persoon en het verbod op foltering en onmenselijke en vernederende behandeling[13].

11. Tegelijkertijd moeten beperkingen van de door het Handvest gewaarborgde rechten, zoals die waarin het voorstel voorziet[14], voldoen aan de voorschriften van artikel 52, lid 1, van het Handvest. Elke maatregel die afbreuk doet aan het recht op vertrouwelijkheid van communicatie en het recht op eerbiediging van het privéleven en van het familie- en gezinsleven moet in de eerste plaats de wezenlijke inhoud van de betrokken rechten eerbiedigen[15]. De wezenlijke inhoud van een recht wordt aangetast wanneer het recht zijn basisinhoud verliest en de persoon het niet kan uitoefenen[16]. De inmenging mag, gelet op het nagestreefde doel, niet een dergelijke onevenredige en ontoelaatbare inmenging vormen waardoor het aldus gewaarborgde recht in zijn kern wordt aangetast[17]. Dit betekent dat zelfs een grondrecht dat niet absoluut van aard is, zoals het recht op vertrouwelijkheid van communicatie en het recht op bescherming van persoonsgegevens, een aantal kernelementen bevat die niet kunnen worden beperkt.

12. Het HvJ-EU heeft op het gebied van de privacy van elektronische communicatie herhaaldelijk de toets van de "wezenlijke inhoud van een recht" toegepast. In het arrest Tele2 Sverige en Watson heeft het Hof geoordeeld dat wetgeving die bewaring van de inhoud van een communicatie niet toestaat, de wezenlijke inhoud van het recht op eerbiediging van het privéleven en op bescherming van persoonsgegevens niet aantast[18]. In het arrest Schrems heeft het Hof geoordeeld dat wetgeving op grond waarvan de overheidsinstanties veralgemeend toegang kunnen krijgen tot de inhoud van elektronische communicatie wordt beschouwd als een aantasting van de wezenlijke inhoud van het grondrecht op eerbiediging van het privéleven zoals gewaarborgd door artikel 7 van het Handvest[19]. In het arrest Digital Rights Ireland en Seitlinger en anderen heeft het Hof geoordeeld dat de door

---

[12] Zie onder meer het arrest van het HvJ-EU in zaak C-311/18, Facebook Ireland en Schrems, punt 172, en de aldaar aangehaalde rechtspraak. Zie ook overweging 4 van de AVG.
[13] HvJ-EU, gevoegde zaken C-511/18, C-512/18 en C-520/18, La Quadrature du Net en anderen, punten 126-128. Zie ook advies 7/2020 van de EDPS over het voorstel voor tijdelijke afwijkingen van Richtlijn 2002/58/EG ten behoeve van de bestrijding van online seksueel misbruik van kinderen (10 november 2020), punt 12.
[14] Zie COM(2022) 209 final, blz. 12-13.
[15] Artikel 52, lid 1, van het Handvest.
[16] Zie 'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (Richtsnoeren van de EDPS betreffende de beoordeling van de evenredigheid van maatregelen die de grondrechten op privacy en op de bescherming van persoonsgegevens beperken) (19 december 2019), blz. 8, beschikbaar op https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.
[17] HvJ-EU, zaak C-393/19, OM, punt 53.
[18] HvJ-EU, gevoegde zaken C-203/15 en C-698/15, *Tele2 Sverige en Watson*, punt 101.
[19] HvJ-EU, zaak C-362/14, Schrems, punt 94.

Richtlijn 2006/24/EG vereiste bewaring van gegevens weliswaar een bijzonder ernstige inmenging vormde in het grondrecht op eerbiediging van het privéleven en de andere in artikel 7 van het Handvest neergelegde rechten, maar de wezenlijke inhoud van die rechten niet aantastte, aangezien de richtlijn niet toestond kennis van de inhoud van de elektronische communicatie als zodanig te verwerven[20]. Uit deze rechtspraak kan worden afgeleid dat maatregelen op grond waarvan de overheidsinstanties veralgemeend toegang kunnen krijgen tot de inhoud van communicatie, de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten eerder kunnen aantasten. Deze overwegingen zijn ook relevant met betrekking tot maatregelen voor de opsporing van materiaal van seksueel misbruik van kinderen en van het benaderen van kinderen, zoals die welke in het voorstel worden beoogd.

13. Voorts heeft het HvJ-EU geoordeeld dat gegevensbeveiligingsmaatregelen een belangrijke rol spelen om ervoor te zorgen dat de wezenlijke inhoud van het grondrecht op bescherming van persoonsgegevens in artikel 8 van het Handvest niet wordt aangetast[21]. In het digitale tijdperk zijn technische oplossingen voor de beveiliging en bescherming van de vertrouwelijkheid van elektronische communicatie, met inbegrip van maatregelen voor versleuteling, van cruciaal belang om het genot van alle grondrechten te waarborgen[22]. Hiermee moet terdege rekening worden gehouden bij de beoordeling van maatregelen voor de verplichte opsporing van materiaal van seksueel misbruik van kinderen of van het benaderen van kinderen, met name wanneer deze zouden leiden tot een verzwakking of aantasting van de versleuteling[23].

14. In artikel 52, lid 1, van het Handvest wordt ook bepaald dat beperkingen op de uitoefening van een door het Handvest gewaarborgd grondrecht bij wet moeten worden vastgesteld. Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen[24]. Om te voldoen aan het vereiste van evenredigheid moet de wetgeving duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregelen bevatten die minimale eisen opleggen, zodat de personen wier gegevens worden verwerkt, over voldoende garanties beschikken dat hun gegevens doeltreffend worden beschermd tegen het risico van misbruik[25]. Die wetgeving moet aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt[26]. Zoals het HvJ-EU heeft verduidelijkt, is de behoefte aan dergelijke waarborgen des te groter wanneer persoonsgegevens automatisch worden verwerkt en

[20] HvJ-EU, gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger en anderen, punt 39.
[21] Ibid., punt 40.
[22] Zie Resolutie 47/16 van de Mensenrechtenraad over de bevordering, bescherming en uitoefening van mensenrechten op het internet, VN-doc. A/HRC/RES/47/16 (26 juli 2021).
[23] Zie ook overweging 25 van de tijdelijke verordening.
[24] Zie 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (Beoordeling van de noodzakelijkheid van maatregelen die het grondrecht op bescherming van persoonsgegevens beperken: een toolkit), 11 april 2019, beschikbaar op https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] HvJ-EU, gevoegde zaken C-511/18, C-512/18 en C-520/18, La Quadrature du Net en anderen, punt 132.
[26] Ibid.

wanneer de bescherming van de specifieke categorie persoonsgegevens die gevoelige gegevens zijn, in het geding is[27].

15. Het voorstel zou de uitoefening van de rechten en verplichtingen waarin artikel 5, leden 1 en 3, en artikel 6, lid 1, van Richtlijn 2002/58/EG ('e-privacyrichtlijn')[28] voorzien, beperken voor zover dat nodig is voor de uitvoering van de overeenkomstig hoofdstuk 1, afdeling 2, van het voorstel uitgevaardigde opsporingsbevelen. Het EDPB en de EDPS zijn van mening dat het voorstel derhalve niet alleen moet worden beoordeeld in het licht van het Handvest en de AVG, maar ook in het licht van de artikelen 5, 6 en 15, lid 1, van de e-privacyrichtlijn.

[27] Ibid.

[28] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) zoals gewijzigd bij Richtlijn 2006/24/EG en Richtlijn 2009/136/EG.

4. SPECIFIEKE OPMERKINGEN

4.1 Verhouding tot bestaande wetgeving

4.1.1 Verhouding tot de AVG en de e-privacyrichtlijn

16. In het voorstel wordt gesteld dat het de regels die voortvloeien uit andere handelingen van de Unie, met name de AVG[29] en de e-privacyrichtlijn, onverlet laat. In tegenstelling tot de tijdelijke verordening voorziet het voorstel niet in een uitdrukkelijke tijdelijke afwijking, maar in een beperking van de uitoefening van de rechten en verplichtingen die zijn vastgelegd in artikel 5, leden 1 en 3, en artikel 6, lid 1, van de e-privacyrichtlijn. Voorts moet worden opgemerkt dat de tijdelijke verordening uitsluitend voorziet in een afwijking van de bepalingen van artikel 5, lid 1, en artikel 6, lid 1, en niet van artikel 5, lid 3, van de e-privacyrichtlijn.

17. In het voorstel wordt voorts verwezen naar artikel 15, lid 1, van de e-privacyrichtlijn, dat de lidstaten de mogelijkheid biedt wettelijke maatregelen te treffen om de reikwijdte van de in de artikelen 5 en 6 van die richtlijn bedoelde rechten en verplichtingen te beperken wanneer een dergelijke beperking een noodzakelijke, passende en evenredige maatregel in een democratische samenleving vormt, onder meer om strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen. Volgens het voorstel wordt artikel 15, lid 1, van de e-privacyrichtlijn naar analogie toegepast wanneer het voorstel de uitoefening van de rechten en verplichtingen waarin artikel 5, leden 1 en 3, en artikel 6, lid 1 van de e-privacyrichtlijn voorzien, beperkt.

18. Het EDPB en de EDPS herinneren eraan dat het HvJ-EU duidelijk heeft gemaakt dat artikel 15, lid 1, van de e-privacyrichtlijn strikt moet worden uitgelegd, wat betekent dat de uitzondering op het beginsel van vertrouwelijkheid van communicatie die op grond van artikel 15, lid 1, wordt toegestaan, een uitzondering moet blijven en niet de regel mag worden[30]. Zoals verder uiteengezet in dit gezamenlijk advies, zijn het EDPB en de EDPS van mening dat het voorstel niet voldoet aan de vereisten van (strikte) noodzakelijkheid, doeltreffendheid en evenredigheid. Bovendien concluderen het EDPB en de EDPS dat het voorstel zou inhouden dat de inmenging in de vertrouwelijkheid van communicatie in feite de regel kan worden in plaats van de uitzondering te blijven.

4.1.2 Verhouding tot Verordening (EU) 2021/1232 en gevolgen voor de vrijwillige opsporing van online seksueel misbruik van kinderen

19. Op grond van artikel 88 van het voorstel zou de vaststelling ervan leiden tot de intrekking van de tijdelijke verordening die voorziet in een tijdelijke afwijking van sommige bepalingen van de e-privacyrichtlijn om het vrijwillige gebruik van technologieën voor het opsporen van materiaal van seksueel misbruik van kinderen en van het benaderen van kinderen door aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten mogelijk te maken. Vanaf de datum van toepassing van de voorgestelde verordening zou er dus geen afwijking van de e-privacyrichtlijn

[29] 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) (Voor de EER relevante tekst) (PB L 119 van 4.5.2016, blz. 1-88).
[30] Arrest van 21 december 2016, gevoegde zaken C-203/15 en C-698/15, Tele2 Sverige AB en Watson, punt 89.

mogelijk zijn die zou voorzien in de vrijwillige opsporing van online seksueel misbruik van kinderen door dergelijke aanbieders.

20. Aangezien de door het voorstel ingevoerde opsporingsverplichtingen alleen van toepassing zouden zijn op ontvangers van opsporingsbevelen, zou het belangrijk zijn in de tekst van de voorgestelde verordening duidelijk te maken dat het vrijwillige gebruik van technologieën voor het opsporen van materiaal van seksueel misbruik van kinderen en van het benaderen van kinderen alleen toegestaan blijft voor zover dit wordt toegelaten overeenkomstig de e-privacyrichtlijn en de AVG. Dit zou er bijvoorbeeld toe leiden dat aanbieders van nummeronafhankelijke interpersoonlijke communicatiediensten wordt belet dergelijke technologieën op vrijwillige basis te gebruiken, tenzij dit is toegestaan op grond van nationale wetgeving tot omzetting van de e-privacyrichtlijn, overeenkomstig artikel 15, lid 1, van de e-privacyrichtlijn en het Handvest.

21. Meer in het algemeen zou de voorgestelde verordening baat hebben bij meer duidelijkheid over de status van de vrijwillige opsporing van online seksueel misbruik van kinderen na de datum van toepassing van de voorgestelde verordening, en bij de overgang van de in de tijdelijke verordening vastgestelde regeling voor vrijwillige opsporing naar de in de voorgestelde verordening vastgestelde opsporingsverplichtingen. Zo bevelen het EDPB en de EDPS aan duidelijk te maken dat de voorgestelde verordening niet voorziet in een rechtsgrondslag voor de verwerking van persoonsgegevens met als enig doel online seksueel misbruik van kinderen op vrijwillige basis op te sporen.

4.2 Rechtsgrondslag op grond van de AVG

22. Het voorstel heeft tot doel een rechtsgrond in de zin van de AVG vast te stellen voor de verwerking van persoonsgegevens voor de opsporing van materiaal van seksueel misbruik van kinderen en grooming. In de toelichting wordt dan ook het volgende opgemerkt: “Wat betreft de verplichte opsporingsactiviteiten waarbij persoonsgegevens worden verwerkt, wordt in het voorstel, en met name in de opsporingsbevelen die op basis daarvan worden uitgevaardigd, aldus de grond voor een dergelijke verwerking vastgesteld als bedoeld in artikel 6, lid 1, punt c, van de AVG, dat voorziet in de verwerking van persoonsgegevens die noodzakelijk is om te voldoen aan een wettelijke verplichting uit hoofde van het recht van de Unie of van de lidstaat waaraan de verwerkingsverantwoordelijke onderworpen is”.[31]

23. Het EDPB en de EDPS zijn ingenomen met het besluit van de Commissie om de rechtsonzekerheid over de rechtsgrondslag voor de verwerking van persoonsgegevens weg te nemen, die in het kader van de tijdelijke verordening is ontstaan. Het EDPB en de EDPS zijn het ook eens met de conclusie van de Commissie dat de gevolgen van de toepassing van opsporingsmaatregelen te verreikend en ernstig zijn om het besluit over de uitvoering van dergelijke maatregelen aan de dienstenaanbieders over te laten [32]. Tegelijkertijd merken het EDPB en de EDPS op dat elke rechtsgrondslag die dienstenaanbieders ertoe verplicht zich te mengen in de grondrechten inzake gegevensbescherming en privacy, alleen geldig is voor zover die voldoet aan de voorwaarden van artikel 52, lid 1, van het Handvest, zoals geanalyseerd in de volgende punten.

4.3 Verplichtingen inzake risicobeoordeling en -beperking

24. In hoofdstuk II, afdeling 1, van het voorstel moeten aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten voor elk van de diensten die zij aanbieden, het risico op het

[31] Ibid., blz. 4.
[32] Zie voorstel, COM(2022) 209 final, blz. 14.

gebruik van de dienst voor online seksueel misbruik van kinderen vaststellen, analyseren en beoordelen, en vervolgens trachten het vastgestelde risico tot een minimum te beperken door "redelijke risicobeperkende maatregelen die zijn afgestemd op het [...] vastgestelde risico" toe te passen.

25. Het EDPB en de EDPS merken op dat de aanbieder bij het uitvoeren van een risicobeoordeling met name rekening moet houden met de in artikel 3, lid 2, punten a tot en met e, van het voorstel genoemde elementen, waaronder: in de algemene voorwaarden van de aanbieder vastgestelde verboden en beperkingen, de wijze waarop gebruikers de dienst gebruiken en de effecten daarvan op dat risico, de wijze waarop de aanbieder de dienst heeft ontworpen en deze exploiteert, met inbegrip van het bedrijfsmodel, beheer en relevante systemen en processen, en de effecten daarvan op dat risico. Wat het risico van het benaderen van kinderen betreft, moet rekening worden gehouden met de volgende elementen: de mate waarin de dienst wordt gebruikt of waarschijnlijk zal worden gebruikt door kinderen, de leeftijdscategorieën en het risico op het benaderen van kinderen in verband met deze leeftijdscategorieën, de beschikbaarheid van functies om andere gebruikers te zoeken, van functies voor gebruikers om rechtstreeks contact op te nemen met andere gebruikers, met name door middel van privéberichten, en van functies voor gebruikers om afbeeldingen of video's met andere gebruikers te delen.

26. Hoewel het EDPB en de EDPS erkennen dat deze criteria relevant lijken, vrezen zij niettemin dat dergelijke criteria redelijk wat ruimte voor interpretatie en beoordeling laten. Verschillende criteria worden in zeer algemene termen beschreven (zoals "de wijze waarop gebruikers de dienst gebruiken en de effecten daarvan op dat risico") of hebben betrekking op basisfuncties die veel onlinediensten gemeen hebben (zoals "de mogelijkheid voor gebruikers om afbeeldingen of video's met andere gebruikers te delen"). Als zodanig lijken de criteria vatbaar voor een subjectieve (in plaats van objectieve) beoordeling.

27. Volgens het EDPB en de EDPS geldt hetzelfde voor de risicobeperkende maatregelen die op grond van artikel 4 van het voorstel moeten worden genomen. Maatregelen zoals het aanpassen, aan de hand van passende technische en operationele maatregelen en de personeelsbezetting, van de inhoudsmoderatie- of aanbevelingssystemen van de aanbieder, lijken relevant om het vastgestelde risico te verminderen. Indien deze criteria echter worden toegepast in het kader van een complex risicobeoordelingsproces en in combinatie met abstracte en vage termen om de aanvaardbare omvang van het risico te beschrijven (zoals "in belangrijke mate"), voldoen zij niet aan de criteria inzake rechtszekerheid en voorspelbaarheid die nodig zijn om inmenging in de vertrouwelijkheid van communicatie tussen particulieren te rechtvaardigen die een duidelijke inmenging vormt in de grondrechten op privacy en vrijheid van meningsuiting.

28. Hoewel aanbieders zich niet mogen mengen in de vertrouwelijkheid van communicatie als onderdeel van hun strategieën inzake risicobeoordeling en -beperking voordat zij een opsporingsbevel ontvangen, bestaat er een rechtstreeks verband tussen de verplichtingen inzake risicobeoordeling en -beperking en de daaruit voortvloeiende opsporingsverplichtingen. In artikel 7, lid 4, van het voorstel wordt de uitvaardiging van een opsporingsbevel afhankelijk gesteld van het bestaan van bewijs van een significant risico dat de betrokken dienst kan worden gebruikt voor online seksueel misbruik van kinderen. Voordat een opsporingsbevel wordt uitgevaardigd, moet een complexe procedure worden gevolgd waarbij de aanbieders, de coördinerende autoriteit en de gerechtelijke of andere onafhankelijke administratieve autoriteit die verantwoordelijk is voor de uitvaardiging van het bevel, betrokken zijn. Ten eerste moeten aanbieders het risico van het gebruik van hun diensten voor online seksueel misbruik van kinderen beoordelen (artikel 3 van het voorstel) en mogelijke risicobeperkende maatregelen evalueren (artikel 4 van het voorstel) om dat risico te beperken. De resultaten hiervan

moeten vervolgens worden meegedeeld aan de bevoegde coördinerende autoriteit (artikel 5 van het voorstel). Indien uit de risicobeoordeling blijkt dat een significant risico blijft bestaan, ondanks de inspanningen om het te beperken, hoort de coördinerende autoriteit de aanbieder over een ontwerpverzoek tot uitvaardiging van een opsporingsbevel en biedt zij de aanbieder de mogelijkheid opmerkingen te maken. De aanbieder is voorts verplicht een uitvoeringsplan voor te leggen, met inbegrip van een advies van de bevoegde gegevensbeschermingsautoriteit in het geval van opsporing van grooming. Indien de coördinerende autoriteit de zaak doorzet, wordt een opsporingsbevel gevraagd en uiteindelijk uitgevaardigd door een rechtbank of een andere onafhankelijke administratieve autoriteit. Daarom vormen de initiële risicobeoordeling en de gekozen maatregelen om het vastgestelde risico te beperken een beslissende basis voor de beoordeling door de coördinerende autoriteit en door de bevoegde gerechtelijke of administratieve autoriteit van de vraag of een opsporingsbevel noodzakelijk is.

29. Het EDPB en de EDPS nemen nota van de complexe stappen die leiden tot de uitvaardiging van een opsporingsbevel, waaronder een initiële risicobeoordeling door de aanbieder en het voorstel van de aanbieder voor risicobeperkende maatregelen, alsook de verdere interactie van de aanbieder met de bevoegde coördinerende autoriteit. Het EDPB en de EDPS zijn van mening dat de aanbieder een aanzienlijke mogelijkheid heeft om het resultaat van het proces te beïnvloeden. In dit verband merken het EDPB en de EDPS op dat in overweging 17 van het voorstel wordt bepaald dat aanbieders in het kader van de risicorapportage "hun bereidheid" moeten kunnen aangeven om uiteindelijk een opsporingsbevel te ontvangen. Daarom kan niet worden aangenomen dat elke aanbieder zal trachten de uitvaardiging van een opsporingsbevel te vermijden teneinde de vertrouwelijkheid van de communicatie van zijn gebruikers te waarborgen door de meest doeltreffende, maar minst indringende risicobeperkende maatregelen toe te passen, met name wanneer dergelijke maatregelen de vrijheid van ondernemerschap van de aanbieder overeenkomstig artikel 16 van het Handvest aantasten.

30. Het EDPB en de EDPS willen benadrukken dat procedurele waarborgen nooit volledig in de plaats kunnen komen van materiële waarborgen. Het hierboven beschreven complexe proces dat leidt tot de mogelijke uitvaardiging van een opsporingsbevel, moet dus gepaard gaan met duidelijke materiële verplichtingen. Het EDPB en de EDPS zijn van mening dat in het voorstel onduidelijkheid bestaat ten aanzien van een aantal belangrijke elementen (zoals de begrippen 'significant risico', 'in belangrijke mate' enz.), wat niet kan worden weggenomen door de aanwezigheid van meerdere lagen procedurele waarborgen. Dit geldt temeer in het licht van het feit dat de entiteiten die belast zijn met de toepassing van deze waarborgen (zoals aanbieders, gerechtelijke autoriteiten, enz.) over een ruime beoordelingsmarge beschikken om de betrokken rechten in elk individueel geval met elkaar in evenwicht te brengen. Gezien de vergaande inmenging in de grondrechten als gevolg van de vaststelling van het voorstel, moet de wetgever ervoor zorgen dat het voorstel meer duidelijkheid verschaft over wanneer en waar dergelijke inmenging is toegestaan. Hoewel het EDPB en de EDPS erkennen dat wetgevingsmaatregelen niet te prescriptief mogen zijn en enige flexibiliteit moeten bieden bij de praktische toepassing ervan, zijn zij van mening dat de huidige tekst van het voorstel te veel ruimte laat voor mogelijk misbruik als gevolg van het ontbreken van duidelijke materiële normen.

31. Gezien de mogelijk aanzienlijke gevolgen voor een zeer groot aantal betrokkenen (d.w.z. potentieel alle gebruikers van interpersoonlijke communicatiediensten), benadrukken het EDPB en de EDPS de noodzaak van een hoge mate van rechtszekerheid, duidelijkheid en voorspelbaarheid van de wetgeving om ervoor te zorgen dat de voorgestelde maatregelen daadwerkelijk doeltreffend zijn om de nagestreefde doelstelling te verwezenlijken en tegelijkertijd de grondrechten in kwestie het minst schaden.

4.4 Voorwaarden voor de uitvaardiging van opsporingsbevelen

32. In artikel 7 van het voorstel wordt bepaald dat de coördinerende autoriteit van vestiging de bevoegdheid heeft om de bevoegde gerechtelijke autoriteit of een andere onafhankelijke administratieve autoriteit van die lidstaat te verzoeken een opsporingsbevel uit te vaardigen om een aanbieder van hostingdiensten of een aanbieder van interpersoonlijke communicatiediensten ertoe te verplichten de in artikel 10 bedoelde maatregelen te nemen om online seksueel misbruik van kinderen op een specifieke dienst op te sporen.

33. Het EDPB en de EDPS houden terdege rekening met de volgende elementen waaraan moet worden voldaan voordat een opsporingsbevel wordt uitgevaardigd:

    a. er is bewijs dat een significant risico bestaat dat de dienst wordt gebruikt voor online seksueel misbruik van kinderen in de zin van artikel 7, leden 5, 6 en 7, naargelang het geval; en

    b. de redenen voor het uitvaardigen van het opsporingsbevel wegen zwaarder dan de negatieve gevolgen voor de rechten en gerechtvaardigde belangen van alle getroffen partijen, waarbij met name de noodzaak in aanmerking wordt genomen om een billijk evenwicht tussen de grondrechten van die partijen te waarborgen.

34. De betekenis van 'significant risico' wordt gespecificeerd in lid 5 en volgende van artikel 7, afhankelijk van het soort opsporingsbevel in kwestie. Er wordt uitgegaan van een significant risico in het geval van opsporingsbevelen met betrekking tot de opsporing van bekend materiaal van seksueel misbruik van kinderen indien:

    a. het, ondanks de risicobeperkende maatregelen die de aanbieder heeft genomen of zal nemen, waarschijnlijk is dat de dienst in belangrijke mate wordt gebruikt voor de verspreiding van bekend materiaal van seksueel misbruik van kinderen; en

    b. er bewijs is dat de dienst, of een vergelijkbare dienst indien de dienst op de datum van het verzoek om uitvaardiging van het opsporingsbevel nog niet in de Unie wordt aangeboden, in de afgelopen twaalf maanden in belangrijke mate is gebruikt voor de verspreiding van bekend materiaal van seksueel misbruik van kinderen.

35. Om een opsporingsbevel voor onbekend materiaal van seksueel misbruik van kinderen uit te vaardigen, moeten de waarschijnlijkheid en het feitelijke bewijs verwijzen naar onbekend materiaal van seksueel misbruik van kinderen, en moet een voorafgaand opsporingsbevel voor bekend materiaal van seksueel misbruik van kinderen zijn uitgevaardigd en hebben geleid tot een aanzienlijk aantal meldingen met betrekking tot materiaal van seksueel misbruik van kinderen die door de aanbieder zijn ingediend (artikel 7, lid 6, van het voorstel). Wat betreft opsporingsbevelen die betrekking hebben op grooming wordt geacht sprake te zijn van het significante risico wanneer de aanbieder een aanbieder van interpersoonlijke communicatiediensten is, het waarschijnlijk is dat de dienst in belangrijke mate wordt gebruikt voor het benaderen van kinderen en het waarschijnlijk is dat de dienst in belangrijke mate is gebruikt voor het benaderen van kinderen (artikel 7, lid 7, van het voorstel).

36. Het EDPB en de EDPS merken op dat zelfs met de specificaties in artikel 7, leden 5 tot en met 7, van het voorstel, in de voorwaarden voor de uitvaardiging van een opsporingsbevel vage juridische termen de overhand hebben, zoals 'in belangrijke mate' en 'aanzienlijk aantal', en deels repetitief van aard zijn, aangezien bewijzen van eerder misbruik vaak zullen bijdragen tot het vaststellen van de waarschijnlijkheid van toekomstig misbruik.

37. Het voorstel voorziet in een systeem waarbij, wanneer wordt beslist of een opsporingsbevel noodzakelijk is, een voorspellende beslissing moet worden genomen over het toekomstige gebruik van een dienst voor online seksueel misbruik van kinderen. Het is dan ook begrijpelijk dat de in artikel 7 genoemde elementen een prognostisch karakter hebben. Het gebruik van vage begrippen in het voorstel maakt het voor aanbieders en voor de bevoegde gerechtelijke of andere onafhankelijke administratieve autoriteit echter moeilijk om de wettelijke voorschriften van het voorstel op voorspelbare en niet-arbitraire wijze toe te passen. Het EDPB en de EDPS vrezen dat deze ruime en vage begrippen zullen leiden tot een gebrek aan rechtszekerheid en ook zullen leiden tot aanzienlijke verschillen in de concrete uitvoering van het voorstel in de hele Unie, afhankelijk van de interpretaties die zullen worden gegeven aan begrippen als 'waarschijnlijkheid' en 'in belangrijke mate' door gerechtelijke of andere onafhankelijke administratieve autoriteiten in de lidstaten. Een dergelijk resultaat zou niet aanvaardbaar zijn in het licht van het feit dat de bepalingen inzake opsporingsbevelen voor aanbieders van interpersoonlijke communicatiediensten 'beperkingen' vormen van het in artikel 5 van de e-privacyrichtlijn neergelegde beginsel van vertrouwelijkheid van communicatie en dat de duidelijkheid en voorspelbaarheid ervan derhalve van het grootste belang is om ervoor te zorgen dat deze beperkingen in de hele Unie op uniforme wijze worden toegepast.

4.5 Analyse van de noodzaak en evenredigheid van de beoogde maatregelen[33]

38. Zoals hierboven aangegeven, kunnen drie soorten opsporingsbevelen worden uitgevaardigd: opsporingsbevelen betreffende de verspreiding van bekend materiaal van seksueel misbruik van kinderen (artikel 7, lid 5, van het voorstel), opsporingsbevelen betreffende de verspreiding van nieuw materiaal van seksueel misbruik van kinderen (artikel 7, lid 6, van het voorstel) en opsporingsbevelen betreffende het benaderen van kinderen (artikel 7, lid 7, van het voorstel). Voor elk opsporingsbevel is normaal gesproken een andere technologie nodig voor de praktische uitvoering ervan. Bijgevolg hebben zij een verschillende mate van indringendheid en dus verschillende gevolgen voor het recht op privacy en de bescherming van persoonsgegevens.

39. Technologieën om bekend materiaal van seksueel misbruik van kinderen op te sporen, zijn meestal matchingtechnologieën in de zin dat zij gebruikmaken van een bestaande databank van bekend materiaal van seksueel misbruik van kinderen waarmee zij beelden kunnen vergelijken (waaronder stilstaande beelden van video's). Om matching mogelijk te maken, moeten de beelden die de aanbieder verwerkt en de beelden in de databank digitaal zijn gemaakt, meestal door ze om te zetten in hashwaarden. Dit soort hashingtechnologie heeft een geschat percentage fout-positieven van niet meer dan 1 op 50 miljard (d.w.z. 0,000000002 % percentage fout-positieven). [34]

40. Voor de opsporing van nieuw materiaal van seksueel misbruik van kinderen wordt doorgaans een andere soort technologie gebruikt, waaronder classificatoren en artificiële intelligentie (AI)[35]. De foutenpercentages daarvan zijn echter over het algemeen aanzienlijk hoger. Uit het effectbeoordelingsverslag blijkt bijvoorbeeld dat er technologieën zijn voor de opsporing van nieuw materiaal van seksueel misbruik van kinderen waarvan het nauwkeurigheidspercentage kan worden

---

[33] Zie ook 'The EDPS quick guide to need and proportionality', beschikbaar op: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

[34] Zie het werkdocument van de diensten van de Commissie bij het voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, SWD(2022) 209 final (hierna 'Effectbeoordelingsverslag' of 'SWD(2022) 209 final'), blz. 281, voetnoot 511.

[35] Effectbeoordelingsverslag, blz. 281.

vastgesteld op 99,9 % (d.w.z. een percentage fout-positieven van 0,1 %), maar met dat nauwkeurigheidspercentage zijn zij slechts in staat om 80 % van het totale materiaal van seksueel misbruik van kinderen in de relevante dataset te identificeren[36].

41. Wat de opsporing van het benaderen van kinderen in op tekst gebaseerde communicatie betreft, wordt in het effectbeoordelingsverslag uitgelegd dat dit doorgaans gebaseerd is op patroondetectie. In het effectbeoordelingsverslag wordt opgemerkt dat sommige van de bestaande technologieën voor het opsporen van grooming een nauwkeurigheidspercentage van 88 % hebben[37]. Volgens de Commissie betekent dit dat "van de 100 gesprekken die worden aangemerkt als een mogelijke criminele benadering van kinderen, er 12 bij nader inzien [volgens het voorstel door het EU-centrum] kunnen worden uitgesloten en niet aan de rechtshandhaving worden gemeld"[38]. Hoewel het voorstel, in tegenstelling tot de tijdelijke verordening, ook van toepassing zou zijn op audiocommunicatie, wordt in het effectbeoordelingsverslag niet nader ingegaan op de technologische oplossingen die kunnen worden gebruikt om grooming in een dergelijke omgeving op te sporen.

4.5.1 Doeltreffendheid van de opsporing

42. Noodzakelijkheid impliceert de noodzaak van een op feiten gebaseerde beoordeling van de doeltreffendheid van de beoogde maatregelen om het nagestreefde doel te bereiken en van de vraag of deze minder indringend zijn dan andere opties om hetzelfde doel te bereiken[39]. Een andere factor waarmee bij de beoordeling van de evenredigheid van een voorgestelde maatregel rekening moet worden gehouden, is de doeltreffendheid van bestaande maatregelen vergeleken met de maatregel die wordt voorgesteld[40]. Indien reeds maatregelen voor hetzelfde of een soortgelijk doel bestaan, moet de doeltreffendheid ervan worden beoordeeld in het kader van de evenredigheidsbeoordeling. Zonder een dergelijke beoordeling van de doeltreffendheid van bestaande maatregelen die hetzelfde of een soortgelijk doel nastreven, kan de evenredigheidstoets voor een nieuwe maatregel niet worden geacht naar behoren te zijn uitgevoerd.

43. De opsporing van materiaal van seksueel misbruik van kinderen of grooming door aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten kan bijdragen tot de algemene doelstelling om seksueel misbruik van kinderen en de onlineverspreiding van materiaal van seksueel misbruik van kinderen te voorkomen en te bestrijden. Tegelijkertijd roept de noodzaak om de doeltreffendheid van de in het voorstel vervatte maatregelen te beoordelen drie belangrijke vragen op:

- Kunnen de maatregelen om online seksueel misbruik van kinderen op te sporen, gemakkelijk worden omzeild?

[36] Ibid., blz. 282.
[37] Ibid., blz. 283.
[38] Voorstel, COM(2022) 209 final, blz. 14, voetnoot 32.
[39] EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit', 11 april 2017, blz. 5; EDPS, 'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (19 december 2019), blz. 8.
[40] EDPS, 'EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (19 december 2019), blz. 11.

- Wat is het effect van de opsporingsactiviteiten op het optreden van rechtshandhavingsautoriteiten[41]?
- Hoe vermindert het voorstel de rechtsonzekerheid?

44. Het is niet aan het EDPB en de EDPS om deze vragen in detail te beantwoorden. Het EDPB en de EDPS merken echter op dat deze vragen noch in het effectbeoordelingsverslag, noch in het voorstel volledig aan bod komen.

45. Wat betreft de mogelijkheid om opsporing van materiaal van seksueel misbruik van kinderen te omzeilen, moet worden opgemerkt dat er momenteel geen technologische oplossing voorhanden lijkt te zijn om materiaal van seksueel misbruik van kinderen op te sporen dat in versleutelde vorm wordt gedeeld. Daarom kan elke opsporingsactiviteit, ook scannen aan de clientzijde bedoeld om eind-tot-eindversleuteling door de aanbieder te omzeilen[42], gemakkelijk worden omzeild door de inhoud met behulp van een afzonderlijke applicatie te versleutelen voordat deze wordt verzonden of geüpload. De opsporingsmaatregelen waarin het voorstel voorziet, kunnen dus een geringer effect hebben op de verspreiding van materiaal van seksueel misbruik van kinderen op het internet dan men zou kunnen hopen.

46. Voorts verwacht de Commissie een toename van het aantal meldingen van seksueel misbruik van kinderen aan rechtshandhavingsautoriteiten met de vaststelling van de bij het voorstel ingevoerde opsporingsverplichtingen[43]. Noch in het voorstel, noch in het effectbeoordelingsverslag wordt echter uitgelegd hoe hierbij de tekortkomingen van de huidige stand van zaken zullen worden aangepakt. Gezien de beperkte middelen waarover rechtshandhavingsautoriteiten beschikken, lijkt het nodig om beter te begrijpen of een toename van het aantal meldingen een betekenisvolle impact zou hebben op rechtshandhavingsactiviteiten ter bestrijding van seksueel misbruik van kinderen. In ieder geval willen het EDPB en de EDPS benadrukken dat dergelijke meldingen tijdig moeten worden beoordeeld om ervoor te zorgen dat zo snel mogelijk een beslissing wordt genomen over de strafrechtelijke relevantie van het gerapporteerde materiaal en om de bewaring van irrelevante gegevens zoveel mogelijk te beperken.

4.5.2 Geen minder indringende maatregelen

47. Ervan uitgaande dat de door de Commissie beoogde positieve effecten van de opsporing van materiaal van seksueel misbruik van kinderen en van grooming kunnen worden gerealiseerd, moet de opsporing de minst indringende maatregel van even doeltreffende maatregelen zijn. In artikel 4 van het voorstel is bepaald dat aanbieders als eerste stap moeten overwegen risicobeperkende maatregelen vast te stellen om het risico te beperken dat hun dienst wordt gebruikt voor online seksueel misbruik van kinderen onder de drempel die de uitvaardiging van een opsporingsbevel rechtvaardigt. Indien er risicobeperkende maatregelen zijn die kunnen leiden tot een aanzienlijke vermindering van de mate van grooming of hoeveelheid materiaal van seksueel misbruik van kinderen die binnen de betrokken dienst wordt uitgewisseld, zouden deze maatregelen vaak minder indringende maatregelen vormen

[41] Volgens het effectbeoordelingsverslag, bijlage II, blz. 132, heeft 85,71 % van de respondenten van de rechtshandhavingsenquête zijn bezorgdheid geuit over de toegenomen hoeveelheid materiaal van seksueel misbruik van kinderen in de afgelopen tien jaar en het gebrek aan middelen (d.w.z. personele en technische).
[42] Zie ook punt 4.10 hieronder.
[43] Zie onder meer het Effectbeoordelingsverslag, bijlage 3, SWD(2022) 209 final, blz. 176.

dan een opsporingsbevel[44]. Indien de betrokken aanbieder nalaat dergelijke maatregelen op vrijwillige basis vast te stellen, moet het voor de bevoegde onafhankelijke administratieve of gerechtelijke autoriteit derhalve mogelijk zijn om de uitvoering van risicobeperkende maatregelen verplicht en afdwingbaar te maken in plaats van een opsporingsbevel uit te vaardigen. Volgens het EDPB en de EDPS volstaat het feit dat de coördinerende autoriteit op grond van artikel 5, lid 4, van het voorstel "vereist" dat de aanbieder de risicobeperkende maatregelen invoert, toetst, stopzet of uitbreidt, niet omdat een dergelijke vereiste niet onafhankelijk zou kunnen worden afgedwongen; het niet tegemoetkomen aan deze eis zou alleen worden "bestraft" door een opsporingsbevel te gelasten.

48. Daarom zijn het EDPB en de EDPS van mening dat de coördinerende autoriteit of de bevoegde onafhankelijke administratieve of gerechtelijke autoriteit uitdrukkelijk de bevoegdheid moet krijgen om minder indringende risicobeperkende maatregelen op te leggen alvorens of in plaats van een opsporingsbevel uit te vaardigen.

4.5.3 Evenredigheid in strikte zin

49. Wil een maatregel in overeenstemming zijn met het in artikel 52, lid 1, van het Handvest neergelegde evenredigheidsbeginsel, dan mogen de voordelen van de maatregel niet opwegen tegen de nadelen die de maatregel voor de uitoefening van de grondrechten meebrengt. Daarom beperkt het evenredigheidsbeginsel "de autoriteiten in de uitoefening van hun bevoegdheden door te eisen dat een evenwicht wordt gevonden tussen de gebruikte middelen en het beoogde doel (of het beoogde resultaat)"[45].

50. Om het effect van een maatregel op de grondrechten op privacy en op de bescherming van persoonsgegevens te kunnen beoordelen, is het van bijzonder belang om de volgende elementen nauwkeurig te bepalen: [46]

- de **reikwijdte van de maatregel**, met inbegrip van het aantal getroffen personen en de vraag of sprake is van "bijkomstige indringendheid" (namelijk inmenging in de privacy van andere personen dan de personen op wie de maatregel betrekking heeft);
- de **omvang van de maatregel**, met inbegrip van de hoeveelheid verzamelde informatie en voor hoe lang, en of de onderzochte maatregel het verzamelen en verwerken van bijzondere categorieën gegevens vereist;
- de **mate van indringendheid**, waarbij rekening wordt gehouden met: de aard van de activiteit waarop de maatregel betrekking heeft (ongeacht of deze betrekking heeft op activiteiten die al dan niet onder de geheimhoudingsplicht vallen, de relatie tussen advocaat en cliënt, of medische activiteiten), de context, of het gaat om profilering van de betrokken personen of

[44] Zo kunnen maatregelen zoals het blokkeren aan de clientzijde van de versturing van materiaal van seksueel misbruik van kinderen door te voorkomen dat inhoud van de elektronische communicatie wordt geüpload en verzonden, worden overwogen, aangezien zij in bepaalde gevallen de verspreiding van bekend materiaal van seksueel misbruik van kinderen kunnen helpen voorkomen.
[45] Zie zaak C-343/09, *Afton Chemical*, punt 45; gevoegde zaken C-92/09 en C-93/09, *Volker und Markus Schecke en Hartmut Eifert*, punt 74; zaken C-581/10 en C-629/10, *Nelson en anderen*, punt 71; zaak C-283/11, *Sky Österreich*, punt 50; en zaak C-101/12, *Schaible*, punt 29. Zie verder EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit' (11 april 2017).
[46] EDPS, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (19 december 2019), blz. 23.

niet, en of de verwerking het gebruik van een (gedeeltelijk of volledig) geautomatiseerd besluitvormingssysteem met een "foutmarge" inhoudt;

- of het al dan niet om **kwetsbare personen** gaat;
- of de maatregel ook **andere grondrechten** aantast (bijvoorbeeld het recht op vrijheid van meningsuiting, zoals in de zaken Digital Rights Ireland en Seitlinger en anderen en Tele2 Sverige en Watson)[47].

51. In dit verband is het ook van belang op te merken dat het effect voor de betrokken persoon gering kan zijn, maar collectief/voor de samenleving als geheel niettemin significant of zeer significant kan zijn[48].

52. In alle drie de soorten opsporingsbevelen (opsporing van bekend materiaal van seksueel misbruik van kinderen, nieuw materiaal van seksueel misbruik van kinderen en grooming) zijn de momenteel beschikbare technologieën afhankelijk van de geautomatiseerde verwerking van inhoudsgegevens van alle betrokken gebruikers. De technologieën die worden gebruikt om de inhoud te analyseren, zijn vaak complex, waarbij doorgaans gebruik wordt gemaakt van AI. Daardoor is het gedrag van deze technologie mogelijk niet volledig begrijpelijk voor de gebruiker van de dienst. Bovendien staan de momenteel beschikbare technologieën, met name die voor het opsporen van nieuw materiaal van seksueel misbruik van kinderen of grooming, bekend om hun relatief hoge foutenpercentages[49]. Bovendien bestaat het risico dat zij overeenkomstig artikel 12, lid 1, en artikel 48, lid 1, van het voorstel op grond van een opsporing van 'potentieel' materiaal van seksueel misbruik van kinderen aan het EU-centrum worden gemeld.

53. Bovendien kunnen de algemene voorwaarden voor de afgifte van een opsporingsbevel in het kader van het voorstel, namelijk toegepast op een volledige dienst en niet alleen op geselecteerde communicatie[50], duur tot 24 maanden voor bekend of nieuw materiaal van seksueel misbruik van kinderen en maximaal 12 maanden voor grooming[51] enz., in de praktijk tot een zeer ruime reikwijdte van het opsporingsbevel leiden. Als gevolg daarvan zou de controle in feite algemeen en willekeurig van aard zijn en in de praktijk niet doelgericht zijn.

54. In het licht van het bovenstaande zijn het EDPB en de EDPS ook bezorgd over de mogelijke afschrikkende effecten voor de uitoefening van de vrijheid van meningsuiting. Het EDPB en de EDPS herinneren eraan dat een dergelijk afschrikkend effect waarschijnlijker wordt geacht naarmate de wet minder duidelijk is.

55. Bij gebrek aan de specificiteit, nauwkeurigheid en duidelijkheid die nodig zijn om te voldoen aan het vereiste van rechtszekerheid[52], en gezien de ruime reikwijdte, namelijk alle aanbieders van relevante diensten van de informatiemaatschappij die dergelijke diensten in de Unie aanbieden[53], waarborgt het voorstel niet dat daadwerkelijk alleen een gerichte aanpak van materiaal van seksueel misbruik

---

[47] Zie ook advies 7/2020 van de EDPS over het voorstel voor tijdelijke afwijkingen van Richtlijn 2002/58/EG ten behoeve van de bestrijding van online seksueel misbruik van kinderen (10 november 2020), blz. 9 en volgende.
[48] EDPS, 'Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data' (19 december 2019), blz. 20.
[49] Zie details hierboven, punt 4.5, en hieronder, onder 4.8.2.
[50] Zie artikel 7, lid 1, van het voorstel.
[51] Zie artikel 7, lid 9, derde alinea, van het voorstel.
[52] Zie HvJ-EU, zaak C-197/96, Commissie van de Europese Gemeenschappen tegen Franse Republiek, punt 15.
[53] Zie artikel 1, lid 2, van het voorstel.

van kinderen en grooming plaatsvindt. Daarom zijn het EDPB en de EDPS van mening dat het voorstel in de praktijk de basis zou kunnen vormen voor het de facto algemeen en willekeurig scannen van de inhoud van vrijwel alle soorten elektronische communicatie van alle gebruikers in de EU/EER. Als gevolg daarvan kan de wetgeving ertoe leiden dat mensen ervan afzien legale inhoud te delen uit vrees dat zij daardoor het doelwit worden.

56. Niettemin erkennen het EDPB en de EDPS dat verschillende maatregelen ter bestrijding van seksueel misbruik van kinderen op het internet verschillende niveaus van indringendheid kunnen inhouden. Om te beginnen merken het EDPB en de EDPS op dat de geautomatiseerde analyse van spraak of tekst met het oog op het identificeren van mogelijke gevallen van het benaderen van kinderen waarschijnlijk een significantere mate van inmenging vormt dan de matching van beelden of video's op basis van eerder bevestigde gevallen van materiaal van seksueel misbruik van kinderen met het oog op het opsporen van de verspreiding van zulk materiaal. Voorts moet een onderscheid worden gemaakt tussen de opsporing van "bekend materiaal van seksueel misbruik van kinderen" en "nieuw materiaal van seksueel misbruik van kinderen". Bovendien moet verder onderscheid worden gemaakt in het effect tussen de maatregelen voor aanbieders van hostingdiensten en de maatregelen die worden opgelegd aan aanbieders van interpersoonlijke communicatiediensten.

4.5.4 Opsporing van bekend materiaal van seksueel misbruik van kinderen

57. Hoewel het voorstel volgens overweging 4 "technologieneutraal" zou zijn, zullen zowel de doeltreffendheid van de voorgestelde opsporingsmaatregelen als het effect ervan op individuen sterk afhangen van de keuze van de toegepaste technologie en van de geselecteerde indicatoren. Dit feit wordt door de Commissie erkend in het effectbeoordelingsverslag, bijlage 8[54], en bevestigd door andere studies, zoals de gerichte vervangende effectbeoordeling van de Onderzoeksdienst van het Europees Parlement over het voorstel van de Commissie inzake de tijdelijke afwijking van de e-privacyrichtlijn ten behoeve van de bestrijding van online seksueel misbruik van kinderen van februari 2021[55].

58. Artikel 10 van het voorstel bevat een aantal voorschriften voor de technologieën die voor opsporingsdoeleinden moeten worden gebruikt, met name wat betreft hun doeltreffendheid, betrouwbaarheid en minst indringende karakter wat betreft het effect op de rechten van gebruikers op eerbiediging van het privéleven en het familie- en gezinsleven, met inbegrip van de vertrouwelijkheid van communicatie, en op de bescherming van persoonsgegevens.

59. In dit verband merken het EDPB en de EDPS op dat momenteel de enige technologieën die in het algemeen aan deze normen lijken te voldoen, de technologieën zijn die worden gebruikt om bekend materiaal van seksueel misbruik van kinderen op te sporen, namelijk technologieën die gebaseerd zijn op een hashdatabank als referentie.

4.5.5 Opsporing van voorheen onbekend materiaal van seksueel misbruik van kinderen

60. De beoordeling van de maatregelen die gericht zijn op de opsporing van voorheen onbekend (nieuw) materiaal van seksueel misbruik van kinderen leidt tot verschillende conclusies over de

[54] Zie informatie over de percentages fout-positieven in het effectbeoordelingsverslag, bijlage 8, blz. 279 en volgende.
[55] Zie het voorstel van de Commissie betreffende de tijdelijke afwijking van de e-privacyrichtlijn ten behoeve van de bestrijding van online seksueel misbruik van kinderen: gerichte vervangende effectbeoordeling (Onderzoeksdienst van het Europees Parlement, februari 2021), blz. 14 en volgende.

doeltreffendheid, betrouwbaarheid en beperking van het effect op de grondrechten op privacy en gegevensbescherming.

61. Ten eerste omvatten de technologieën die momenteel worden gebruikt voor de opsporing van voorheen onbekend materiaal van seksueel misbruik van kinderen, zoals uiteengezet in het effectbeoordelingsverslag bij het voorstel, classificatoren en AI. Een classificator is elk algoritme dat gegevens door middel van patroonherkenning in gelabelde klassen of categorieën informatie onderverdeelt [56]. Deze technologieën hebben dus verschillende resultaten en effecten qua nauwkeurigheid, doeltreffendheid en mate van indringendheid. Tegelijkertijd zijn zij ook gevoeliger voor fouten.

62. De technieken die worden gebruikt om voorheen onbekend materiaal van seksueel misbruik van kinderen op te sporen, zijn vergelijkbaar met die welke worden gebruikt om het benaderen van kinderen op te sporen, aangezien beide niet gebaseerd zijn op eenvoudige matchingtechnologieën, maar op voorspellende modellen die gebruikmaken van AI-technologieën. Het EDPB en de EDPS zijn van mening dat er een grote mate van voorzichtigheid moet worden betracht bij het opsporen van voorheen onbekend materiaal van seksueel misbruik van kinderen; een fout door het systeem zou immers ernstige gevolgen hebben voor betrokkenen, die automatisch zouden worden gemarkeerd als personen die mogelijk een zeer ernstig misdrijf hebben gepleegd wiens persoonsgegevens en details van hun communicatie zouden worden gemeld.

63. Ten tweede verschaffen de in de literatuur vermelde prestatie-indicatoren, waarvan sommige in het effectbeoordelingsverslag bij het voorstel worden benadrukt [57], zeer weinig informatie over de voorwaarden die zijn gebruikt voor de berekening ervan en over de geschiktheid ervan voor reële omstandigheden; dit betekent dat hun reële prestaties aanzienlijk lager kunnen zijn dan verwacht, wat leidt tot minder nauwkeurigheid en een hoger percentage 'fout-positieven'.

64. Ten derde moeten prestatie-indicatoren in aanmerking worden genomen in de specifieke context van het gebruik van de relevante opsporingsinstrumenten en een volledig inzicht verschaffen in het gedrag ervan. In het geval van het gebruik van algoritmen op basis van kunstmatige intelligentie op beelden of tekst is goed gedocumenteerd dat vertekening en discriminatie kunnen optreden als gevolg van het gebrek aan representativiteit van bepaalde bevolkingsgroepen in de gegevens die worden gebruikt om het algoritme te trainen. Deze vertekeningen moeten worden vastgesteld en gemeten en tot een aanvaardbaar niveau worden teruggebracht, zodat de opsporingssystemen de samenleving als geheel echt ten goede komen.

65. Hoewel een studie is verricht naar de technologieën die voor opsporing worden gebruikt [58], zijn het EDPB en de EDPS van mening dat verdere analyse nodig is om de betrouwbaarheid van de bestaande instrumenten te beoordelen. Bij deze analyse moet gebruik worden gemaakt van uitgebreide prestatie-indicatoren en moet het effect van potentiële fouten in reële omstandigheden voor alle betrokkenen waarop het voorstel betrekking heeft, worden beoordeeld.

66. Zoals hierboven opgemerkt, hebben het EDPB en de EDPS ernstige twijfels over de mate waarin de procedurele waarborgen van artikel 7, lid 6, van het voorstel volstaan om deze risico's te compenseren. Bovendien merken zij, zoals eerder aangegeven, op dat het voorstel nogal abstracte en vage termen gebruikt om het aanvaardbare risiconiveau te beschrijven (zoals 'in belangrijke mate').

---

[56] Effectbeoordelingsverslag, bijlage 8, blz. 281.
[57] Effectbeoordelingsverslag, bijlage 8, blz. 281-283.
[58] Effectbeoordelingsverslag, blz. 279 en volgende.

67. Het EDPB en de EDPS vrezen dat deze ruime en vage begrippen zullen leiden tot een gebrek aan rechtszekerheid en ook zullen leiden tot grote verschillen in de concrete uitvoering van het voorstel in de hele Unie, afhankelijk van de interpretaties die zullen worden gegeven aan begrippen als 'waarschijnlijkheid' en 'in belangrijke mate' door gerechtelijke of andere onafhankelijke administratieve autoriteiten in de lidstaten. Dit is ook zorgwekkend in het licht van het feit dat de bepalingen inzake opsporingsbevelen 'beperkingen' vormen voor het in artikel 5 van de e-privacyrichtlijn neergelegde vertrouwelijkheidsbeginsel. Daarom moet de duidelijkheid en voorspelbaarheid ervan in de voorgestelde verordening worden verbeterd.

4.5.6 Opsporing van het benaderen van kinderen (grooming)

68. Het EDPB en de EDPS merken op dat de voorgestelde maatregelen betreffende de opsporing van het benaderen van kinderen (grooming), die geautomatiseerde analyse van spraak of tekst meebrengen, waarschijnlijk de meest significante vorm van inmenging vormen in de rechten van gebruikers op eerbiediging van het privéleven en het familie- en gezinsleven, met inbegrip van de vertrouwelijkheid van communicatie, en op de bescherming van persoonsgegevens.

69. Hoewel de opsporing van bekend en zelfs nieuw materiaal van seksueel misbruik van kinderen kan worden beperkt tot de analyse van beelden en video's, zou grooming per definitie ook betrekking hebben op alle op tekst gebaseerde (en mogelijk audio-) communicatie die binnen de reikwijdte van een opsporingsbevel valt. Daardoor is de intensiteit van de inmenging in de vertrouwelijkheid van de betrokken communicatie veel groter.

70. Het EDPB en de EDPS zijn van mening dat *de facto* algemene en willekeurige geautomatiseerde analyse van op tekst gebaseerde communicatie die via interpersoonlijke communicatiediensten wordt verstuurd om het mogelijk benaderen van kinderen vast te stellen, niet voldoet aan de vereisten van noodzakelijkheid en evenredigheid. Hoewel de gebruikte technologie beperkt is tot het gebruik van indicatoren, zijn het EDPB en de EDPS van mening dat de toepassing van een dergelijke algemene en willekeurige analyse buitensporig is en zelfs de kern van het in artikel 7 van het Handvest verankerde grondrecht op privacy kan aantasten.

71. Zoals reeds vermeld, kan het ontbreken van materiële waarborgen in het kader van de maatregelen voor het opsporen van het benaderen van kinderen niet alleen door procedurele waarborgen worden gecompenseerd. Bovendien is het probleem van het gebrek aan voldoende juridische duidelijkheid en rechtszekerheid (zoals het gebruik van vage juridische bewoordingen als 'in belangrijk mate') nog ernstiger in het geval van geautomatiseerde analyse van op tekst gebaseerde persoonlijke communicatie, vergeleken met de vergelijking van foto's op basis van hashingtechnologie.

72. Voorts zijn het EDPB en de EDPS van mening dat het 'remmend effect' op de vrijheid van meningsuiting met name significant is wanneer tekst- (of audio-) communicatie van personen op grote schaal wordt gescand en geanalyseerd. Het EDPB en de EDPS herinneren eraan dat een dergelijk remmend effect des te groter is naarmate de wet minder duidelijk is.

73. Bovendien is (zoals aangegeven in het effectbeoordelingsverslag [59] en in de studie van de Onderzoeksdienst van het Europees Parlement[60]) de nauwkeurigheidsgraad van technologieën voor de opsporing van op tekst gebaseerde grooming veel lager dan de nauwkeurigheidsgraad van

[59] Effectbeoordelingsverslag, bijlage 8, blz. 281-283.
[60] Blz. 15-18.

technologieën voor de opsporing van bekend materiaal van seksueel misbruik van kinderen[61]. Technieken voor de opsporing van grooming zijn ontworpen om waarschijnlijkheidsbeoordelingen te analyseren en toe te kennen aan elk aspect van het gesprek; daarom beschouwen het EDPB en de EDPS deze ook als foutgevoelig en kwetsbaar voor misbruik.

4.5.7 Conclusie over de noodzakelijkheid en evenredigheid van de beoogde maatregelen

74. Wat de noodzakelijkheid en evenredigheid van de beoogde opsporingsmaatregelen betreft, zijn het EDPB en de EDPS met name bezorgd over de voorgenomen maatregelen voor de opsporing van onbekend materiaal van seksueel misbruik van kinderen en het benaderen van kinderen (grooming), gezien hun indringendheid vanwege het mogelijk verlenen van toegang tot inhoud van communicatie op algemene basis, hun probabilistische aard en de foutenpercentages die met dergelijke technologieën verband houden.

75. Bovendien kan uit de rechtspraak van het HvJ-EU worden afgeleid dat maatregelen die de overheidsinstanties algemene toegang verlenen tot de inhoud van communicatie, eerder de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten kunnen aantasten. Deze overwegingen zijn specifiek relevant met betrekking tot de in het voorstel beoogde maatregelen voor het opsporen van het benaderen van kinderen.

76. Hoe dan ook zijn het EDPB en de EDPS van mening dat de inmenging die met name wordt veroorzaakt door de maatregelen voor het opsporen van het benaderen van kinderen, verder gaat dan strikt noodzakelijk en evenredig is. Deze maatregelen moeten daarom uit het voorstel worden gehaald.

4.6 Meldingsplichten

77. Het EDPB en de EDPS bevelen aan om de lijst van specifieke meldingsvoorschriften in artikel 13 van het voorstel aan te vullen met het voorschrift om in de melding informatie op te nemen over de specifieke technologie die de aanbieder in staat heeft gesteld kennis te nemen van de relevante onrechtmatige inhoud, indien de aanbieder kennis kreeg van het mogelijke seksueel misbruik van kinderen als gevolg van maatregelen die zijn genomen om een overeenkomstig artikel 7 van het voorstel uitgevaardigd opsporingsbevel uit te voeren.

4.7 Verwijderings- en blokkeringsverplichtingen

78. Een van de maatregelen waarin het voorstel voorziet om de risico's van de verspreiding van materiaal van seksueel misbruik van kinderen te beperken, is de uitvaardiging van verwijderings- en blokkeringsbevelen die aanbieders zouden verplichten de toegang tot onlinemateriaal van seksueel misbruik van kinderen te verwijderen, ontoegankelijk te maken of te blokkeren[62].

79. Hoewel het effect van verwijderingsbevelen op de gegevensbescherming en de privacy van communicatie relatief beperkt is, herinneren het EDPB en de EDPS er in het algemeen aan dat het overkoepelende beginsel dat dergelijke maatregelen zo doelgericht mogelijk moeten zijn, in acht moet worden genomen.

80. Tegelijkertijd vestigen het EDPB en de EDPS de aandacht op het feit dat aanbieders van internettoegangsdiensten alleen toegang hebben tot de precieze URL van inhoud als deze inhoud

[61] Zie punt 40 hierboven.
[62] Voorstel, artikelen 14 en 16.

in duidelijke tekst beschikbaar wordt gesteld. Telkens wanneer inhoud via https toegankelijk wordt gemaakt, heeft de aanbieder van internettoegangsdiensten geen toegang tot de precieze URL, tenzij de versleuteling van de communicatie wordt gekraakt. Daarom hebben het EDPB en de EDPS twijfels over de doeltreffendheid van blokkeringsmaatregelen en zijn zij van mening dat het onevenredig zou zijn om aanbieders van internettoegangsdiensten te verplichten onlinecommunicatie te ontsleutelen om het betreffende materiaal van seksueel misbruik van kinderen te blokkeren.

81. Bovendien en meer in het algemeen moet worden opgemerkt dat het blokkeren (of uitschakelen) van de toegang tot een digitaal element een handeling is die plaatsvindt op netwerkniveau en dat de uitvoering ervan ondoeltreffend kan blijken in het geval van meerdere (mogelijk vergelijkbare en niet identieke) kopieën van hetzelfde element. Bovendien kan een dergelijke handeling onevenredig blijken als de blokkering gevolgen heeft voor andere, niet illegale, digitale elementen wanneer deze worden opgeslagen op dezelfde server die ontoegankelijk wordt gemaakt door middel van netwerkcommando's (zoals IP-adres- of DNS-blacklisting). Bovendien zijn niet alle benaderingen van blokkering op netwerkniveau even doeltreffend en sommige kunnen gemakkelijk worden omzeild met vrij eenvoudige technische vaardigheden.

82. Ten slotte moeten de bevoegdheden van de coördinerende autoriteiten met betrekking tot het uitvaardigen van blokkeringsbevelen in de voorgestelde verordening worden verduidelijkt. Aan de hand van de huidige formulering van artikel 16, lid 1, en artikel 17, lid 1, is bijvoorbeeld niet duidelijk of de coördinerende autoriteiten bevoegd zijn om blokkeringsbevelen uit te vaardigen of om alleen om de uitvaardiging van blokkeringsbevelen te verzoeken[63].

4.8 Relevante technologieën en waarborgen

4.8.1 Gegevensbescherming door ontwerp en door standaardinstellingen

83. De voorschriften van het voorstel die van toepassing zijn op de technologieën die moeten worden toegepast voor de opsporing van materiaal van seksueel misbruik van kinderen en het benaderen van kinderen, lijken niet streng genoeg. Het EDPB en de EDPS hebben met name opgemerkt dat het voorstel, in tegenstelling tot de overeenkomstige bepalingen in de tijdelijke verordening[64], geen uitdrukkelijke verwijzing bevat naar het beginsel van gegevensbescherming door ontwerp en door standaardinstellingen, en niet bepaalt dat technologieën die worden gebruikt om tekst in communicatie te scannen, niet de essentie van de inhoud van de communicatie mogen afleiden. In artikel 10, lid 3, punt b, van het voorstel wordt alleen bepaald dat de technologieën geen andere informatie "uit" de desbetreffende communicatie mogen "halen" dan de informatie die strikt noodzakelijk is voor het opsporen. Deze norm lijkt echter niet streng genoeg, aangezien het mogelijk zou kunnen zijn om andere informatie uit de essentie van de inhoud van communicatie *af te leiden* zonder deze als zodanig *eruit te halen*.

---

[63] Artikel 16, lid 1, van het voorstel luidt als volgt: "De coördinerende autoriteit van vestiging is bevoegd om de bevoegde gerechtelijke autoriteit van de lidstaat die haar heeft aangewezen of een onafhankelijke administratieve autoriteit van die lidstaat te verzoeken een blokkeringsbevel uit te vaardigen […]", terwijl in artikel 17, lid 1, het volgende staat: "De coördinerende autoriteit van vestiging vaardigt de in artikel 16 bedoelde blokkeringsbevelen uit […]" (onderstreping toegevoegd).

[64] Tijdelijke verordening, artikel 3, lid 1, punt b.

84. Bijgevolg bevelen het EDPB en de EDPS aan om in het voorstel een overweging op te nemen waarin wordt bepaald dat het in artikel 25 van Verordening (EU) 2016/679 neergelegde beginsel van gegevensbescherming door ontwerp en door standaardinstellingen van toepassing is op de technologieën die bij wet onder artikel 10 van het voorstel vallen en derhalve niet in de wetstekst hoefde te worden herhaald. Bovendien moet artikel 10, lid 3, punt b, worden gewijzigd om ervoor te zorgen dat andere informatie niet alleen niet eruit wordt gehaald, maar ook niet wordt afgeleid, zoals momenteel is bepaald in artikel 3, lid 1, punt b, van de tijdelijke verordening.

4.8.2 Betrouwbaarheid van de technologieën

85. In het voorstel wordt ervan uitgegaan dat dienstenaanbieders verschillende soorten technologische oplossingen kunnen gebruiken om opsporingsbevelen uit te voeren. Het voorstel gaat er met name van uit dat artificiële-intelligentiesystemen beschikbaar zijn en werken voor de opsporing van onbekend materiaal van seksueel misbruik van kinderen en voor de opsporing van het benaderen van kinderen [65], en door sommige coördinerende autoriteiten als geavanceerd kunnen worden beschouwd. Hoewel de doeltreffendheid van het voorstel afhangt van de betrouwbaarheid van deze technologische oplossingen, is er zeer weinig informatie beschikbaar over het algemene en systematische gebruik van deze technieken, waarmee met grote zorgvuldigheid moet worden omgegaan.

86. Hoewel het EDPB en de EDPS er bij hun evenredigheidsbeoordeling gebruik van moesten maken wegens een gebrek aan alternatieven, moet bovendien worden opgemerkt dat de prestatie-indicatoren van opsporingstechnologieën die in het effectbeoordelingsverslag bij het voorstel worden genoemd, zeer weinig informatie verschaffen over de wijze waarop zij zijn beoordeeld en of zij de reële prestaties van de desbetreffende technologieën weerspiegelen. Er is geen informatie voorhanden over de tests of benchmarks die door de technologieleveranciers worden gebruikt om die prestaties te meten. Zonder dergelijke informatie is het niet mogelijk de tests te reproduceren of de geldigheid van de prestatieverklaringen te beoordelen. In dit verband moet worden opgemerkt dat de prestatie-indicatoren, hoewel zij kunnen worden geïnterpreteerd als een aanwijzing dat sommige opsporingsinstrumenten een hoge mate van nauwkeurigheid hebben (zo zijn bepaalde instrumenten voor de opsporing van grooming 88 % nauwkeurig[66]), moeten worden beoordeeld in het licht van het beoogde praktische gebruik van de opsporingsinstrumenten en de ernst van de risico's die een onjuiste beoordeling van bepaald materiaal voor de betrokkenen met zich mee zou brengen. Bovendien zijn het EDPB en de EDPS van mening dat, met een dergelijke verwerking met een hoog risico, het foutenpercentage van 12 % een hoog risico inhoudt voor betrokkenen die aan fout-positieven zijn blootgesteld, zelfs wanneer er waarborgen bestaan ter voorkoming van valse meldingen aan rechtshandhavingsinstanties. Het is hoogst onwaarschijnlijk dat dienstenaanbieders voldoende middelen kunnen inzetten om een dergelijk percentage fout-positieven te evalueren.

87. Zoals eerder vermeld[67], moeten prestatie-indicatoren een volledig inzicht verschaffen in het gedrag van de opsporingsinstrumenten. In het geval van het gebruik van algoritmen op basis van kunstmatige intelligentie op beelden of tekst is goed gedocumenteerd dat vertekening en discriminatie kunnen optreden als gevolg van het gebrek aan representativiteit van bepaalde bevolkingsgroepen in de gegevens die worden gebruikt om het algoritme te trainen. Deze vertekeningen moeten worden

[65] Zie het effectbeoordelingsverslag, blz. 281-282.
[66] Ibid., blz. 283.
[67] Zie de punten 63-64 hierboven.

vastgesteld en gemeten en tot een aanvaardbaar niveau worden teruggebracht, zodat de opsporingssystemen de samenleving als geheel echt ten goede komen.

88. Hoewel een studie is verricht naar de technologieën die voor opsporing worden gebruikt[68], zijn het EDPB en de EDPS van mening dat verdere analyse nodig is om de betrouwbaarheid van de bestaande instrumenten in reële praktijkvoorbeelden onafhankelijk te beoordelen. Bij deze analyse moet gebruik worden gemaakt van uitgebreide prestatie-indicatoren en moet het effect van potentiële fouten in reële omstandigheden voor alle betrokkenen waarop het voorstel betrekking heeft, worden beoordeeld. Aangezien deze technologieën de basis vormen voor het voorstel, zijn het EDPB en de EDPS van mening dat deze analyse van cruciaal belang is voor de beoordeling van de adequaatheid van het voorstel.

89. Het EDPB en de EDPS merken ook op dat het voorstel geen voorschriften voor specifieke technologieën bevat, of het nu gaat om de foutenpercentages, het gebruik van classificatoren en de validering daarvan, of andere beperkingen. Hierdoor wordt het aan de praktijk overgelaten om dergelijke criteria te ontwikkelen bij de beoordeling van de evenredigheid van het gebruik van een specifieke technologie, wat verder bijdraagt tot het gebrek aan nauwkeurigheid en duidelijkheid.

90. Gezien het belang van de gevolgen voor de betrokkenen in geval van fout-positieven, zijn het EDPB en de EDPS van mening dat de percentages fout-positieven tot een minimum moeten worden beperkt. Bovendien moeten die systemen naar hun mening worden ontworpen met inachtneming van het feit dat het overgrote merendeel van de elektronische communicatie geen materiaal van seksueel misbruik van kinderen of van het benaderen van kinderen bevat, en dat zelfs een zeer laag percentage fout-positieven een zeer groot aantal fout-positieven zal inhouden, gezien de hoeveelheid gegevens die aan opsporing zullen worden onderworpen. Meer in het algemeen maken het EDPB en de EDPS zich ook zorgen over het feit dat de prestaties van de in het effectbeoordelingsverslag vermelde beschikbare instrumenten geen nauwkeurige en vergelijkbare indicatoren bevatten met betrekking tot percentages fout-positieven en fout-negatieven. Zij zijn van mening dat voor die technologieën vergelijkbare en zinvolle prestatie-indicatoren moeten worden vastgesteld alvorens ze als beschikbaar en efficiënt te beschouwen.

4.8.3 Scannen van audiocommunicatie

91. In tegenstelling tot de tijdelijke verordening [69] wordt in het voorstel het scannen van audiocommunicatie in het kader van de opsporing van grooming niet van het toepassingsgebied uitgesloten[70]. Het EDPB en de EDPS zijn van mening dat het scannen van audiocommunicatie bijzonder indringend is, aangezien daarvoor doorgaans actieve, doorlopende en 'live' onderschepping is vereist. Bovendien geniet in sommige lidstaten de privacy van het gesproken woord bijzondere bescherming[71]. Aangezien in beginsel alle inhoud van audiocommunicatie moet worden geanalyseerd, kan deze maatregel bovendien de wezenlijke inhoud van de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten aantasten. Deze opsporingsmethode moet dus buiten de reikwijdte van de opsporingsverplichtingen van de voorgestelde verordening blijven, zowel met betrekking tot spraakberichten als livecommunicatie, temeer daar in het effectbeoordelingsverslag bij het voorstel

[68] Zie het effectbeoordelingsverslag, blz. 279 en volgende.
[69] Zie tijdelijke verordening, artikel 1, lid 2.
[70] Zie voorstel, artikel 1.
[71] Zie bijvoorbeeld het Duitse wetboek van strafrecht, artikel 201.

geen specifieke risico's of veranderingen in het scala aan dreigingen werden vastgesteld die het gebruik ervan zouden rechtvaardigen[72].

4.8.4 Leeftijdsverificatie

92. Het voorstel moedigt aanbieders aan gebruik te maken van maatregelen voor leeftijdsverificatie en leeftijdsbepaling om minderjarige gebruikers van hun diensten te identificeren[73]. In dit verband merken het EDPB en de EDPS op dat er momenteel geen technologische oplossing voorhanden is waarmee de leeftijd van een gebruiker in een onlinecontext met zekerheid kan worden bepaald, zonder te vertrouwen op een officiële digitale identiteit, die in dit stadium niet voor elke Europese burger beschikbaar is[74]. Daarom zou het beoogde gebruik van maatregelen voor leeftijdsverificatie in het voorstel kunnen leiden tot de uitsluiting van bijvoorbeeld jong uitziende volwassenen van de toegang tot onlinediensten of tot de toepassing van zeer indringende instrumenten voor leeftijdsverificatie, wat het legitieme gebruik van de betrokken diensten zou kunnen belemmeren of ontmoedigen.

93. Hoewel in overweging 16 van het voorstel wordt verwezen naar instrumenten voor ouderlijk toezicht als mogelijke beperkende maatregelen, bevelen het EDPB en de EDPS in dit verband aan dat de voorgestelde verordening wordt gewijzigd om aanbieders uitdrukkelijk toe te staan gebruik te maken van mechanismen voor ouderlijk toezicht naast of als alternatief voor leeftijdsverificatie.

4.9 Bewaring van informatie

94. In artikel 22 van het voorstel worden de doeleinden beperkt waarvoor de onder het voorstel vallende aanbieders de inhoudelijke gegevens en andere gegevens die zijn verwerkt in verband met de maatregelen die zijn genomen om aan de verplichtingen van het voorstel te voldoen, mogen bewaren. In het voorstel wordt echter aangegeven dat aanbieders deze informatie ook mogen bewaren met het oog op het verbeteren van de doeltreffendheid en nauwkeurigheid van de technologieën voor het opsporen van online seksueel misbruik van kinderen om een opsporingsbevel uit te voeren, maar zij mogen voor dat doel geen persoonsgegevens opslaan[75].

95. Het EDPB en de EDPS zijn van mening dat alleen aanbieders die hun eigen opsporingstechnologieën gebruiken, gegevens mogen bewaren om de doeltreffendheid en nauwkeurigheid van de technologieën te verbeteren, terwijl degenen die gebruikmaken van technologieën die door het EU-centrum ter beschikking worden gesteld, niet van deze mogelijkheid mogen profiteren. Bovendien merken het EDPB en de EDPS op dat het in de praktijk moeilijk kan zijn ervoor te zorgen dat er voor dat doel geen persoonsgegevens worden opgeslagen, aangezien de meeste inhoudelijke gegevens en andere gegevens die voor opsporingsdoeleinden worden verwerkt waarschijnlijk als persoonsgegevens worden aangemerkt.

---

[72] Zie effectbeoordelingsverslag.
[73] Zie voorstel, artikel 4, lid 3, artikel 6, lid 1, punt c, en overweging 16.
[74] Zie bijvoorbeeld CNIL, 'Recommendation 7: Check the age of the child and parental consent while respecting the child's privacy' (Aanbeveling 7: Controleer de leeftijd van het kind en de toestemming van de ouders, met inachtneming van de privacy van het kind) (9 augustus 2021).
[75] Voorstel, artikel 22, lid 1.

4.10 Effect op versleuteling

96. De Europese gegevensbeschermingsautoriteiten hebben voortdurend gepleit voor de brede beschikbaarheid van robuuste versleutelingsinstrumenten en tegen het bestaan van allerlei achterdeurtjes[76]. Versleuteling is immers belangrijk om het genot van alle mensenrechten offline en online te waarborgen[77]. Bovendien dragen versleutelingstechnologieën op fundamentele wijze bij tot de eerbiediging van het privéleven en de vertrouwelijkheid van communicatie, alsook tot innovatie en de groei van de digitale economie, die afhankelijk is van de hoge mate van vertrouwen die dergelijke technologieën bieden.

97. In de context van interpersoonlijke communicatie is eind-tot-eindversleuteling een cruciaal instrument om de vertrouwelijkheid van elektronische communicatie te waarborgen, aangezien deze voorziet in sterke technische waarborgen tegen toegang tot de inhoud van de communicatie door anderen dan de afzender en de ontvanger(s), ook door de aanbieder. Het op enigerlei wijze voorkomen of ontmoedigen van het gebruik van eind-tot-eindversleuteling, het aan dienstenaanbieders opleggen van een verplichting om elektronischecommunicatiegegevens te verwerken voor andere doeleinden dan het aanbieden van hun diensten of het aan derden opleggen van een verplichting om op proactieve wijze elektronische communicatie door te geven, zou het risico inhouden dat aanbieders minder versleutelde diensten aanbieden om beter aan de verplichtingen te voldoen; daardoor zou de rol van versleuteling in het algemeen worden verzwakt en de eerbiediging van de grondrechten van de Europese burgers worden ondermijnd. Er zij op gewezen dat eind-tot-eindversleuteling weliswaar een van de meest gebruikte beveiligingsmaatregelen in de context van elektronische communicatie is, maar dat andere technische oplossingen (zoals het gebruik van andere cryptografische systemen) even belangrijk kunnen zijn of worden om de vertrouwelijkheid van digitale communicatie te waarborgen en te beschermen. Het gebruik ervan mag daarom niet ook worden verhinderd of ontmoedigd.

98. De toepassing van instrumenten voor het onderscheppen en analyseren van interpersoonlijke elektronische communicatie is fundamenteel in strijd met eind-tot-eindversleuteling, aangezien deze laatste beoogt technisch te waarborgen dat communicatie tussen de afzender en de ontvanger vertrouwelijk blijft.

99. Hoewel het voorstel niet voorziet in een verplichting tot systematische onderschepping voor aanbieders, zal de loutere mogelijkheid dat een opsporingsbevel wordt uitgevaardigd, waarschijnlijk zwaar meewegen in de technische keuzes van aanbieders, met name gezien de beperkte termijn waarin zij aan een dergelijk bevel zullen moeten voldoen en de zware sancties die zij zouden riskeren als zij dat niet doen[78]. In de praktijk kan dit ertoe leiden dat bepaalde aanbieders stoppen met het gebruik van eind-tot-eindversleuteling.

100. Het effect van het verminderen of ontmoedigen van het gebruik van eind-tot-eindversleuteling, dat uit het voorstel kan voortvloeien, moet naar behoren worden beoordeeld. Elk van de technieken om de privacy beschermende aard van eind-tot-eindversleuteling te omzeilen, zoals uiteengezet in het

---

[76] Zie bijvoorbeeld de Groep gegevensbescherming artikel 29, verklaring van de Groep artikel 29 over versleuteling en het effect ervan op de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens in de EU (11 april 2018).

[77] Zie Resolutie 47/16 van de Mensenrechtenraad over de bevordering, bescherming en uitoefening van mensenrechten op het internet, VN-doc. A/HRC/RES/47/16 (26 juli 2021).

[78] Zie voorstel, artikel 35.

effectbeoordelingsverslag bij het voorstel, zou lacunes in de beveiliging creëren[79]. Scannen aan de clientzijde[80] zou bijvoorbeeld waarschijnlijk leiden tot aanzienlijke, niet-gerichte toegang tot en verwerking van onversleutelde inhoud op apparaten van de eindgebruiker. Een dergelijke aanzienlijke aantasting van de vertrouwelijkheid zou met name gevolgen hebben voor kinderen, aangezien de diensten die zij gebruiken vaker het voorwerp zijn van opsporingsbevelen, waardoor zij kwetsbaar zijn voor monitoring of afluisteren. Tegelijkertijd is scannen aan de serverzijde ook fundamenteel onverenigbaar met het paradigma van eind-tot-eindversleuteling, aangezien het communicatiekanaal, dat peer-to-peer is versleuteld, zou moeten worden gekraakt, wat tot de bulkverwerking van persoonsgegevens op de servers van de aanbieders zou leiden.

101. Hoewel in het voorstel staat dat het "de betrokken aanbieder derhalve de vrije keuze [laat] wat betreft de te gebruiken technologieën om op doeltreffende wijze aan opsporingsbevelen te voldoen, en niet [mag] worden opgevat als een aansporing of ontmoediging om een bepaalde technologie te gebruiken"[81], komt de structurele onverenigbaarheid van een bepaald opsporingsbevel met eind-tot-eindversleuteling in feite neer op een grote belemmering om gebruik te maken van eind-tot-eindversleuteling. De onmogelijkheid om toegang te krijgen tot en gebruik te maken van diensten die gebruikmaken van eind-tot-eindversleuteling (die de huidige stand van de techniek op het gebied van de technische garantie van vertrouwelijkheid vormt) kan een remmend effect hebben op de vrijheid van meningsuiting en het legitieme privégebruik van elektronischecommunicatiediensten. De ongunstige verhouding tussen de opsporing van materiaal van seksueel misbruik van kinderen of van grooming en eind-tot-eindversleuteling wordt ook door de Commissie erkend toen zij in het effectbeoordelingsverslag[82] opmerkte dat de uitvoering van eind-tot-eindversleuteling door Facebook in 2023 waarschijnlijk zou inhouden dat Facebook zou stoppen met vrijwillig scannen.

102. Om ervoor te zorgen dat de voorgestelde verordening de veiligheid of vertrouwelijkheid van elektronische communicatie van Europese burgers niet ondermijnt, zijn het EDPB en de EDPS van mening dat in het dispositief van het voorstel duidelijk moet worden bepaald dat niets in de voorgestelde verordening mag worden uitgelegd als een verbod op of verzwakking van de versleuteling, in overeenstemming met overweging 25 van de tijdelijke verordening.

4.11 Toezicht, handhaving en samenwerking

4.11.1 Rol van nationale toezichthoudende autoriteiten in het kader van de AVG

103. Het voorstel voorziet in de oprichting van een netwerk van nationale coördinerende autoriteiten, die verantwoordelijk zijn voor de toepassing en handhaving van de voorgestelde verordening[83]. Hoewel in overweging 54 van het voorstel staat dat "[de] voorschriften van deze verordening met betrekking tot toezicht en handhaving geen afbreuk [doen] aan de bevoegdheden en competenties van de

[79] Zie hoofdstuk 4.2 in Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague en Carmela Troncoso, 'Bugs in our Pockets: The Risks of client-side Scanning', arXiv abs/2110.07450 (2021).
[80] Scannen aan de clientzijde verwijst in algemene zin naar systemen die de inhoud van berichten scannen op matches met een databank van bezwaarlijke inhoud voordat het bericht naar de beoogde ontvanger wordt verzonden.
[81] Voorstel, overweging 26.
[82] Effectbeoordelingsverslag, blz. 27.
[83] Voorstel, artikel 25.

gegevensbeschermingsautoriteiten uit hoofde van Verordening (EU) 2016/679", zijn het EDPB en de EDPS van mening dat de verhouding tussen de taken van coördinerende autoriteiten en die van gegevensbeschermingsautoriteiten beter moet worden geregeld en dat gegevensbeschermingsautoriteiten een prominentere rol moeten krijgen in de voorgestelde verordening.

104. Met name moeten aanbieders worden verplicht om gegevensbeschermingsautoriteiten te raadplegen door middel van een procedure van voorafgaande raadpleging als bedoeld in artikel 36 van de AVG alvorens maatregelen voor de opsporing van materiaal van seksueel misbruik van kinderen of van grooming te nemen, en niet uitsluitend in verband met het gebruik van maatregelen om het benaderen van kinderen op te sporen, zoals momenteel in het voorstel is voorzien [84] . Alle opsporingsmaatregelen moeten worden geacht standaard te resulteren in 'hoog risico' en moeten dus aan een procedure van voorafgaande raadpleging worden onderworpen, ongeacht of zij betrekking hebben op grooming of materiaal van seksueel misbruik van kinderen, zoals reeds het geval is in het kader van de tijdelijke verordening[85]. Bovendien moeten de in het kader van de AVG aangewezen bevoegde gegevensbeschermingsautoriteiten altijd de bevoegdheid hebben hun standpunt te geven over de beoogde opsporingsmaatregelen, en niet alleen in specifieke omstandigheden[86].

105. Bovendien moet de voorgestelde verordening voorzien in een systeem om geschillen tussen bevoegde autoriteiten en gegevensbeschermingsautoriteiten over opsporingsbevelen aan te pakken en op te lossen. De gegevensbeschermingsautoriteiten moeten met name het recht krijgen om een opsporingsbevel aan te vechten bij de rechtbanken van de lidstaat van de bevoegde gerechtelijke autoriteit of de onafhankelijke administratieve autoriteit die het opsporingsbevel heeft uitgevaardigd. In dit verband merken het EDPB en de EDPS op dat in de huidige versie van het voorstel de bevoegde autoriteit het advies van de bevoegde gegevensbeschermingsautoriteiten kan afwijzen wanneer zij een opsporingsbevel uitvaardigt. Dit kan leiden tot tegenstrijdige beslissingen, aangezien gegevensbeschermingsautoriteiten, zoals bevestigd in artikel 36, lid 2, van de AVG, hun volledige reeks corrigerende bevoegdheden uit hoofde van artikel 58 van de AVG zouden behouden, met inbegrip van de bevoegdheid om een verwerkingsverbod op te leggen.

4.11.2 Rol van het EDPB

106. Het EDPB en de EDPS merken op dat in artikel 50, lid 1, derde zin, van het voorstel is bepaald dat "het EU-centrum zijn technologisch comité en het Europees Comité voor gegevensbescherming om advies [vraagt]", voordat het een specifieke technologie toevoegt aan de lijsten van technologieën die aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten kunnen overwegen te gebruiken voor de uitvoering van opsporingsbevelen. Voorts is bepaald dat het EDPB zijn adviezen binnen een termijn van acht weken uitbrengt, die indien nodig met nog eens zes weken kan worden verlengd, rekening houdend met de complexiteit van het onderwerp. Tot slot moet het EDPB het EU-centrum binnen een maand na ontvangst van het verzoek om raadpleging in kennis stellen van een eventuele verlenging, samen met de redenen voor de vertraging.

[84] Voorstel, artikel 7, lid 3, tweede streepje, punt b.
[85] Tijdelijke verordening, artikel 3, lid 1, punt c.
[86] Zie voorstel, artikel 7, lid 3, tweede streepje, punt c.

107. De bestaande taken van het EDPB zijn vastgelegd in artikel 70 van de AVG en artikel 51 van Richtlijn (EU) 2016/680 ('Richtlijn voor gegevensbescherming bij rechtshandhaving')[87]. In het kader van deze taken is bepaald dat het EDPB advies verstrekt aan de Commissie en adviezen uitbrengt op verzoek van de Commissie, een nationale toezichthoudende autoriteit of zijn voorzitter. Hoewel in artikel 1, lid 3, punt d, van het voorstel wordt bepaald dat het voorstel geen afbreuk doet aan de regels van de AVG en van de richtlijn gegevensbescherming bij rechtshandhaving, gaat de bevoegdheid van het EU-centrum om advies in te winnen bij het EDPB verder dan de taken die krachtens de AVG en de richtlijn gegevensbescherming bij rechtshandhaving aan het EDPB zijn toegewezen. Daarom moet in de voorgestelde verordening, ten minste in een overweging, duidelijk worden gemaakt dat het voorstel de taken van het EDPB uitbreidt. In dit verband waarderen het EDPB en de EDPS de belangrijke rol die in het voorstel aan het EDPB wordt toebedeeld door zijn betrokkenheid bij de praktische uitvoering van de voorgestelde verordening te verlangen. In de praktijk speelt het secretariaat van het EDPB een essentiële rol bij het verlenen van de analytische, administratieve en logistieke ondersteuning die nodig is voor de vaststelling van de adviezen van het EDPB. Om ervoor te zorgen dat het EDPB en zijn leden hun taken kunnen vervullen, is het daarom van essentieel belang voldoende financiële en personele middelen aan het EDPB toe te wijzen. Helaas wordt in het financieel memorandum van het voorstel niet aangegeven dat er aanvullende middelen beschikbaar zullen worden gesteld voor de uitvoering van de aanvullende taken die in het voorstel aan het EDPB worden toegewezen[88].

108. Voorts merken het EDPB en de EDPS op dat in artikel 50 van het voorstel niet wordt aangegeven hoe het EU-centrum zal handelen nadat het een advies van het EDPB heeft ontvangen[89]. In overweging 27 van het voorstel wordt alleen vermeld dat het EU-centrum en de Europese Commissie rekening moeten houden met het advies van het EDPB. Daarom moet worden verduidelijkt wat het doel van het gevraagde advies zal zijn in de in artikel 50 van het voorstel uiteengezette procedure en hoe het EU-centrum moet handelen nadat het een advies van het EDPB heeft ontvangen.

109. Bovendien zijn het EDPB en de EDPS van mening dat, hoewel richtsnoeren van het EDPB of eventueel advies over het gebruik van opsporingstechnologieën het gebruik van dergelijke technologieën op algemeen niveau zullen beoordelen, de nationale toezichthoudende autoriteit voor een voorafgaande raadpleging uit hoofde van artikel 36 van de AVG rekening zal moeten houden met de specifieke omstandigheden en per geval een beoordeling moet uitvoeren van de voorgenomen verwerking door de betrokken verwerkingsverantwoordelijke. Het EDPB en de EDPS merken op dat toezichthoudende autoriteiten de criteria van artikel 36 van de AVG zullen en moeten toepassen om te beslissen of het nodig is de in de AVG vastgestelde termijn voor het uitbrengen van hun adviezen naar aanleiding van een voorafgaande raadpleging te verlengen. Het is volgens hen niet nodig verschillende normen toe te passen wanneer een voorafgaande raadpleging betrekking heeft op het gebruik van een opsporingtechnologie[90].

110. Tot slot bepaalt het voorstel bij de toepassing van artikel 11 ('Richtsnoeren inzake opsporingsverplichtingen') dat de Commissie richtsnoeren kan uitvaardigen voor de toepassing van

---

[87] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

[88] Zie voorstel, blz. 105 en volgende.

[89] Zie daarentegen artikel 51, lid 4, van de richtlijn gegevensbescherming bij rechtshandhaving.

[90] Zie voorstel, overweging 24.

de artikelen 7 tot en met 10 van het voorstel. Artikel 11 van het voorstel moet worden gewijzigd om duidelijk te maken dat, naast de coördinerende autoriteiten en het EU-centrum, het EDPB door de Commissie moet worden geraadpleegd over de ontwerprichtsnoeren buiten het beoogde openbare raadplegingsproces alvorens richtsnoeren inzake opsporingsverplichtingen uit te vaardigen.

111. Deze taak van het EDPB en zijn rol binnen het rechtskader dat met het voorstel zou worden ingevoerd, rechtvaardigen daarom verdere beoordeling door de wetgever.

4.11.3 Rol van het EU-centrum inzake seksueel misbruik van kinderen

112. In hoofdstuk IV van het voorstel zou het EU-centrum worden opgericht als een nieuw gedecentraliseerd agentschap om het voorstel te kunnen uitvoeren. Het EU-centrum moet onder andere betrouwbare opsporingstechnologieën beter toegankelijk maken voor de aanbieders, indicatoren aanbieden die zijn opgesteld op basis van online seksueel misbruik van kinderen (geverifieerd door rechterlijke instanties of onafhankelijke administratieve autoriteiten van de lidstaten) met het oog op de opsporing van dergelijk misbruik, op verzoek bepaalde bijstand verlenen in verband met de uitvoering van risicobeoordelingen en steun verlenen bij het communiceren met de bevoegde nationale autoriteiten[91].

113. In dat opzicht zijn het EDPB en de EDPS ingenomen met artikel 77, lid 2, van het voorstel, waarin wordt bevestigd dat de verwerking van persoonsgegevens door het EU-centrum onderworpen is aan de EUDPR. Ook wordt daarin bepaald dat de maatregelen voor de toepassing van die verordening door het EU-centrum, onder meer de maatregelen betreffende de benoeming van een functionaris voor gegevensbescherming van het EU-centrum, worden vastgesteld na raadpleging van de EDPS. Het EDPB en de EDPS zijn echter van mening dat verschillende bepalingen van dit hoofdstuk nader moeten worden bekeken.

114. Ten eerste merken zij op dat artikel 48 van het voorstel voorschrijft dat alle meldingen die "niet kennelijk ongegrond"[92] zijn, worden doorgestuurd aan de nationale rechtshandhavingsinstanties en het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol). Deze drempel voor het door het EU-centrum doorsturen van meldingen aan de nationale rechtshandhavingsinstanties en Europol (die "niet kennelijk ongegrond" zijn) lijkt te laag, met name gezien het feit dat de oprichting van het EU-centrum (zoals uiteengezet in het effectbeoordelingsverslag van de Commissie[93]) tot doel heeft de last van het filteren van inhoud die ten onrechte als materiaal van seksueel misbruik van kinderen wordt gemarkeerd voor rechtshandhavingsinstanties en Europol te verlichten. In dit opzicht is het onduidelijk waarom het EU-centrum als expertisecentrum geen grondigere juridische en feitelijke beoordeling zou kunnen uitvoeren om het risico te beperken dat gegevens van onschuldige personen aan rechtshandhavingsinstanties worden verstuurd.

115. Ten tweede lijkt de bepaling betreffende de duur van de opslag van persoonsgegevens door het EU-centrum relatief onbepaald gezien de gevoeligheid van de betrokken gegevens. Zelfs indien het niet mogelijk zou zijn een maximale bewaartermijn voor de opslag van die gegevens vast te stellen, bevelen het EDPB en de EDPS aan om in het voorstel ten minste een maximumtermijn vast te stellen voor het

---

[91] COM(2022) 209 final, blz. 7.
[92] De term 'kennelijk ongegrond' wordt in overweging 65 van het voorstel omschreven als "wanneer het zonder enige inhoudelijke juridische of feitelijke analyse onmiddellijk duidelijk is dat de gemelde activiteiten geen online seksueel misbruik van kinderen vormen".
[93] Zie bijvoorbeeld blz. 349 van het effectbeoordelingsverslag.

evalueren van de noodzaak dat gegevens opgeslagen blijven en voor het rechtvaardigen van een verlenging van de bewaring na die periode.

116. Gezien de zeer hoge gevoeligheid van de persoonsgegevens die door het EU-centrum moeten worden verwerkt, zijn het EDPB en de EDPS bovendien van mening dat de verwerking aan aanvullende waarborgen moet worden onderworpen, met name om doeltreffend toezicht te waarborgen. Dit zou onder meer de verplichting voor het EU-centrum kunnen omvatten om logbestanden bij te houden voor verwerkingshandelingen in geautomatiseerde verwerkingssystemen met betrekking tot de gegevens (d.w.z. rekening houdend van de vereiste inzake operationele persoonsgegevens uit hoofde van hoofdstuk IX van de EUDPR), waaronder het registreren van de invoer, wijziging, toegang, raadpleging, bekendmaking, combinatie en verwijdering van persoonsgegevens. De logbestanden van raadpleging en bekendmaking maken het mogelijk de redenen voor en de datum en het tijdstip van die handelingen te achterhalen, alsook de identiteit van de persoon die operationele persoonsgegevens heeft geraadpleegd of bekendgemaakt, en voor zover mogelijk de identiteit van de ontvangers. Deze logbestanden zouden worden gebruikt om de rechtmatigheid van de verwerking te controleren, interne controle uit te oefenen en de integriteit en beveiliging ervan te waarborgen, en zouden op verzoek beschikbaar worden gesteld aan de functionaris voor gegevensbescherming van het EU-centrum en aan de EDPS.

117. Voorts wordt in het voorstel verwezen naar de verplichting voor aanbieders om gebruikers te informeren over de opsporing van materiaal van seksueel misbruik van kinderen via opsporingsbevelen, alsook over het recht om een klacht in te dienen bij een coördinerende autoriteit[94]. Het voorstel voorziet echter niet in procedures voor de uitoefening van de rechten van betrokkenen, waarbij ook rekening wordt gehouden met de verschillende locaties waar persoonsgegevens kunnen worden doorgegeven en opgeslagen in het kader van het voorstel (EU-centrum, Europol, nationale rechtshandhavingsinstanties). De vereiste om gebruikers te informeren moet de verplichting omvatten personen ervan in kennis te stellen dat hun gegevens zijn doorgegeven en worden verwerkt door verschillende entiteiten, indien van toepassing (zoals door nationale rechtshandhavingsinstanties en Europol). Daarnaast moet er een gecentraliseerde procedure voorhanden zijn voor het ontvangen en coördineren van verzoeken om het recht op toegang, rectificatie en verwijdering, of anders een verplichting dat de entiteit die een verzoek van een betrokkene ontvangt, met de andere betrokken entiteiten coördineert.

118. Het EDPB en de EDPS merken op dat het EU-centrum op grond van artikel 50 van het voorstel is belast met het specificeren van de lijst van technologieën die kunnen worden gebruikt voor de uitvoering van opsporingsbevelen. Overeenkomstig artikel 12, lid 1, van het voorstel zijn aanbieders echter verplicht alle informatie te melden die wijst op mogelijk online seksueel misbruik van kinderen via hun diensten, niet alleen die welke voortkomt uit de uitvoering van een opsporingsbevel. Het is zeer waarschijnlijk dat een aanzienlijke hoeveelheid van dergelijke informatie voortkomt uit de toepassing van risicobeperkende maatregelen van aanbieders, overeenkomstig artikel 4 van het voorstel. Het lijkt dan ook van cruciaal belang te bepalen wat deze maatregelen zouden kunnen zijn, hoe doeltreffend ze zijn, hoe groot het foutenpercentage is bij het melden van mogelijk seksueel misbruik van kinderen en wat het effect ervan is op de rechten en vrijheden van personen. Ondanks het feit dat in artikel 4, lid 5, van het voorstel is bepaald dat de Commissie, in samenwerking met de coördinerende autoriteiten en het EU-centrum en na een openbare raadpleging te hebben gehouden, relevante richtsnoeren kan uitvaardigen, vinden het EDPB en de EDPS het belangrijk dat de wetgever in artikel 50

[94] Zie artikel 10, lid 6, en, na indiening van een verslag bij het EU-centrum, artikel 12, lid 2, van het voorstel.

een taak voor het EU-centrum opneemt om ook een lijst te verstrekken van aanbevolen risicobeperkende maatregelen en relevante beste praktijken die met name doeltreffend zijn om mogelijk online seksueel misbruik van kinderen op te sporen. Aangezien dergelijke maatregelen de grondrechten op gegevensbescherming en privacy kunnen aantasten, wordt ook aanbevolen dat het EU-centrum het advies van het EDPB inwint alvorens een dergelijke lijst te verstrekken.

119. Tot slot moeten de beveiligingsvoorschriften van artikel 51, lid 4, van het voorstel specifieker zijn. Hierbij is het dienstig uit te gaan van de beveiligingsvoorschriften die zijn vastgelegd in andere verordeningen met betrekking tot grootschalige systemen voor verwerking met een hoog risico, zoals Verordening (EG) nr. 767/2008[95] (zie artikel 32), Verordening (EG) nr. 1987/2006[96] (zie artikel 16), Verordening (EU) 2018/1862[97] (zie artikel 16) en Verordening (EU) nr. 603/2013[98] (zie artikel 34).

4.11.4 Rol van Europol

120. Het voorstel voorziet in nauwe samenwerking tussen het EU-centrum en Europol. Op grond van hoofdstuk IV van het voorstel controleert het EU-centrum ontvangen meldingen van aanbieders over vermoedelijk materiaal van seksueel misbruik van kinderen, om te beoordelen welke meldingen bruikbaar zijn (niet kennelijk ongegrond) en stuurt het deze door aan Europol en aan de nationale rechtshandhavingsinstanties[99]. Het EU-centrum verleent Europol toegang tot zijn databanken van indicatoren en databanken van meldingen om Europol te helpen bij het onderzoeken van vermoedelijke strafbare feiten met betrekking tot seksueel misbruik van kinderen[100]. Bovendien zou het EU-centrum worden voorzien van een "zo volledig mogelijke" toegang tot de informatiesystemen van Europol[101]. De twee agentschappen zullen ook gebouwen en bepaalde (niet-operationele) infrastructuur delen[102].

---

[95] Verordening (EG) nr. 767/2008 van het Europees Parlement en de Raad van 9 juli 2008 betreffende het Visuminformatiesysteem (VIS) en de uitwisseling tussen de lidstaten van gegevens op het gebied van visa voor kort verblijf (PB L 218 van 13.8.2008, blz. 60).

[96] Verordening (EG) nr. 1987/2006 van het Europees Parlement en de Raad van 20 december 2006 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II) (PB L 381 van 28.12.2006, blz. 4).

[97] Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politiële en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie (PB L 312 van 7.12.2018, blz. 56).

[98] Verordening (EU) nr. 603/2013 van het Europees Parlement en van de Raad van 26 juni 2013 betreffende de instelling van 'Eurodac' voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EU) nr. 604/2013 tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend en betreffende verzoeken van rechtshandhavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving, en tot wijziging van Verordening (EU) nr. 1077/2011 tot oprichting van een Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht (PB L 180 van 29.6.2013, blz. 1).

[99] Zie artikel 48 van het voorstel.

[100] Zie artikel 46, leden 4 en 5, van het voorstel.

[101] Zie artikel 53, lid 2, van het voorstel.

[102] Met name op het gebied van personeelsbeheer, informatietechnologie (IT), met inbegrip van cyberbeveiliging, het gebouw en communicatie.

121. Het EDPB en de EDPS merken op dat verschillende aspecten in verband met de samenwerking tussen het voorgestelde EU-centrum en Europol aanleiding geven tot bezorgdheid of nadere precisering vereisen.

Over het doorsturen van meldingen door het EU-centrum aan Europol (artikel 48)

122. In artikel 48 van de voorgestelde verordening wordt bepaald dat het EU-centrum meldingen die niet kennelijk ongegrond worden geacht, samen met eventuele aanvullende relevante informatie, moet doorsturen aan Europol en de bevoegde rechtshandhavingsinstantie of -instanties van de lidstaat die waarschijnlijk rechtsmacht heeft om het potentiële seksuele misbruik van kinderen waarop de melding betrekking heeft, te onderzoeken of te vervolgen. Hoewel in dit artikel Europol de rol krijgt toebedeeld om de relevante rechtshandhavingsinstantie te identificeren wanneer de betrokken lidstaat onduidelijk is, wordt in de bepaling in feite voorzien dat alle meldingen aan Europol worden toegezonden, ongeacht of de nationale autoriteit is geïdentificeerd en de melding reeds door het EU-centrum is verstuurd.

123. In het voorstel wordt echter niet verduidelijkt wat de toegevoegde waarde zou zijn van de betrokkenheid van Europol of zijn verwachte rol na ontvangst van de meldingen, met name in gevallen waarin de nationale rechtshandhavingsinstantie parallel is geïdentificeerd en in kennis is gesteld[103].

124. Het EDPB en de EDPS herinneren eraan dat het mandaat van Europol beperkt is tot het ondersteunen van het optreden van de bevoegde autoriteiten van de lidstaten en hun wederzijdse samenwerking bij het voorkomen en bestrijden van zware criminaliteit waarbij twee of meer lidstaten betrokken zijn[104]. In artikel 19 van Verordening (EU) 2016/794[105], zoals gewijzigd bij Verordening (EU) 2022/991[106] ('gewijzigde Europol-verordening'), is bepaald dat een orgaan van de Unie dat informatie aan Europol verstrekt, verplicht is het doel of de doelen waarvoor de informatie door Europol moet worden verwerkt, alsook de voorwaarden voor verwerking vast te stellen. Het is ook verantwoordelijk voor de nauwkeurigheid van de doorgegeven persoonsgegevens[107].

125. Een algemeen doorsturen van meldingen aan Europol zou derhalve in strijd zijn met de gewijzigde Europol-verordening en zou een aantal risico's op het gebied van gegevensbescherming meebrengen. Dubbele verwerking van persoonsgegevens kan ertoe leiden dat meerdere kopieën van dezelfde zeer gevoelige persoonsgegevens gelijktijdig worden opgeslagen (zoals bij het EU-centrum, Europol, de nationale rechtshandhavingsinstantie), met risico's voor de nauwkeurigheid van de gegevens als gevolg van de mogelijke desynchronisatie van databanken alsook voor de uitoefening van de rechten

[103] In overweging 71 van het voorstel wordt slechts in algemene zin verwezen naar de ervaring van Europol met het identificeren van bevoegde nationale autoriteiten in onduidelijke situaties en naar zijn databank van criminele inlichtingen, die kan bijdragen tot het identificeren van verbanden met onderzoeken in andere lidstaten.

[104] Zie artikel 3 van de gewijzigde Europol-verordening.

[105] Verordening (EU) 2016/794 van het Europees Parlement en de Raad van 11 mei 2016 betreffende het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (Europol) en tot vervanging en intrekking van de Besluiten 2009/371/JBZ, 2009/934/JBZ, 2009/935/JBZ, 2009/936/JBZ en 2009/968/JBZ van de Raad (PB L 135 van 24.5.2016, blz. 53).

[106] Verordening (EU) 2022/991 van het Europees Parlement en de Raad van 8 juni 2022 tot wijziging van Verordening (EU) 2016/794, wat betreft de samenwerking van Europol met particuliere partijen, de verwerking van persoonsgegevens door Europol ter ondersteuning van strafrechtelijke onderzoeken en de rol van Europol bij onderzoek en innovatie (PB L 169 van 27.6.2022, blz. 1).

[107] Artikel 38, lid 2, punt a, van de gewijzigde Europol-verordening.

van betrokkenen. Bovendien houdt de in het voorstel vastgestelde lage drempel voor het delen van meldingen met rechtshandhavingsinstanties (die "niet kennelijk ongegrond" zijn) een grote kans in dat fout-positieven (namelijk inhoud die ten onrechte als seksueel misbruik van kinderen wordt gemarkeerd) in de informatiesystemen van Europol zullen worden opgeslagen, mogelijk voor langere perioden[108].

126. Het EDPB en de EDPS bevelen daarom aan dat in het voorstel de omstandigheden en doeleinden worden gespecificeerd en beperkt in het kader waarvan het EU-centrum meldingen aan Europol kan doorsturen, overeenkomstig de gewijzigde Europolverordening. Dit moet uitdrukkelijk de omstandigheden uitsluiten waarin meldingen zijn doorgestuurd aan de betrokken rechtshandhavingsinstantie van de lidstaat, die erop wijzen geen grensoverschrijdend karakter te hebben. Daarnaast moet in het voorstel het voorschrift worden opgenomen dat het EU-centrum alleen persoonsgegevens aan Europol doorgeeft die toereikend en relevant zijn en beperkt blijven tot wat strikt noodzakelijk is. Er moet ook worden voorzien in specifieke waarborgen om de kwaliteit en betrouwbaarheid van de gegevens te waarborgen.

[108] Volgens het effectbeoordelingsverslag van de Commissie heeft Europol slechts 20 % van de 50 miljoen unieke beelden en video's van materiaal van seksueel misbruik van kinderen in zijn databank kunnen onderzoeken, wat duidt op een gebrek aan middelen om de bijdragen van materiaal van seksueel misbruik van kinderen die het momenteel ontvangt, te behandelen. Zie het effectbeoordelingsverslag bij het voorstel voor een verordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen, SWD(2022) 209, blz. 47-48.

Artikel 53, lid 2, over samenwerking tussen het EU-centrum en Europol

127. In artikel 53, lid 2, van het voorstel wordt bepaald dat Europol en het EU-centrum "[elkaar] voorzien van een zo volledig mogelijke toegang tot relevante informatie en informatiesystemen, waar nodig voor de uitoefening van hun respectieve taken en in overeenstemming met de handelingen van het Unierecht inzake een dergelijke toegang".

128. In artikel 46, leden 4 en 5, van het voorstel wordt verder gespecificeerd dat Europol toegang heeft tot de indicatorendatabank en de meldingendatabank van het EU-centrum, en in artikel 46, lid 6, wordt de procedure voor het verlenen van deze toegang bepaald: Europol dient een verzoek in met vermelding van het doel en de mate van inzage die nodig zijn om dat doel te bereiken, dat door het EU-centrum naar behoren wordt beoordeeld.

129. De criteria en waarborgen voor de inzage van Europol in en het gebruik van gegevens uit de informatiesystemen van het EU-centrum worden niet gespecificeerd. Bovendien wordt niet uitgelegd waarom het nodig is Europol rechtstreeks toegang te verlenen tot de informatiesystemen van een niet-rechtshandhavingsinstantie die zeer gevoelige persoonsgegevens bevatten, waarvan het verband met criminele activiteiten en misdaadpreventie mogelijk niet is aangetoond. Om een hoog niveau van gegevensbescherming en naleving van het doelbindingsbeginsel te waarborgen, bevelen het EDPB en de EDPS aan dat de doorgifte van persoonsgegevens door het EU-centrum aan Europol alleen per geval, na een naar behoren beoordeeld verzoek, plaatsvindt via een communicatie-instrument voor beveiligde uitwisseling, zoals Siena[109].

130. Artikel 53, lid 2, bevat de enige verwijzing in het voorstel naar de toegang van het EU-centrum tot de informatiesystemen van Europol. Het is dan ook onduidelijk voor welke doeleinden en volgens welke specifieke waarborgen een dergelijke toegang zou plaatsvinden.

131. Het EDPB en de EDPS herinneren eraan dat Europol een rechtshandhavingsinstantie is die is opgericht krachtens de EU-Verdragen en een kerntaak heeft op het gebied van het voorkomen en bestrijden van zware criminaliteit. De operationele persoonsgegevens die door Europol worden verwerkt, zijn bijgevolg onderworpen aan strikte regels en waarborgen inzake gegevensverwerking. Het voorgestelde EU-centrum is geen rechtshandhavingsinstantie en mag in geen geval rechtstreeks toegang krijgen tot de informatiesystemen van Europol.

132. Het EDPB en de EDPS merken voorts op dat een groot deel van de informatie die van gemeenschappelijk belang is voor het EU-centrum en voor Europol, betrekking zal hebben op persoonsgegevens van slachtoffers van vermoedelijke misdaden, persoonsgegevens van minderjarigen en persoonsgegevens die het seksuele gedrag betreffen, die in het kader van de gewijzigde Europol-verordening als bijzondere categorieën persoonsgegevens worden aangemerkt. De gewijzigde Europol-verordening stelt strikte voorwaarden op voor de toegang tot bijzondere categorieën persoonsgegevens. In artikel 30, lid 3, van de gewijzigde Europol-verordening wordt bepaald dat alleen Europol rechtstreeks toegang heeft tot dergelijke persoonsgegevens, meer bepaald slechts een beperkt aantal Europol-functionarissen die naar behoren door de uitvoerend directeur zijn gemachtigd[110].

[109] Secure Information Exchange Network Application (Siena).

[110] Krachtens de gewijzigde Europol-verordening gelden uitzonderingen op dit verbod voor krachtens titel V VWEU opgerichte agentschappen van de Unie. Gezien de rechtsgrondslag voor het voorstel (artikel 114 VWEU, met betrekking tot de harmonisatie van de interne markt), zou het voorgestelde EU-centrum echter niet onder deze uitzondering vallen.

133. Het EDPB en de EDPS bevelen daarom aan om de formulering van artikel 53, lid 2, van het voorstel te verduidelijken teneinde de beperkingen uit hoofde van de gewijzigde Europol-verordening naar behoren weer te geven en de voorwaarden voor toegang voor het EU-centrum te specificeren. Met name mag toegang tot persoonsgegevens die in de informatiesystemen van Europol worden verwerkt, wanneer dit strikt noodzakelijk wordt geacht voor de uitvoering van de taken van het EU-centrum, alleen per geval worden verleend, na indiening van een uitdrukkelijk verzoek waarin het specifieke doel en de motivering worden gedocumenteerd. Europol moet worden verplicht die verzoeken zorgvuldig te beoordelen en alleen persoonsgegevens aan het EU-centrum toe te sturen wanneer dit strikt noodzakelijk is en in verhouding staat tot het vereiste doel.

Artikel 10, lid 6, over de rol van Europol bij het informeren van gebruikers na de uitvoering van een opsporingsbevel

134. Het EDPB en de EDPS zijn ingenomen met de in artikel 10, lid 6, van het voorstel neergelegde verplichting voor aanbieders om gebruikers van wie de persoonsgegevens bij de uitvoering van een opsporingsbevel betrokken kunnen zijn, te informeren. Deze informatie mag pas aan gebruikers worden verstrekt na bevestiging van Europol of de nationale rechtshandhavingsinstantie van een lidstaat die de in artikel 48 van het voorstel bedoelde melding heeft ontvangen dat het verstrekken van informatie aan gebruikers geen afbreuk zou doen aan activiteiten voor het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten met betrekking tot seksueel misbruik van kinderen.

135. Het ontbreekt echter aan duidelijkheid wat betreft de praktische uitvoering van deze bepaling. Wanneer meldingen zowel aan Europol als aan een rechtshandhavingsinstantie van een lidstaat worden doorgestuurd, wordt in het voorstel niet bepaald of bevestiging van een of beide ontvangers vereist is, noch worden de procedures/modaliteiten voor het verkrijgen van deze bevestiging in het voorstel beschreven (zoals of bevestigingen via het EU-centrum moeten worden doorgegeven). Rekening houdend met de grote hoeveelheid materiaal van seksueel misbruik van kinderen die Europol en de nationale rechtshandhavingsinstanties moeten verwerken en het ontbreken van een precieze termijn voor het verstrekken van bevestiging (“zonder onnodige vertraging”), bevelen het EDPB en de EDPS aan de toepasselijke procedures te verduidelijken om ervoor te zorgen dat deze waarborg in de praktijk wordt verwezenlijkt. Voorts moet de verplichting om gebruikers te informeren ook informatie bevatten over de ontvangers van de betrokken persoonsgegevens.

Over gegevensverzameling en transparantieverslaglegging (artikel 83)

136. In artikel 83, lid 3, van het voorstel is bepaald dat het EU-centrum gegevens moet verzamelen en statistieken moet produceren met betrekking tot een aantal van zijn taken uit hoofde van de voorgestelde verordening. Voor controledoeleinden bevelen het EDPB en de EDPS aan om aan deze lijst statistieken toe te voegen over het aantal meldingen dat overeenkomstig artikel 48 aan Europol is doorgestuurd, alsook over het aantal verzoeken om inzage dat Europol uit hoofde van artikel 46, leden 4 en 5 heeft ontvangen, met inbegrip van het aantal verzoeken dat door het EU-centrum is ingewilligd en geweigerd.

5. CONCLUSIE

137. Hoewel het EDPB en de EDPS ingenomen zijn met de inspanningen van de Commissie om doeltreffend op te treden tegen online seksueel misbruik van kinderen, zijn zij van mening dat het voorstel aanleiding geeft tot ernstige bezorgdheid over gegevensbescherming en privacy. Daarom verzoeken het EDPB en de EDPS de medewetgevers de voorgestelde verordening te wijzigen, met name om

ervoor te zorgen dat de beoogde opsporingsverplichtingen voldoen aan de toepasselijke normen inzake noodzakelijkheid en evenredigheid en niet leiden tot een verzwakking of aantasting van de versleuteling op algemeen niveau. Het EDPB en de EDPS blijven beschikbaar om tijdens het wetgevingsproces hun steun te verlenen, indien hun inbreng noodzakelijk wordt geacht om de in dit gezamenlijk advies genoemde punten van zorg aan te pakken.

Voor de Europese toezichthouder voor gegevensbescherming	Voor het Europees Comité voor gegevensbescherming
De Europese Toezichthouder voor gegevensbescherming	De voorzitter
(Wojciech Wiewiorowski)	(Andrea Jelinek)