EDPB–EDPS

Gemensamt yttrande 4/2022 över förslaget till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn

Antaget den 28 juli 2022

Translations proofread by EDPB Members.

This language version has not yet been proofread.

INNEHÅLLSFÖRTECKNING

Sammanfattning

Den 11 maj 2022 lade Europeiska kommissionen fram sitt förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn.

Förslaget innebär att kvalificerade skyldigheter införs för värdtjänstleverantörer, leverantörer av interpersonella kommunikationstjänster och andra tjänsteleverantörer när det gäller spårning, rapportering, avlägsnande och blockering av känt och nytt material med sexuella övergrepp mot barn på nätet samt kontaktsökning med barn. Förslaget innehåller också bestämmelser om inrättande av en ny, decentraliserad EU-byrå (nedan kallat *EU-centrumet*) och ett nätverk av nationella samordningsmyndigheter för frågor som rör sexuella övergrepp mot barn för att möjliggöra genomförandet av den föreslagna förordningen. Såsom anges i motiveringen till förslaget skulle åtgärderna i förslaget påverka utövandet av de grundläggande rättigheterna för användarna av de berörda tjänsterna.

Sexuella övergrepp mot barn är ett särskilt allvarligt och avskyvärt brott och målet att möjliggöra effektiva åtgärder för att bekämpa sådana är ett mål av allmänt intresse som erkänns av unionen och som syftar till att skydda brottsoffrens rättigheter och friheter. Samtidigt konstaterar Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) att alla begränsningar av de grundläggande rättigheterna, såsom de som avses i förslaget, måste uppfylla kraven i artikel 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna.

EDPB och EDPS betonar att förslaget ger upphov till allvarliga farhågor när det gäller proportionaliteten i det planerade ingreppet och begränsningarna av skyddet av de grundläggande rättigheterna till privatliv och skydd av personuppgifter. I detta avseende påpekar EDPB och EDPS att rättssäkerhetsgarantier aldrig helt kan ersätta materiella skyddsåtgärder. Ett komplext system med eskalering från riskbedömning och riskbegränsningsåtgärder till en spårningsorder kan inte ersätta den tydlighet som krävs i fråga om de materiella skyldigheterna.

EDPB och EDPS anser att förslaget är otydligt i fråga om centrala aspekter, såsom begreppet ”betydande risk”. Dessutom har de enheter som ansvarar för att tillämpa dessa skyddsåtgärder, från privata aktörer till administrativa och/eller rättsliga myndigheter, ett mycket stort utrymme för skönsmässig bedömning, vilket leder till rättslig osäkerhet om hur man ska balansera de rättigheter som står på spel i varje enskilt fall. EDPB och EDPS betonar att lagstiftaren, när den tillåter särskilt allvarliga ingrepp i de grundläggande rättigheterna, måste skapa rättslig klarhet om när och var ingrepp är tillåtna. EDPB och EDPS är medvetna om att lagstiftningen inte kan vara alltför preskriptiv, utan måste medge en viss flexibilitet i den praktiska tillämpningen, men anser att förslaget lämnar alltför stort utrymme för potentiellt missbruk på grund av avsaknaden av tydliga materiella normer.

När det gäller de planerade spårningsåtgärdernas nödvändighet och proportionalitet är EDPB och EDPS särskilt oroade när det gäller åtgärder som planeras för spårning av okänt material med sexuella övergrepp mot barn och kontaktsökning av barn (gromning) inom interpersonella kommunikationstjänster. På grund av graden av intrång, den probabilistiska utformningen och felnivån i samband med sådan teknik anser EDPB och EDPS att de ingripanden som dessa åtgärder medför går utöver vad som är nödvändigt och proportionerligt. Åtgärder som gör det möjligt för offentliga myndigheter att allmänt få tillgång till innehållet i en överföring för att spåra kontaktsökning med barn kommer dessutom med större sannolikhet att påverka det väsentliga innehållet i de rättigheter som garanteras i artiklarna 7 och 8 i stadgan. Därför bör de berörda bestämmelserna om gromning tas bort från förslaget. Dessutom utesluter förslaget inte genomsökning av

ljudkommunikation från sitt tillämpningsområde. EDPB och EDPS anser att genomsökning av ljudkommunikation är särskilt inkräktande och därför fortsatt måste ligga utanför tillämpningsområdet för de spårningsskyldigheter som fastställs i den föreslagna förordningen, både när det gäller röstmeddelanden och direktkommunikation.

EDPB och EDPS betvivlar också att blockeringsåtgärder är effektiva och anser att det skulle vara oproportionerligt att kräva att leverantörer av internettjänster dekrypterar kommunikation online för att blockera kommunikation som rör material med sexuella övergrepp mot barn.

Dessutom påpekar EDPB och EDPS att krypteringsteknik på ett grundläggande sätt bidrar till respekten för privatlivet och konfidentialiteten vid kommunikation, yttrandefriheten samt till innovation och tillväxt i den digitala ekonomin, som är beroende av den höga graden av tillit och förtroende för sådan teknik. Enligt skäl 26 i förslaget omfattas inte bara valet av spårningsteknik, utan även de tekniska åtgärderna för att skydda konfidentialiteten vid kommunikation, såsom kryptering, av förbehållet att detta tekniska val måste uppfylla kraven i den föreslagna förordningen, dvs. det måste möjliggöra spårning. Detta stöder tanken i artiklarna 8.3 och 10.2 i förslaget att en leverantör inte kan vägra att verkställa en spårningsorder på grund av att det är tekniskt omöjligt. EDPB och EDPS anser att det bör finnas en bättre balans mellan samhällets behov av säkra och privata kommunikationskanaler och behovet av att bekämpa missbruk av dem. Det bör tydligt anges i förslaget att ingenting i den föreslagna förordningen bör tolkas som att kryptering förbjuds eller försvagas.

Även om EDPB och EDPS välkomnar uttalandet i förslaget om att det inte påverkar dataskyddsmyndigheternas befogenheter och behörigheter enligt den allmänna dataskyddsförordningen, anser EDPB och EDPS att förhållandet mellan de samordnande myndigheternas och dataskyddsmyndigheternas uppgifter ändå bör regleras bättre. I detta avseende uppskattar EDPB och EDPS den roll som EDPB tilldelas enligt förslaget, där det krävs att den ska vara delaktig i det praktiska genomförandet av förslaget och särskilt att EDPB behöver avge ett yttrande om den teknik som EU-centrumet skulle göra tillgänglig för att verkställa spårningsorder. Det bör dock klargöras vilket syfte yttrandet skulle ha i processen och hur EU-centrumet skulle agera efter att ha mottagit ett yttrande från EDPB.

Slutligen noterar EDPB och EDPS att förslaget föreskriver ett nära samarbete mellan EU-centrumet och Europol, som ”i största möjliga utsträckning [bör] ge varandra åtkomst till relevant information”. EDPB och EDPS stöder i princip samarbetet mellan de båda byråerna, men med tanke på att EU-centrumet inte är en brottsbekämpande myndighet, lämnar EDPB och EDPS ändå flera rekommendationer om förbättring av de relevanta bestämmelserna, bland annat om att överföringen av personuppgifter mellan EU-centrumet och Europol endast ska göras från fall till fall, efter en vederbörligen bedömd begäran, via ett säkert kommunikationsverktyg för utbyte, såsom Siena-nätverket.

Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen har antagit detta gemensamma yttrande

med beaktande av artikel 42.2 i Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (nedan kallad *Europeiska unionens dataskyddsförordning*),[1]

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018,[2]

med beaktande av kommissionens begäran om ett gemensamt yttrande från Europeiska dataskyddsstyrelsen och Europeiska datatillsynsmannen av den 12 maj 2022 över förslaget till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn[3].

HÄRIGENOM FRAMFÖRS FÖLJANDE.

1. BAKGRUND

1. Den 11 maj 2022 lade Europeiska kommissionen (nedan kallad *kommissionen*) fram sitt förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn (nedan kallat *förslaget* eller *förslaget till förordning*).[4]

2. Förslaget lades fram efter antagandet av förordning (EU) 2021/1232 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet (nedan kallad *interimsförordningen*).[5] Enligt interimsförordningen är de berörda tjänsteleverantörerna inte skyldiga att vidta åtgärder för att spåra material med sexuella övergrepp mot barn (t.ex. bilder, videor osv.) eller kontaktsökning med barn (även kallad gromning) på sina tjänster, men gör det möjligt för dessa leverantörer att göra detta på frivillig basis, i enlighet med villkoren i den förordningen.[6]

---

[1] EUT L 295, 21.11.2018, s. 39.
[2] Hänvisningar till ”medlemsstater” i detta dokument ska tolkas som hänvisningar till ”EES-medlemsstater”.
[3] Förslag till Europaparlamentets och rådets förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn, COM(2022) 209 final.
[4] Ibid.
[5] Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet, EUT L 274, [2021], s. 41.
[6] Se även Europeiska datatillsynsmannens yttrande 7/2020 om förslaget till tillfälliga undantag från direktiv 2002/58/EG för att bekämpa sexuella övergrepp mot barn på nätet (10 november 2020).

3. Förslaget består av två huvuddelar. För det första införs kvalificerade skyldigheter för värdtjänstleverantörer, leverantörer av interpersonella kommunikationstjänster och av andra tjänster när det gäller spårning, rapportering, avlägsnande och blockering av känt och nytt material med sexuella övergrepp mot barn på nätet samt kontaktsökning med barn. För det andra föreskrivs i förslaget att det ska inrättas en ny decentraliserad EU-byrå (nedan kallad *EU-centrumet mot sexuella övergrepp mot barn* eller *EU-centrumet*) och ett nätverk av nationella samordningsmyndigheter för frågor som rör sexuella övergrepp mot barn, för att möjliggöra genomförandet av den föreslagna förordningen.[7]

4. Såsom anges i motiveringen till förslaget skulle åtgärderna i förslaget påverka utövandet av de grundläggande rättigheterna för användarna av de berörda tjänsterna. Dessa rättigheter omfattar särskilt de grundläggande rättigheterna till skydd för privatlivet (inbegripet konfidentialitet vid kommunikation, som en del av den bredare rätten till skydd för privat- och familjeliv), skydd av personuppgifter samt yttrande- och informationsfrihet.[8]

5. Dessutom är de föreslagna åtgärderna avsedda att utgå från och i viss utsträckning komplettera EU:s befintliga lagstiftning om dataskydd och integritet. I detta avseende konstateras följande i motiveringen:

> ”Förslaget bygger på den allmänna dataskyddsförordningen (dataskyddsförordningen). I praktiken tenderar leverantörer att åberopa olika behandlingsgrunder i enlighet med dataskyddsförordningen för att behandla personuppgifter som de stöter på i samband med deras frivilliga spårning och rapportering av sexuella övergrepp mot barn på nätet. I förslaget fastställs ett system med riktade spårningsorder och villkoren för spårningen specificeras, vilket ger dessa åtgärder större rättssäkerhet. När det gäller sådan obligatorisk spårningsverksamhet som inbegriper behandling av personuppgifter fastställs i förslaget, särskilt när det gäller spårningsorder som utfärdas på grundval av denna, att grunden för denna behandling är artikel 6.1 c i dataskyddsförordningen, dvs. behandling av personuppgifter som är nödvändig för att fullgöra en rättslig förpliktelse som enligt unionsrätten eller medlemsstaternas lagstiftning åvilar den personuppgiftsansvarige.
>
> Förslaget omfattar bland annat leverantörer som erbjuder interpersonella elektroniska kommunikationstjänster och därför omfattas av nationella bestämmelser om genomförande av direktivet om integritet och elektronisk kommunikation och den föreslagna översynen av detta direktiv som för närvarande pågår. De åtgärder som anges i förslaget begränsar i vissa avseenden omfattningen för rättigheterna och skyldigheterna enligt de relevanta bestämmelserna i det direktivet, nämligen när det gäller verksamhet som är absolut nödvändig för att verkställa spårningsorder. I detta avseende inbegriper förslaget en analog tillämpning av artikel 15.1 i det direktivet.”[9]

6. Med tanke på hur allvarliga de planerade ingreppen i de grundläggande rättigheterna är har förslaget särskilt stor betydelse för skyddet av enskildas rättigheter och friheter i samband med behandling av personuppgifter. Den 12 maj 2022 beslutade kommissionen därför att samråda med Europeiska dataskyddsstyrelsen (EDPB) och Europeiska datatillsynsmannen (EDPS) i enlighet med artikel 42.2 i Europeiska unionens dataskyddsförordning.

---

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

2. YTTRANDETS OMFATTNING

7. I detta gemensamma yttrande anges EDPB:s och EDPS gemensamma ståndpunkter om förslaget. Yttrandet är begränsat till de aspekter av förslaget som rör skyddet av privatlivet och personuppgifter. I det gemensamma yttrandet framhålls särskilt de områden där förslaget inte säkerställer ett tillräckligt skydd av de grundläggande rättigheterna till privatlivet och uppgiftsskydd eller kräver ytterligare anpassning till EU:s rättsliga ram för skydd av privatlivet och personuppgifter.

8. Såsom förklaras närmare i detta gemensamma yttrande ger förslaget upphov till allvarliga farhågor om huruvida de planerade ingreppen och begränsningarna i skyddet av de grundläggande rättigheterna till privatliv och skydd av personuppgifter är nödvändiga och proportionerliga. Syftet med detta gemensamma yttrande är dock varken att ge en uttömmande förteckning över alla frågor om privatliv och uppgiftsskydd som tas upp i förslaget eller att lägga fram konkreta förslag för att förbättra förslagets ordalydelse. I stället innehåller detta gemensamma yttrande kommentarer på hög nivå om de huvudfrågor som tas upp i förslaget och som identifierats av EDPB och EDPS. EDPB och EDPS förblir dock tillgängliga för att lämna ytterligare kommentarer och rekommendationer till medlagstiftarna under lagstiftningsprocessen om förslaget.

3. ALLMÄNNA KOMMENTARER OM RÄTTEN TILL KONFIDENTIALITET VID KOMMUNIKATION OCH TILL SKYDDET AV PERSONUPPGIFTER

9. Konfidentialitet vid kommunikation är en väsentlig del av den grundläggande rätten till skydd för privat- och familjeliv, som fastställs i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad *stadgan*).[10] I artikel 8 i Europakonventionen ingår rätten till skydd av personuppgifter. Rätten till konfidentialitet vid kommunikation och rätten till privat- och familjeliv garanteras också i artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (nedan kallad *Europakonventionen*) och ingår i medlemsstaternas gemensamma konstitutionella traditioner.[11]

10. EDPB och EDPS noterar att de rättigheter som fastställs i artiklarna 7 och 8 i stadgan inte är absoluta rättigheter, utan måste beaktas i förhållande till deras funktion i samhället.[12] Sexuella övergrepp mot barn är ett särskilt allvarligt och avskyvärt brott och målet att möjliggöra effektiva åtgärder för att bekämpa sådana är ett mål av allmänt intresse som erkänns av unionen och som syftar till att skydda brottsoffrens rättigheter och friheter. När det gäller effektiva åtgärder för att bekämpa brott som begås mot minderåriga och andra utsatta personer har Europeiska unionens domstol (nedan kallad *EU-domstolen*) påpekat att positiva skyldigheter kan följa av artikel 7 i stadgan, som kräver att offentliga myndigheter vidtar rättsliga åtgärder för att skydda privat- och familjeliv, hem och kommunikation. Sådana skyldigheter kan också följa av artiklarna 3 och 4 i stadgan, vad gäller skyddet

[10] Se t.ex. EDPB:s uttalande om översynen av förordningen om integritet och elektronisk kommunikation och dess inverkan på skyddet för enskilda personer med avseende på integriteten och konfidentialiteten i deras kommunikation (25 maj 2018).
[11] Nästan alla europeiska konstitutioner innehåller en rätt till skydd av konfidentialitet vid kommunikation. Se t.ex. artikel 15 i Republiken Italiens konstitution, artikel 10 i Förbundsrepubliken Tysklands grundlag, artikel 22 i den belgiska konstitutionen och artikel 13 i Konungariket Nederländernas konstitution.
[12] Se, bland annat, EU-domstolens dom i mål C-311/18, Facebook Ireland och Schrems, punkt 172 och däri angiven rättspraxis. Se även skäl 4 i den allmänna dataskyddsförordningen.

av en persons fysiska och psykiska integritet och förbudet mot tortyr och omänsklig och förnedrande behandling.[13]

11. Samtidigt måste alla begränsningar av de rättigheter som garanteras i stadgan, såsom de som anges i förslaget, [14] uppfylla kraven i artikel 52.1 i stadgan. Varje åtgärd som inkräktar på rätten till konfidentialitet vid kommunikation och rätten till privat- och familjeliv måste först och främst respektera det väsentliga innehållet i de aktuella rättigheterna. [15] Det väsentliga innehållet i en rättighet påverkas om rättigheten töms på sitt grundläggande innehåll och den enskilde inte kan utöva den[16]. Ingreppet får inte, i förhållande till det eftersträvade målet, utgöra ett sådant oproportionerligt och oacceptabelt ingrepp som påverkar själva det väsentliga innehållet i den på detta sätt garanterade rättigheten.[17] Detta innebär att även en grundläggande rättighet som inte är absolut till sin natur, såsom rätten till konfidentialitet vid kommunikation och rätten till skydd av personuppgifter, har vissa centrala delar som inte får begränsas.

12. EU-domstolen har vid flera tillfällen tillämpat ”det väsentliga innehållet i en rättighet” på området integritet för elektronisk kommunikation. I sin dom i målet Tele2 Sverige och Watson slog EU-domstolen fast att lagstiftning som inte medger lagring av innehållet i en kommunikation inte kan kränka det väsentliga innehållet i rättigheterna till integritet och skydd av personuppgifter. [18] I sin dom i målet Schrems slog EU-domstolen fast att en lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer anses kränka det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet, som garanteras i artikel 7 i stadgan[19]. I sin dom i målet Digital Rights Ireland och Seitlinger m.fl. slog domstolen fast att även om den lagring av uppgifter som föreskrivs i direktiv 2006/24 utgör ett synnerligen allvarligt ingrepp i den grundläggande rättigheten till privatliv och de andra rättigheter som föreskrivs i artikel 7 i stadgan kan den inte kränka deras väsentliga innehåll, eftersom det enligt direktivet inte var tillåtet att skaffa sig kännedom om själva innehållet i de elektroniska kommunikationerna. [20] Av denna rättspraxis kan slutsatsen dras att åtgärder som gör det möjligt för offentliga myndigheter att allmänt få tillgång till innehållet i en kommunikationsöverföring med större sannolikhet kommer att påverka det väsentliga innehållet i de rättigheter som garanteras i artiklarna 7 och 8 i stadgan. Dessa överväganden är också relevanta när det gäller åtgärder för spårning av material med sexuella övergrepp mot barn och kontaktsökning med barn, såsom de åtgärder som föreslås i förslaget.

13. Dessutom har EU-domstolen funnit att datasäkerhetsåtgärder spelar en viktig roll för att säkerställa att det väsentliga innehållet i den grundläggande rätten till skydd av personuppgifter i artikel 8 i

---

[13] EU-domstolen, förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., punkterna 126–128. Se även EDPS yttrande 7/2020 om förslaget till tillfälliga undantag från direktiv 2002/58/EG för att bekämpa sexuella övergrepp mot barn på nätet (10 november 2020), punkt 12.

[14] Se COM(2022) 209 final, s. 12–13.

[15] Artikel 52.1 i stadgan.

[16] Se 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), s. 8, finns på https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (ej översatt till svenska)..

[17] EU-domstolen, mål C-393/19, *OM*, punkt 53.

[18] EU-domstolen, förenade målen C-203/15 och C-698/15, Tele2 Sverige och Watson, punkt 101.

[19] EU-domstolen, mål C-362/14, Schrems, punkt 94.

[20] EU-domstolen, förenade målen C-293/12 och C-594/12, Digital Rights Ireland och Seitlinger m.fl., punkt 39.

stadgan inte påverkas negativt.[21] I den digitala tidsåldern är tekniska lösningar för att säkra och skydda konfidentialiteten vid elektronisk kommunikation, inbegripet åtgärder för kryptering, avgörande för att säkerställa åtnjutandet av alla grundläggande rättigheter.[22] Detta bör vederbörligen beaktas vid bedömningen av åtgärder för obligatorisk spårning av material med sexuella övergrepp mot barn eller kontaktsökning med barn, särskilt om de skulle leda till att krypteringen försvagas eller försämras.[23]

14. I artikel 52.1 i stadgan föreskrivs också att varje begränsning i utövandet av en grundläggande rättighet som garanteras i stadgan ska vara föreskriven i lag. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.[24] För att uppfylla proportionalitetskravet måste det i lagstiftningen föreskrivas tydliga och precisa bestämmelser som reglerar den aktuella åtgärdens räckvidd och tillämplighet och som fastslår minimisäkerhetskrav, så att de personer vars personuppgifter är menligt påverkade får tillräckliga garantier för att uppgifterna är effektivt skyddade mot risken för missbruk.[25] Lagstiftningen måste precisera under vilka omständigheter och på vilka villkor en åtgärd för behandling av personuppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strikt nödvändigt.[26] Såsom EU-domstolen har klargjort är behovet av sådana skyddsåtgärder desto större när personuppgifter omfattas av automatiserad behandling och när skyddet av den särskilda kategori av personuppgifter som är känsliga uppgifter står på spel.[27]

15. Förslaget skulle begränsa utövandet av de rättigheter och skyldigheter som föreskrivs i artiklarna 5.1, 5.3 och 6.1 i direktiv 2002/58/EG (nedan kallat *direktivet om integritet och elektronisk kommunikation*)[28] i den mån det är nödvändigt för att verkställa de spårningsorder som utfärdats i enlighet med kapitel 1 avsnitt 2 i förslaget. EDPB och EDPS anser därför att det är nödvändigt att bedöma förslaget inte bara mot bakgrund av stadgan och dataskyddsförordningen, utan även mot bakgrund av artiklarna 5, 6 och 15.1 i direktivet om integritet och elektronisk kommunikation.

[21] Ibid., punkt 40.
[22] Se FN:s råd för mänskliga rättigheter, resolution 47/16 om främjande, skydd och åtnjutande av mänskliga rättigheter på internet, UN Doc. A/HRC/RES/47/16 (26 juli 2021).
[23] Se även skäl 25 i interimsförordningen.
[24] Se ”Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit”, 11 april 2019, tillgänglig på https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] EU-domstolen, förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., punkt 132.
[26] Ibid.
[27] Ibid.
[28] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), ändrat genom direktiv 2006/24/EG och direktiv 2009/136/EG.

4. SÄRSKILDA KOMMENTARER

4.1 Förhållande till befintlig lagstiftning

4.1.1 Förhållande till den allmänna dataskyddsförordningen och direktivet om integritet och elektronisk kommunikation

16. I förslaget anges att det inte påverkar tillämpningen av de regler som följer av andra unionsakter, särskilt den allmänna dataskyddsförordningen [29] och direktivet om integritet och elektronisk kommunikation. I motsats till interimsförordningen föreskrivs i förslaget inte något uttryckligt tillfälligt undantag från, utan en begränsning av utövandet av de rättigheter och skyldigheter som fastställs i artiklarna 5.1, 5.3 och 6.1 i direktivet om integritet och elektronisk kommunikation. Det bör dessutom noteras att det i interimsförordningen föreskrivs ett undantag enbart från bestämmelserna i artiklarna 5.1 och 6.1 och inte från artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

17. I förslaget hänvisas vidare till artikel 15.1 i direktivet om integritet och elektronisk kommunikation, som gör det möjligt för medlemsstaterna att anta lagstiftningsåtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som föreskrivs i artiklarna 5 och 6 i det direktivet när en sådan begränsning utgör en nödvändig, lämplig och proportionell åtgärd i ett demokratiskt samhälle, bland annat för att förebygga, utreda, upptäcka och lagföra brott. Enligt förslaget tillämpas artikel 15.1 i direktivet om integritet och elektronisk kommunikation analogt när förslaget begränsar utövandet av de rättigheter och skyldigheter som föreskrivs i artiklarna 5.1, 5.3 och 6.1 i direktivet om integritet och elektronisk kommunikation.

18. EDPB och EDPS påminner om att EU-domstolen har klargjort att artikel 15.1 i direktivet om integritet och elektronisk kommunikation ska tolkas restriktivt, vilket innebär att det undantag från principen om konfidentialitet vid kommunikation som medges i artikel 15.1 måste förbli ett undantag och inte får bli regel. [30] Såsom beskrivs närmare i detta gemensamma yttrande anser EDPB och EDPS att förslaget inte uppfyller kraven på (strikt) nödvändighet, effektivitet och proportionalitet. Dessutom drar EDPB och EDPS slutsatsen att förslaget skulle innebära att ingrepp i konfidentialiteten vid kommunikation i själva verket kan bli regel snarare än förbli undantag.

4.1.2 Förhållande till förordning (EU) 2021/1232 och inverkan på frivillig spårning av sexuella övergrepp mot barn på nätet

19. Enligt artikel 88 i förslaget skulle interimsförordningen upphävas. I den förordningen föreskrivs ett tillfälligt undantag från vissa bestämmelser i direktivet om integritet och elektronisk kommunikation för att göra det möjligt för leverantörer av nummeroberoende interpersonella kommunikationstjänster att använda teknik för spårning av material med sexuella övergrepp mot barn och kontaktsökning med barn. Från och med den dag då den föreslagna förordningen börjar tillämpas skulle det således inte finnas något undantag från direktivet om integritet och elektronisk

[29] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES) (EUT L 119, 4.5.2016, s. 1).
[30] Domstolens dom av den 21 december 2016 i de förenade målen C-203/15 och C-698/15, Tele2 Sverige AB och Watson, punkt 89.

kommunikation som skulle göra det möjligt för sådana leverantörer att frivilligt spåra sexuella övergrepp mot barn på nätet.

20. Med tanke på att de spårningsskyldigheter som införs genom förslaget endast skulle gälla mottagare av spårningsorder, skulle det vara viktigt att i den föreslagna förordningen klargöra att frivillig användning av teknik för att spåra material med sexuella övergrepp mot barn och kontaktsökning av barn endast är tillåten i den mån den är tillåten enligt direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen. Detta skulle till exempel innebära att leverantörer av nummeroberoende interpersonella kommunikationstjänster skulle hindras från att använda sådan teknik på frivillig basis, såvida detta inte är tillåtet enligt den nationella lagstiftning som införlivar direktivet om integritet och elektronisk kommunikation, i enlighet med artikel 15.1 i direktivet om integritet och elektronisk kommunikation och stadgan.

21. Mer allmänt skulle den föreslagna förordningen gynnas av ytterligare tydlighet när det gäller statusen för frivillig spårning av sexuella övergrepp mot barn på nätet efter den dag då den föreslagna förordningen börjar tillämpas, och av övergången från det system för frivillig spårning som fastställs i interimsförordningen till de spårningsskyldigheter som fastställs i den föreslagna förordningen. Till exempel rekommenderar EDPB och EDPS att det klargörs att den föreslagna förordningen inte skulle tillhandahålla någon laglig grund för behandling av personuppgifter enbart i syfte att spåra sexuella övergrepp mot barn på nätet på frivillig basis.

4.2 Laglig grund enligt den allmänna dataskyddsförordningen

22. Förslaget syftar till att fastställa en laglig grund, i den mening som avses i den allmänna dataskyddsförordningen, för behandling av personuppgifter för spårning av material med sexuella övergrepp mot barn och gromning. I motiveringen anges följande: ”När det gäller sådan obligatorisk spårningsverksamhet som inbegriper behandling av personuppgifter fastställs i förslaget, särskilt när det gäller spårningsorder som utfärdas på grundval av denna, att grunden för denna behandling är artikel 6.1 c i dataskyddsförordningen, dvs. behandling av personuppgifter som är nödvändig för att fullgöra en rättslig förpliktelse som enligt unionsrätten eller medlemsstaternas lagstiftning åvilar den personuppgiftsansvarige.”[31]

23. EDPB och EDPS välkomnar kommissionens beslut att undanröja den rättsosäkerhet när det gäller den rättsliga grunden för behandlingen av personuppgifter som har uppstått inom ramen för interimsförordningen. EDPB och EDPS instämmer också i kommissionens slutsats att konsekvenserna av införandet av spårningsåtgärder är alltför långtgående och allvarliga för att överlåta på tjänsteleverantörerna att besluta huruvida sådana åtgärder ska vidtas.[32] Samtidigt noterar EDPB och EDPS att en rättslig grund som ålägger tjänsteleverantörer att ingripa i de grundläggande rättigheterna till dataskydd och privatliv endast kommer att vara giltig om den uppfyller villkoren i artikel 52.1 i stadgan, vilket analyseras i följande avsnitt.

4.3 Skyldigheter avseende riskbedömning och riskreducering

24. Enligt kapitel II avsnitt 1 i förslaget är värdtjänstleverantörer och leverantörer av interpersonella kommunikationstjänster skyldiga att för varje sådan tjänst som de erbjuder identifiera, analysera och bedöma risken för användning av tjänsten för sexuella övergrepp mot barn på nätet, och därefter

[31] Ibid, s. 4.
[32] Jfr förslaget, COM(2022) 209 final, s. 14.

försöka minimera den identifierade risken genom att vidta ”rimliga begränsningsåtgärder, som ska anpassas till den risk som identifieras”.

25. EDPB och EDPS noterar att leverantören vid genomförandet av en riskbedömning särskilt bör beakta de faktorer som förtecknas i artikel 3.2 a–e i förslaget, däribland de förbud och restriktioner som fastställs i leverantörens villkor, det sätt på vilket användarna använder tjänsten och hur detta påverkar denna risk, det sätt på vilket leverantören har utformat och driver tjänsten, inbegripet affärsmodell, styrning och relevanta system och processer, och hur detta påverkar den risken. När det gäller risken för kontaktsökning med barn föreslås att följande faktorer bör beaktas: I vilken utsträckning tjänsten används eller sannolikt kommer att användas av barn. Åldersgrupperna och risken för kontaktsökning i förhållande till dessa åldersgrupper. Tillgången till funktioner som möjliggör sökning av användare. Funktioner som gör det möjligt för användare att direkt kontakta andra användare, särskilt genom privat kommunikation och funktioner som gör det möjligt för användare att dela bilder eller videoklipp med andra användare.

26. EDPB och EDPS erkänner att dessa kriterier verkar vara relevanta, men är ändå oroade över att sådana kriterier ger ett tämligen brett utrymme för tolkning och bedömning. Flera kriterier beskrivs i mycket allmänna ordalag (t.ex. ”[d]et sätt på vilket användarna använder tjänsten och hur detta påverkar denna risk”) eller avser grundläggande funktioner som är gemensamma för många onlinetjänster (t.ex. ”gör det möjligt för användare att dela bilder eller videoklipp med andra användare”). Kriterierna förefaller därför tendera att bli föremål för en subjektiv (snarare än objektiv) bedömning.

27. Enligt EDPB och EDPS gäller detsamma för de riskbegränsningsåtgärder som ska vidtas i enlighet med artikel 4 i förslaget. Åtgärder som att genom lämpliga tekniska och operativa åtgärder och bemanning anpassa leverantörens innehållsmodererings- eller rekommendationssystem förefaller relevanta för att minska den identifierade risken. Om dessa kriterier tillämpas inom ramen för en komplicerad riskbedömningsprocess och kombineras med abstrakta och vaga termer för att beskriva den godtagbara risknivån (t.ex. ”betydande utsträckning”) uppfyller de emellertid inte de kriterier för rättssäkerhet och förutsebarhet som krävs för att motivera ett intrång i konfidentialiteten vid kommunikation mellan privatpersoner, vilket utgör ett tydligt intrång i den grundläggande rätten till privatliv och yttrandefrihet.

28. Leverantörer har inte rätt att göra intrång i konfidentialiteten vid kommunikation som en del av sina strategier för riskbedömning och riskbegränsning innan de tar emot en spårningsorder, men det finns en direkt koppling mellan riskbedömnings- och begränsningsskyldigheterna och de därav följande spårningsskyldigheterna. Enligt artikel 7.4 i förslaget är utfärdandet av en spårningsorder beroende av att det finns bevis för en betydande risk för att den berörda tjänsten kan användas för sexuella övergrepp mot barn på nätet. Innan en spårningsorder utfärdas måste en komplicerad process följas med deltagande av leverantörer, samordningsmyndigheten och den rättsliga eller andra oberoende administrativa myndighet som ansvarar för att utfärda ordern. För det första måste leverantörerna bedöma risken för att deras tjänster används för sexuella övergrepp mot barn på nätet (artikel 3 i förslaget) och utvärdera möjliga riskbegränsningsåtgärder (artikel 4 i förslaget) för att minska denna risk. Resultaten av detta arbete ska sedan rapporteras till den behöriga samordnande myndigheten (artikel 5 i förslaget). Om riskbedömningen visar att en betydande risk kvarstår trots insatserna för att minska den, ska den samordnande myndigheten höra leverantören om ett utkast till begäran om utfärdande av en spårningsorder och ge leverantören möjlighet att lämna synpunkter. Vid spårning av gromning är leverantören dessutom skyldig att lägga fram en genomförandeplan, inklusive ett yttrande från den behöriga dataskyddsmyndigheten. Om samordningsmyndigheten fortsätter ärendet, begärs en spårningsorder som så småningom utfärdas av en domstol eller annan oberoende administrativ myndighet. Därför är den inledande riskbedömningen och de åtgärder som valts för att

begränsa den identifierade risken en avgörande grund för den samordnande myndighetens och den behöriga rättsliga eller administrativa myndighetens bedömning av huruvida en spårningsorder är nödvändig.

29. EDPB och EDPS noterar de komplexa steg som leder fram till utfärdandet av en spårningsorder, vilka inbegriper en inledande riskbedömning av leverantören och leverantörens förslag till riskbegränsningsåtgärder, samt leverantörens fortsatta samverkan med den behöriga samordnande myndigheten. EDPB och EDPS anser att det finns en betydande möjlighet för leverantören att påverka resultatet av processen. I detta avseende noterar EDPB och EDPS att det i skäl 17 i förslaget föreskrivs att leverantörer som en del av riskrapporteringen bör kunna ange om de är ”villiga och beredda” att eventuellt få en spårningsorder utfärdad till sig. Det kan därför inte antas att alla leverantörer kommer att försöka undvika utfärdandet av spårningsorder för att bevara konfidentialiteten i användarnas kommunikation genom att vidta de åtgärder som är effektivast och samtidigt medför ett så litet intrång som möjligt, särskilt när sådana begränsningsåtgärder påverkar leverantörens näringsfrihet enligt artikel 16 i stadgan.

30. EDPS och EDPB vill betona att rättssäkerhetsgarantier aldrig helt kan ersätta materiella skyddsåtgärder. Denna komplexa process, som leder till ett eventuellt utfärdande av en spårningsorder, bör därför åtföljas av tydliga materiella skyldigheter. EDPB och EDPS anser att förslaget saknar klarhet om flera viktiga aspekter (t.ex. begreppen ”betydande risk”, ”betydande utsträckning” osv.), vilket inte kan avhjälpas genom att det finns flera nivåer av rättssäkerhetsgarantier. Detta är desto viktigare med tanke på att de enheter som ansvarar för att tillämpa dessa skyddsåtgärder (t.ex. leverantörer, rättsliga myndigheter osv.) har ett stort utrymme för skönsmässig bedömning när det gäller hur de rättigheter som står på spel i varje enskilt fall ska balanseras. Med tanke på de omfattande intrång i de grundläggande rättigheterna som skulle följa av att förslaget antas, bör lagstiftaren se till att förslaget ger större klarhet om när och var sådana intrång är tillåtna. EDPB och EDPS är medvetna om att lagstiftningsåtgärder inte kan vara alltför preskriptiva, utan måste medge viss flexibilitet i den praktiska tillämpningen, men anser att förslagets nuvarande lydelse lämnar alltför stort utrymme för potentiellt missbruk på grund av avsaknaden av tydliga materiella normer.

31. Med tanke på den potentiellt betydande inverkan på ett mycket stort antal registrerade (dvs. potentiellt alla användare av interpersonella kommunikationstjänster) betonar EDPB och EDPS behovet av en hög nivå av rättssäkerhet, tydlighet och förutsägbarhet i lagstiftningen för att säkerställa att de föreslagna åtgärderna verkligen är effektiva när det gäller att uppnå det mål som eftersträvas och samtidigt är så lite skadliga som möjligt för de grundläggande rättigheter som står på spel.

4.4 Villkor för utfärdande av spårningsorder

32. I artikel 7 i förslaget föreskrivs att samordningsmyndigheten i etableringslandet ska ha befogenhet att begära att den behöriga rättsliga myndigheten eller en annan oberoende administrativ myndighet i den medlemsstaten utfärdar en spårningsorder som ålägger en värdtjänstleverantör eller en leverantör av interpersonella kommunikationstjänster att vidta de åtgärder som anges i artikel 10 för att spåra sexuella övergrepp mot barn på nätet på en viss tjänst.

33. EDPB och EDPS tar vederbörlig hänsyn till följande villkor som ska vara uppfyllda innan en spårningsorder utfärdas:

a. Bevis föreligger för betydande risk för att tjänsten används i samband med sexuella övergrepp mot barn på nätet i den mening som avses i punkterna 5, 6 och 7, beroende på vad som är tillämpligt.

b. Skälen till att spårningsordern utfärdas uppväger de negativa konsekvenserna för alla berörda parters rättigheter och legitima intressen, särskilt med beaktande av behovet av att säkerställa en rättvis balans mellan dessa parters grundläggande rättigheter.

34. Innebörden av betydande risk anges i artikel 7.5 och följande, beroende på vilken typ av spårningsorder som övervägs. Betydande risk ska anses föreligga vid spårningsorder avseende spårning av känt material med sexuella övergrepp mot barn om

a. det är sannolikt, trots alla begränsningsåtgärder som leverantören kan ha vidtagit eller kommer att vidta, att tjänsten används i betydande utsträckning för att sprida känt material med sexuella övergrepp mot barn, och

b. det finns bevis för att tjänsten, eller en jämförbar tjänst om tjänsten ännu inte har erbjudits i unionen vid datumet för begäran om utfärdande av spårningsordern, har använts under de senaste tolv månaderna och i betydande omfattning för att sprida känt material med sexuella övergrepp mot barn.

35. För att utfärda en spårningsorder för okänt material med sexuella övergrepp mot barn måste sannolikheten och de faktiska bevisen avse okänt material med sexuella övergrepp mot barn, och en tidigare spårningsorder för känt material med sexuella övergrepp måste ha utfärdats och ha lett till ett betydande antal rapporter från leverantören (artikel 7.6 i förslaget). För en spårningsorder som rör gromning ska betydande risk anses föreligga om leverantören uppfyller kraven som leverantör av interpersonella kommunikationstjänster, tjänsten används i betydande omfattning för kontaktsökning med barn och det finns bevis för att tjänsten i betydande omfattning har använts för kontaktsökning med barn (artikel 7.7 i förslaget).

36. EDPB och EDPS konstaterar att även med specifikationerna i artikel 7.5–7.7 i förslaget utgörs villkoren för utfärdande av en spårningsorder till övervägande del av vaga rättsliga begrepp, såsom ”betydande utsträckning”, ”betydande antal”, och de är delvis upprepande, eftersom bevis för tidigare övergrepp ofta kommer att bidra till att fastställa sannolikheten för framtida övergrepp.

37. I förslaget planeras ett system där man, när beslut fattas om huruvida en spårningsorder är nödvändig, måste fatta ett prediktivt beslut om den framtida användningen av en tjänst för sexuella övergrepp mot barn på nätet. Det är därför förståeligt att de faktorer som anges i artikel 7 har en prognostisk karaktär. Användningen av vaga begrepp i förslaget gör det dock svårt för tjänsteleverantörer, för den behöriga rättsliga myndigheten eller andra oberoende administrativa myndigheter med motsvarande befogenhet, att tillämpa de rättsliga krav som införs genom förslaget på ett förutsägbart och icke godtyckligt sätt. EDPB och EDPS är oroade över att dessa breda och vaga begrepp kommer att leda till bristande rättssäkerhet och även kommer att leda till betydande skillnader i det konkreta genomförandet av förslaget i hela unionen, beroende på vilka tolkningar som kommer att ges av begrepp som ”sannolikhet” och ”betydande utsträckning” av rättsliga eller andra oberoende administrativa myndigheter i medlemsstaterna. Ett sådant resultat skulle inte vara godtagbart mot bakgrund av att bestämmelserna om spårningsorder för leverantörer av interpersonella kommunikationstjänster kommer att utgöra ”begränsningar” av den princip om konfidentialitet vid kommunikation som fastställs i artikel 5 i direktivet om integritet och elektronisk kommunikation, och deras tydlighet och förutsebarhet är därför av yttersta vikt för att säkerställa att dessa begränsningar tillämpas på ett enhetligt sätt i hela unionen.

4.5 Analys av de planerade åtgärdernas nödvändighet och proportionalitet[33]

38. Som anges ovan kan tre typer av spårningsorder utfärdas: spårningsorder om spridning av känt material med sexuella övergrepp mot barn (artikel 7.5 i förslaget), spårningsorder om spridning av nytt material med sexuella övergrepp mot barn (artikel 7.6 i förslaget) och spårningsorder om kontaktsökning med barn (artikel 7.7 i förslaget). Normalt skulle det krävas olika teknik för varje spårningsorder, för det praktiska genomförandet. Det innebär att de skulle innebära olika grad av intrång och därmed olika inverkan på rätten till privatliv och skydd av personuppgifter.

39. Teknik för att spåra känt material med sexuella övergrepp mot barn är oftast en matchningsteknik, i den meningen att den baseras på en befintlig databas över känt material med sexuella övergrepp mot barn, som används för bildjämförelser (inklusive stillbilder från videofilmer). För att möjliggöra matchningen måste de bilder som leverantören behandlar samt bilderna i databasen ha digitaliserats, vanligtvis genom att de konverteras till hashvärden. Denna typ av hashteknik har en uppskattad andel falska positiva resultat på högst 1 av 50 miljarder (dvs. 0,000000002 procent falska positiva resultat).[34]

40. För att spåra nytt material med sexuella övergrepp mot barn används vanligtvis en annan typ av teknik, däribland klassificerare och artificiell intelligens (AI).[35] Deras felfrekvens är dock i allmänhet betydligt större. I konsekvensbedömningsrapporten anges till exempel att det finns teknik för spårning av nytt material med sexuella övergrepp mot barn vars noggrannhetsgrad kan ställas in på 99,9 procent (dvs. 0,1 procent falska positiva resultat), men med den noggrannheten kan de endast identifiera 80 procent av det totala materialet med sexuella övergrepp mot barn i den berörda datamängden.[36]

41. I konsekvensbedömningsrapporten förklaras också att spårning av kontaktsökning med barn i textbaserad kommunikation vanligtvis bygger på mönsterspårning. I konsekvensbedömningsrapporten konstateras att en del av den befintliga tekniken för spårning av gromning har en ”noggrannhetsgrad” på 88 procent.[37] Enligt kommissionen innebär detta att ”av de 100 konversationer som flaggats som möjlig brottslig kontaktsökning med barn kan 12 uteslutas vid granskning [av EU-centrumet, enligt förslaget] och kommer inte att rapporteras till de brottsbekämpande myndigheterna”.[38] Även om förslaget – i motsats till interimsförordningen – skulle vara tillämpligt även på ljudkommunikation, tar konsekvensbedömningsrapporten dock inte upp de tekniska lösningar som skulle kunna användas för att spåra gromning i en sådan miljö.

4.5.1 Spårningens effektivitet

42. Nödvändighet innebär att det behöver göras en faktabaserad bedömning av de planerade åtgärdernas effektivitet för att nå det eftersträvade målet och av huruvida de innebär mindre intrång än andra

---

[33] Se även EDPS snabbvägledning om nödvändighet och proportionalitet, tillgänglig på https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

[34] Se Europeiska kommissionens arbetsdokument, *Konsekvensbedömningsrapport som åtföljer förslaget till Europaparlamentets och rådets förordning om fastställande av bestämmelser för att förebygga och bekämpa sexuella övergrepp mot barn*, SWD(2022) 209 final (nedan kallad *konsekvensbedömningsrapporten* eller *SWD(2022)209final*), s. 281, fotnot 511 (ej översatt till svenska).

[35] Konsekvensbedömningsrapporten, s. 281.

[36] Ibid, s. 282.

[37] Ibid, s. 283.

[38] Förslag COM(2022) 209 final, s. 14, fotnot 32.

alternativ för att uppnå samma mål. [39] En annan faktor som bör beaktas vid proportionalitetsbedömningen av en föreslagen åtgärd är effektiviteten hos befintliga åtgärder utöver den åtgärd som föreslås.[40] Om det redan finns åtgärder för samma eller liknande ändamål bör deras effektivitet bedömas som en del av proportionalitetsbedömningen. Utan en sådan bedömning av effektiviteten hos befintliga åtgärder med samma eller liknande syfte kan proportionalitetstestet för en ny åtgärd inte anses ha utförts i vederbörlig ordning.

43. Om värdtjänstleverantörer och leverantörer av interpersonella kommunikationstjänster spårar material med sexuella övergrepp mot barn eller gromning kan detta bidra till det övergripande målet att förebygga och bekämpa sexuella övergrepp mot barn och spridning på nätet av material med sexuella övergrepp mot barn. Samtidigt ger behovet av att bedöma effektiviteten hos de åtgärder som föreskrivs i förslaget upphov till tre nyckelfrågor:

- Kan åtgärderna för att spåra sexuella övergrepp mot barn på nätet enkelt kringgås?
- Vilken effekt kommer spårningsverksamheten att få på de brottsbekämpande myndigheternas åtgärder?[41]
- Hur skulle förslaget minska rättsosäkerheten?

44. Det ankommer inte på EDPB och EDPS att besvara dessa frågor i detalj. EDPB och EDPS noterar dock att varken konsekvensbedömningsrapporten eller förslaget tar upp dessa frågor fullt ut.

45. När det gäller möjligheten att kringgå spårning av material med sexuella övergrepp mot barn bör det noteras att det för närvarande inte verkar finnas någon teknisk lösning för att spåra sådant material som delas i krypterad form. Därför kan all spårningsverksamhet – även genomsökning av klienter i syfte att kringgå totalsträckskryptering som erbjuds av leverantören[42] – enkelt kringgås genom kryptering av innehållet med hjälp av en separat applikation innan det skickas eller laddas upp. De spårningsåtgärder som föreslås i förslaget kan således få mindre effekt på spridningen av material med sexuella övergrepp mot barn på internet än vad man kanske skulle kunna hoppas på.

46. Dessutom förväntar sig kommissionen en ökning av antalet rapporter om sexuella övergrepp mot barn till brottsbekämpande myndigheter i och med antagandet av de spårningsskyldigheter som införs genom förslaget.[43] Varken förslaget eller konsekvensbedömningsrapporten förklarar dock hur detta kommer att avhjälpa de nuvarande bristerna. Med tanke på de brottsbekämpande myndigheternas begränsade resurser förefaller det nödvändigt att få en bättre förståelse av huruvida ett ökat antal rapporter skulle få en meningsfull inverkan på brottsbekämpande verksamhet mot sexuella övergrepp mot barn. Under alla omständigheter vill EDPB och EDPS betona att sådana rapporter bör bedömas snabbt för att säkerställa att ett beslut om det rapporterade materialets straffrättsliga relevans fattas så tidigt som möjligt och för att i möjligaste mån begränsa lagringen av irrelevanta uppgifter.

---

[39] EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, 11 april 2017, s. 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), s. 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), s. 11 (ej översatt till svenska).

[41] Enligt konsekvensbedömningsrapporten, bilaga II, s. 132, uttryckte 85,71 procent av de svarande i brottsbekämpningsundersökningen sin oro över den ökade mängden material med sexuella övergrepp mot barn under det senaste årtiondet och bristen på resurser (dvs. mänskliga, tekniska).

[42] Se vidare i avsnitt 4.10 nedan.

[43] Se bland annat konsekvensbedömningsrapporten, bilaga 3, SWD (2022) 209 final, s. 176.

4.5.2 Ingen åtgärd som innebär mindre intrång

47. Om man antar att de positiva effekter av spårning av material med sexuella övergrepp mot barn och gromning som kommissionen planerar skulle kunna förverkligas, måste spårningen vara den åtgärd som medför minst intrång av en uppsättning lika effektiva åtgärder. I artikel 4 i förslaget föreskrivs att leverantörer som ett första steg bör överväga att vidta riskbegränsningsåtgärder för att minska risken för att deras tjänster används för sexuella övergrepp mot barn på nätet, så att den hamnar under det tröskelvärde som motiverar utfärdande av en spårningsorder. Om det finns riskbegränsningsåtgärder som skulle kunna leda till en betydande minskning av den mängd gromning eller material med sexuella övergrepp mot barn som utbyts inom den berörda tjänsten, skulle sådana åtgärder ofta innebära mindre intrång än en spårningsorder[44]. Om den berörda leverantören underlåter att vidta sådana åtgärder på frivillig basis bör det därför vara möjligt för den behöriga oberoende administrativa myndigheten eller rättsliga myndigheten att göra det obligatoriskt att vidta och verkställa riskbegränsningsåtgärder, i stället för att utfärda en spårningsorder. EDPP och EDPS menar att det inte är tillräckligt att artikel 5.4 i förslaget gör det möjligt för den samordnande myndigheten att ”kräva” av leverantören att införa, se över, avbryta eller utvidga riskbegränsningsåtgärder, eftersom ett sådant krav inte skulle gå att verkställa självständigt. Bristande efterlevnad skulle enbart ge ”påföljder” i form av ett beslut om en spårningsorder.

48. EDPB och EDPS anser därför att den samordnande myndigheten eller den behöriga oberoende administrativa eller rättsliga myndigheten uttryckligen bör ges befogenhet att vidta mindre inkräktande begränsningsåtgärder innan de utfärdar, eller i stället för att utfärda, en spårningsorder.

4.5.3 Proportionalitet i strikt mening

49. För att en åtgärd ska vara förenlig med proportionalitetsprincipen i artikel 52.1 i stadgan bör de fördelar som följer av åtgärden inte uppvägas av de nackdelar som åtgärden medför för utövandet av de grundläggande rättigheterna. Proportionalitetsprincipen begränsar således myndigheternas utövande av sina befogenheter genom att kräva en avvägning mellan de medel som används och det avsedda syftet (eller det eftersträvade resultatet).[45]

50. För att kunna bedöma en åtgärds inverkan på de grundläggande rättigheterna till privatliv och skydd av personuppgifter är det särskilt viktigt att exakt identifiera [46]

- **åtgärdens räckvidd**, inklusive antalet berörda personer och huruvida den medför ”intrång i säkerheten” (dvs. ingrepp i privatlivet för andra personer än de som berörs av åtgärden),

---

[44] Till exempel skulle man kunna överväga åtgärder som blockering på klientsidan av överföring av material med sexuella övergrepp mot barn genom att förhindra att innehållet i den elektroniska kommunikationen laddas upp och skickas, eftersom detta i vissa fall skulle kunna bidra till att förhindra spridningen av känt material med sexuella övergrepp mot barn.

[45] Se mål C-343/09, Afton Chemical, punkt 45, förenade målen C-92/09 och C-93/09, Volker und Markus Schecke och Hartmut Eifert, punkt 74, målen C-581/10 och C-629/10, Nelson m.fl., punkt 71, mål C-283/11, Sky Österreich, punkt 50, och mål C-101/12, Schaible, punkt 29. Se 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), s. 23 (ej översatt till svenska).

- **åtgärdens omfattning**, inklusive mängden information som samlas in, under hur lång tid, om den åtgärd som granskas kräver insamling och behandling av särskilda uppgiftskategorier,
- **graden av intrång** med hänsyn till arten av den verksamhet som omfattas av åtgärden (om den påverkar verksamhet som omfattas av tystnadsplikt eller ej, förhållandet mellan advokat och klient, vårdverksamhet,) sammanhanget, huruvida åtgärden innebär profilering av de berörda personerna, om behandling innebär att (helt eller delvis) automatiserat beslutsfattande med en ”felmarginal” används,
- om den gäller **utsatta personer** eller ej,
- om den också påverkar **andra grundläggande rättigheter** (till exempel yttrandefriheten som i målen Digital Rights Ireland och Seitlinger m.fl. och Tele2 Sverige och Watson).[47]

51. I detta sammanhang är det också viktigt att notera att effekterna kan vara små för den berörda personen, men ändå betydande eller mycket betydande för samhället som helhet.[48]

52. I alla de tre typerna av spårningsorder (spårning av känt material med sexuella övergrepp mot barn, nytt material med sexuella övergrepp mot barn och gromning) bygger den nuvarande tillgängliga tekniken på automatisk behandling av innehållsdata från alla berörda användare. Den teknik som används för att analysera innehållet är ofta komplex, vanligtvis med användning av AI. Detta innebär att beteendet hos denna teknik kanske inte är helt begripligt för användaren av tjänsten. Dessutom är det känt att den teknik som för närvarande finns tillgänglig, särskilt den för att spåra nytt material med sexuella övergrepp mot barn eller gromning, har förhållandevis hög felfrekvens.[49] Dessutom finns det risk för att rapporteras till EU-centrumet i enlighet med artiklarna 12.1 och 48.1 i förslaget baserat på spårning av ”potentiellt” material med sexuella övergrepp mot barn.

53. Dessutom kan de allmänna villkoren för utfärdande av en spårningsorder enligt förslaget, dvs. som gäller för en hel tjänst och inte bara för utvald kommunikation[50], en varaktighet på upp till 24 månader för känt eller nytt material med sexuella övergrepp mot barn och upp till tolv månader för gromning[51] osv., leda till ett mycket brett tillämpningsområde för ordern i praktiken. Till följd av detta skulle övervakningen i själva verket vara allmän och urskillningslös till sin karaktär och inte vara riktad i praktiken.

54. Mot bakgrund av ovanstående är EDPB och EDPS också oroade över de möjliga dämpande effekterna på utövandet av yttrandefriheten. EDPB och EDPS konstaterar att en sådan dämpande effekt anses bli mer sannolik ju otydligare lagstiftningen är.

55. I avsaknad av den specificitet, precision och tydlighet som krävs för att uppfylla kravet på rättssäkerhet[52] och med tanke på dess breda räckvidd, dvs. alla leverantörer av relevanta informationssamhällstjänster som erbjuder sådana tjänster i unionen,[53] säkerställer förslaget inte att det enbart är en riktad strategi för spårning av material med sexuella övergrepp mot barn och

---

[47] Se även EDPS, yttrande 7/2020 om förslaget till tillfälliga undantag från direktiv 2002/58/EG för att bekämpa sexuella övergrepp mot barn på nätet (10 november 2020), s 9 och följande.
[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), s. 20 (ej översatt till svenska).
[49] Se närmare uppgifter ovan, avsnitt 4.5 och nedan i underavsnitt 4.8.2.
[50] Se artikel 7.1 i förslaget.
[51] Se artikel 7.9 tredje stycket i förslaget.
[52] Jfr EU-domstolens dom i mål C-197/96, Europeiska gemenskapernas kommission mot Frankrike, punkt 15.
[53] Se artikel 1.2 i förslaget.

gromning som kommer att genomföras i praktiken. EDPB och EDPS anser därför att förslaget i praktiken skulle kunna utgöra grunden för en faktisk generell och urskillningslös genomsökning av innehållet i praktiskt taget alla typer av elektronisk kommunikation för alla användare i EU/EES. Till följd av detta kan lagstiftningen leda till att människor avstår från att dela lagligt innehåll av rädsla för att de skulle kunna bli föremål för åtgärder på grundval av sina handlingar.

56. EDPB och EDPS erkänner dock att olika åtgärder för att bekämpa sexuella övergrepp mot barn på nätet kan innebära olika grader av intrång. Inledningsvis konstaterar EDPB och EDPS att den automatiska analysen av tal eller text i syfte att identifiera potentiella fall av kontaktsökning med barn sannolikt kommer att utgöra ett större intrång än matchning av bilder eller videor på grundval av tidigare bekräftade fall av material med sexuella övergrepp mot barn i syfte att spåra spridning av material med sexuella övergrepp mot barn. Dessutom bör man skilja mellan spårning av ”känt material med sexuella övergrepp mot barn” och av ”nytt material med sexuella övergrepp mot barn”. Vidare bör effekterna ytterligare differentieras mellan de åtgärder som riktar sig till värdtjänstleverantörer och de som åläggs leverantörer av interpersonella kommunikationstjänster.

4.5.4 Spårning av känt material med sexuella övergrepp mot barn

57. Enligt skäl 4 skulle förslaget vara ”teknikneutralt”, men både de föreslagna spårningsåtgärdernas effektivitet och deras inverkan på enskilda personer kommer i hög grad att bero på valet av tillämpad teknik och på de utvalda indikatorerna. Detta erkänns av kommissionen i bilaga 8 till konsekvensbedömningsrapporten [54] och bekräftas av andra studier, såsom Europaparlamentets utredningstjänsts riktade alternativa konsekvensbedömning av kommissionens förslag om det tillfälliga undantaget från direktivet om integritet och elektronisk kommunikation i syfte att bekämpa sexuella övergrepp mot barn på nätet från februari 2021. [55]

58. I artikel 10 i förslaget fastställs ett antal krav för den teknik som ska användas för spårningsändamål, särskilt när det gäller dess effektivitet, tillförlitlighet och minst inkräktande inverkan på användarnas rätt till privat- och familjeliv, inbegripet konfidentialitet vid kommunikation, och skydd av personuppgifter.

59. I detta sammanhang noterar EDPB och EDPS att de enda tekniker som i allmänhet verkar kunna uppfylla dessa standarder för närvarande är de som används för att spåra känt material med sexuella övergrepp mot barn, dvs. matchningsteknik som bygger på en databas med hashvärden som referens.

4.5.5 Spårning av tidigare okänt material med sexuella övergrepp mot barn

60. Bedömningen av de åtgärder som syftar till att spåra tidigare okänt (nytt) material med sexuella övergrepp mot barn leder till olika slutsatser om deras effektivitet, tillförlitlighet och begränsning av inverkan på de grundläggande rättigheterna till integritet och dataskydd.

61. För det första omfattar den teknik som för närvarande används för att spåra tidigare okänt material med sexuella övergrepp mot barn klassificerare och AI, vilket förklaras i

[54] Jfr med informationen om falska positiva resultat i bilaga 8 till konsekvensbedömningsrapporten, s. 279 och följande.
[55] Jfr med kommissionens förslag om det tillfälliga undantaget från direktivet om integritet och elektronisk kommunikation för att bekämpa sexuella övergrepp mot barn på nätet: Riktad alternativ konsekvensbedömning (Europaparlamentets utredningstjänst, februari 2021), s. 14 och följande.

konsekvensbedömningsrapporten. En klassificerare är en algoritm som sorterar data i angivna klasser, eller kategorier av information, genom mönsterigenkänning.[56] Dessa tekniker har således olika resultat och effekter när det gäller exakthet, effektivitet och grad av intrång. Samtidigt är de också mer benägna att drabbas av fel.

62. De tekniker som används för att spåra tidigare okänt material med sexuella övergrepp mot barn liknar dem som används för att spåra kontaktsökning med barn, eftersom båda inte bygger på enkel matchningsteknik, utan på prognosmodeller som använder AI-teknik. EDPB och EDPS anser att en hög nivå av försiktighet bör iakttas när man spårar tidigare okänt material med sexuella övergrepp mot barn, eftersom ett fel i systemet skulle få allvarliga konsekvenser för de registrerade, som automatiskt skulle flaggas som att de eventuellt har begått ett mycket allvarligt brott och skulle få sina personuppgifter och uppgifter om sin kommunikation rapporterade.

63. För det andra ger de resultatindikatorer som finns i litteraturen, varav vissa framhålls i den konsekvensbedömningsrapport som åtföljde förslaget[57], mycket lite information om de förutsättningar som användes för beräkningen av dem och deras lämplighet vid verkliga förhållanden, vilket innebär att deras verkliga resultat skulle kunna vara betydligt lägre än vad som förväntas, vilket leder till mindre noggrannhet och en högre andel ”falska positiva resultat”.

64. För det tredje bör resultatindikatorer beaktas i det specifika sammanhang där de relevanta spårningsverktygen används och ge en uttömmande inblick i hur spårningsverktygen fungerar. När algoritmer för artificiell intelligens används på bilder eller text är det väldokumenterat att snedvridning och diskriminering kan förekomma på grund av att vissa befolkningsgrupper inte är representerade i de data som används för att träna algoritmen. Dessa snedvridningar bör identifieras, mätas och reduceras till en godtagbar nivå för att spårningssystemen verkligen ska vara till nytta för samhället som helhet.

65. Även om det har genomförts en studie av den teknik som används för spårning[58] anser EDPB och EDPS att det krävs ytterligare analyser för att bedöma tillförlitligheten hos de befintliga verktygen. Denna analys bör bygga på heltäckande resultatindikatorer och bedöma effekten av potentiella fel under verkliga förhållanden för alla registrerade som berörs av förslaget.

66. Som anges ovan hyser EDPB och EDPS allvarliga tvivel om i vilken utsträckning de rättssäkerhetsgarantier som föreskrivs i artikel 7.6 i förslaget är tillräckliga för att kompensera dessa risker. De noterar dessutom att förslaget använder tämligen abstrakta och vaga termer för att beskriva den godtagbara risknivån (t.ex. ”betydande omfattning”).

67. EDPB och EDPS är oroade över att dessa breda och vaga begrepp kommer att leda till bristande rättssäkerhet och även kommer att leda till stora skillnader i det konkreta genomförandet av förslaget i hela unionen, beroende på de tolkningar som kommer att ges av begrepp som ”sannolikhet” och ”betydande omfattning” av rättsliga eller andra oberoende administrativa myndigheter i medlemsstaterna. Detta är också oroande med tanke på att bestämmelserna om spårningsorder kommer att utgöra ”begränsningar” av den princip om konfidentialitet som fastställs i artikel 5 i direktivet om integritet och elektronisk kommunikation. Därför måste deras tydlighet och förutsägbarhet förbättras i den föreslagna förordningen.

[56] Konsekvensbedömningsrapport, bilaga 8, s. 281.
[57] Konsekvensbedömningsrapport, bilaga 8, s. 281–283.
[58] Konsekvensbedömningsrapporten, s. 279 och följande.

4.5.6 Spårning av kontaktsökning med barn (gromning)

68. EDPB och EDPS konstaterar att de föreslagna åtgärderna för att spåra kontaktsökning med barn (gromning), som inbegriper automatisk analys av tal eller text, sannolikt kommer att utgöra det mest betydande ingreppet i användarnas rätt till privatliv och familjeliv, inbegripet konfidentialitet vid kommunikation, och till skydd av personuppgifter.

69. Medan spårning av känt och till och med nytt material med sexuella övergrepp mot barn kan begränsas till analys av bilder och videor, skulle gromningsspårningen per definition utvidgas till att omfatta all textbaserad (och eventuellt ljudbaserad) kommunikation som omfattas av en spårningsorder. Till följd av detta är ingreppet i den berörda kommunikationens konfidentialitet betydligt större.

70. EDPB och EDPS anser att en allmän och urskillningslös automatiserad analys av textbaserad kommunikation som överförs via interpersonella kommunikationstjänster i syfte att identifiera eventuell kontaktsökning med barn inte uppfyller kraven på nödvändighet och proportionalitet. Även om den teknik som används är begränsad till användningen av indikatorer anser EDPB och EDPS att införandet av en sådan allmän och urskillningslös analys är överdrivet och till och med kan påverka det väsentliga innehållet i den grundläggande rätten till integritet som fastställs i artikel 7 i stadgan.

71. Som redan nämnts kan avsaknaden av materiella garantier i samband med åtgärder för att spåra kontaktsökning med barn inte kompenseras enbart genom rättssäkerhetsgarantier. Problemet med bristen på tillräcklig rättslig klarhet och säkerhet (t.ex. användningen av vaga rättsliga formuleringar som ”betydande omfattning”) är dessutom ännu allvarligare när det gäller automatisk analys av textbaserad personlig kommunikation, jämfört med fotojämförelse baserad på hashteknik.

72. Dessutom anser EDPB och EDPS att den ”dämpande effekten” på yttrandefriheten är särskilt viktig när enskilda personers textkommunikation (eller ljudkommunikation) skannas och analyseras i stor skala. EDPB och EDPS erinrar om att en sådan dämpande effekt anses bli mer sannolik ju mer otydlig lagstiftningen är.

73. Såsom anges i konsekvensbedömningsrapporten [59] och i studien från Europaparlamentets utredningstjänst[60] är dessutom noggrannhetsgraden för teknik för att spåra textbaserad gromning mycket lägre än noggrannhetsgraden för teknik för spårning av känt material med sexuella övergrepp mot barn. [61] Teknik för att spåra gromning är utformad för att analysera och tilldela sannolikhetsbedömningar till varje aspekt av samtalet, och därför anser EDPB och EDPS också att den är felbenägen och sårbar för missbruk.

4.5.7 Slutsats om de planerade åtgärdernas nödvändighet och proportionalitet

74. När det gäller de planerade spårningsåtgärdernas nödvändighet och proportionalitet är EDPB och EDPS särskilt oroade över de åtgärder som planeras för spårning av okänt material med sexuella övergrepp mot barn och kontaktsökning med barn (gromning), på grund av graden av intrång då åtkomst till kommunikationsinnehåll skulle kunna beviljas på ett allmänt sätt, den probabilistiska utformningen och felnivån i samband med sådan teknik.

---

[59] Bilaga 8, konsekvensbedömningsrapport, s. 281–283.
[60] S. 15–18.
[61] Se ovan, punkt 40.

75. Dessutom kan man av EU-domstolens rättspraxis dra slutsatsen att åtgärder som gör det möjligt för offentliga myndigheter att allmänt få tillgång till innehållet i en kommunikation i högre grad påverkar det väsentliga innehållet i de rättigheter som garanteras i artiklarna 7 och 8 i stadgan. Dessa överväganden är särskilt relevanta när det gäller åtgärder för att spåra kontaktsökning med barn enligt förslaget.

76. Under alla omständigheter anser EDPB och EDPS att den inverkan som i synnerhet skapas genom åtgärderna för att spåra kontaktsökning med barn går utöver vad som är strikt nödvändigt och proportionerligt. Dessa åtgärder bör därför tas bort från förslaget.

4.6 Rapporteringsskyldigheter

77. EDPB och EDPS rekommenderar att förteckningen över särskilda rapporteringskrav i artikel 13 i förslaget kompletteras med ett krav på att i rapporten inkludera information om den specifika teknik som gjorde det möjligt för leverantören att få kännedom om det relevanta missbruket av innehåll, om leverantören fick kännedom om de potentiella sexuella övergreppen mot barn efter åtgärder som vidtagits för att verkställa en spårningsorder som utfärdats i enlighet med artikel 7 i förslaget.

4.7 Krav på avlägsnande och blockering

78. En av de åtgärder som planeras i förslaget för att minska riskerna för spridning av material med sexuella övergrepp mot barn är utfärdande av order om avlägsnande och blockering, vilket skulle tvinga leverantörer att avlägsna eller blockera material med sexuella övergrepp mot barn på nätet eller göra det oåtkomligt.[62]

79. Även om avlägsnandeorders inverkan på dataskyddet och kommunikationens integritet är relativt begränsad erinrar EDPB och EDPS som en allmän anmärkning om den övergripande princip som ska följas, att alla sådana åtgärder bör vara så riktade som möjligt.

80. Samtidigt uppmärksammar EDPB och EDPS det faktum att leverantörer av internetanslutningstjänster endast har tillgång till den exakta webbadressen för innehåll om detta innehåll görs tillgängligt i tydlig text. Varje gång innehåll görs tillgängligt via HTTPS kommer leverantören av internetanslutningstjänster inte att ha tillgång till den exakta webbadressen, såvida den inte bryter krypteringen av kommunikationen. EDPB och EDPS betvivlar därför att blockeringsåtgärderna är effektiva och anser att det skulle vara oproportionerligt att kräva att leverantörer av internetanslutningstjänster ska dekryptera kommunikation online för att blockera dem som rör material med sexuella övergrepp mot barn.

81. Mer allmänt bör det dessutom noteras att blockering av (eller förhindrad åtkomst till) en digital artikel är en åtgärd som genomförs på nätnivå och att detta kan visa sig vara ineffektivt, om det finns flera (eventuellt liknande och inte identiska) kopior av samma föremål. Vidare kan en sådan åtgärd visa sig vara oproportionerlig om blockeringen påverkar andra, inte olagliga, digitala föremål när de lagras på samma server som gjorts oåtkomlig med hjälp av nätkommandon (t.ex. IP-adress eller svartlistning av DNS). Dessutom är inte alla nätverksstrategier för blockering lika effektiva, och vissa kan lätt kringgås med ganska grundläggande tekniska färdigheter.

[62] Förslaget, artiklarna 14 och 16.

82. Slutligen bör de samordnande myndigheternas befogenheter när det gäller utfärdande av blockeringsorder klargöras i den föreslagna förordningen. I den nuvarande lydelsen av artiklarna 16.1 och 17.1 är det till exempel oklart om de samordnande myndigheterna har befogenhet att utfärda eller endast att begära utfärdande av blockeringsorder.[63]

4.8 Relevant teknik och skyddsåtgärder

4.8.1 Inbyggt dataskydd och dataskydd som standard

83. De krav i förslaget som gäller den teknik som ska användas för att spåra material med sexuella övergrepp mot barn och kontaktsökning av barn förefaller inte vara tillräckligt stränga. EDPB och EDPS har särskilt noterat att förslaget – i motsats till motsvarande bestämmelser i interimsförordningen[64] – inte innehåller någon uttrycklig hänvisning till principen om inbyggt dataskydd och dataskydd som standard och inte föreskriver att teknik som används för att skanna text i kommunikation inte får kunna härleda innehållet i meddelandena. I artikel 10.3 b i förslaget föreskrivs endast att tekniken inte får ”utvinna” annan information från relevant kommunikation än sådan information som är absolut nödvändig för spårning. Denna standard förefaller emellertid inte vara tillräckligt strikt, eftersom det kan vara möjligt att *härleda* annan information från innehållet i ett meddelande utan att *utvinna* information ur den som sådan.

84. Följaktligen rekommenderar EDPS och EDPB att det i förslaget ska införas ett skäl där det anges att den princip om inbyggt dataskydd och dataskydd som standard som fastställs i artikel 25 i förordning (EU) 2016/679 är tillämplig på den teknik som regleras i artikel 10 i förslaget genom lag och därför inte behöver upprepas i lagtexten. Dessutom bör artikel 10.3 b ändras för att inte enbart säkerställa att ingen annan information utvinns, utan också att den inte härleds, vilket för närvarande föreskrivs i artikel 3.1 b i interimsförordningen.

4.8.2 Teknikens tillförlitlighet

85. Förslaget förutsätter att flera typer av tekniska lösningar kan användas av tjänsteleverantörer för att verkställa spårningsorder. I förslaget förutsätts i synnerhet att system för artificiell intelligens finns tillgängliga och fungerar för att spåra okänt material med sexuella övergrepp mot barn och för att spåra kontaktsökning med barn,[65] och att de skulle kunna betraktas som den senaste tekniken av vissa samordnande myndigheter. Förslagets effektivitet är beroende av att dessa tekniska lösningar är tillförlitliga, men det finns mycket lite information om den allmänna och systematiska användningen av dessa tekniker, vilken kräver noggranna överväganden.

86. Även om EDPB och EDPS var tvungna att använda dem i sin proportionalitetsbedömning, på grund av bristen på alternativ, måste det noteras att de resultatindikatorer för spårningsteknik som nämns i den konsekvensbedömning som åtföljde förslaget ger mycket lite information om hur de har bedömts och om de återspeglar den berörda teknikens verkliga prestanda. Det finns ingen information om de

---

[63] Artikel 16.1 i förslaget har följande lydelse: ”Den samordnande myndigheten i etableringslandet ska ha befogenhet att begära att den behöriga rättsliga myndigheten i den medlemsstat som har utsett den eller en oberoende administrativ myndighet i den medlemsstaten ska utfärda en blockeringsorder […]”, medan artikel 17.1 har följande lydelse: ”Den samordnande myndigheten i etableringslandet ska utfärda de blockeringsorder som avses i artikel 16 […]” (min kursivering).

[64] Interimsförordningen, artikel 3.1 b.

[65] Se konsekvensbedömningsrapporten, s. 281–282.

tester eller riktmärken som teknikleverantörerna använder för att mäta dessa prestanda. Utan sådan information är det inte möjligt att upprepa testerna eller utvärdera resultatförklaringarnas giltighet. I detta avseende bör det noteras att även om resultatindikatorerna skulle kunna tolkas som att vissa spårningsverktyg har en hög grad av noggrannhet (till exempel är noggrannheten hos vissa verktyg för gromning 88 procent),[66] bör dessa indikatorer beaktas mot bakgrund av den planerade praktiska användningen av spårningsverktygen och hur allvarliga de risker är som en felaktig bedömning av ett visst material skulle medföra för de berörda registrerade. Dessutom anser EDPB och EDPS att med en sådan högriskbehandling utgör en felfrekvens på 12 procent en hög risk för registrerade som har varit föremål för falska positiva resultat, även om det finns skyddsåtgärder för att förhindra falska rapporter till brottsbekämpande myndigheter. Det är högst osannolikt att tjänsteleverantörerna skulle kunna avsätta tillräckliga resurser för att granska en sådan procentandel falska positiva resultat.

87. Som tidigare nämnts[67] bör resultatindikatorer ge en uttömmande inblick i hur spårningsverktygen fungerar. När algoritmer för artificiell intelligens används på bilder eller text är det väldokumenterat att snedvridning och diskriminering kan förekomma på grund av att vissa befolkningsgrupper inte är representerade i de data som används för att träna algoritmen. Dessa snedvridningar bör identifieras, mätas och reduceras till en godtagbar nivå för att spårningssystemen verkligen ska vara lönsamma för samhället som helhet.

88. Även om det har genomförts en studie av den teknik som används för spårning[68] anser EDPB och EDPS att det krävs ytterligare analyser för att göra en oberoende bedömning av befintliga verktygens tillförlitlighet i verkliga användningsfall. Denna analys bör bygga på heltäckande resultatindikatorer och bedöma effekten av potentiella fel under verkliga förhållanden för alla registrerade som berörs av förslaget. Eftersom denna teknik är den grund som förslaget bygger på anser EDPB och EDPS att denna analys är av yttersta vikt för bedömningen av förslagets lämplighet.

89. EDPB och EDPS noterar också att förslaget inte definierar teknikspecifika krav, vare sig när det gäller felfrekvens, användning av klassificerare och validering av dem, eller andra begränsningar. Därmed överlåts utvecklingen av sådana kriterier till den praktiska tillämpningen när proportionaliteten i användningen av en viss teknik bedöms, vilket ytterligare bidrar till bristen på precision och tydlighet.

90. Med tanke på hur viktiga konsekvenserna är för de registrerade i fall av falska positiva resultat anser EDPB och EDPS att andelen falska positiva resultat måste reduceras till ett minimum, och att dessa system måste utformas samtidigt som man beaktar att den stora majoriteten av den elektroniska kommunikationen inte omfattar något material med sexuella övergrepp mot barn eller kontaktsökande med barn, och att även en mycket låg andel falska positiva resultat kommer att innebära ett mycket stort antal falska positiva resultat med tanke på den mängd uppgifter som kommer att bli föremål för spårning. Mer allmänt är EDPB och EDPS också oroade över att resultaten av de tillgängliga verktyg som anges i konsekvensbedömningsrapporten inte återspeglar exakta och jämförbara indikatorer för falska positiva och falska negativa värden, och anser att jämförbara och meningsfulla resultatindikatorer för dessa tekniker bör utfärdas innan de anses vara tillgängliga och effektiva.

---

[66] Ibid, s. 283.
[67] Se punkterna 63–64 ovan.
[68] Se konsekvensbedömningsrapporten, s. 279 och följande.

4.8.3 Genomsökning av ljudkommunikation

91. I motsats till interimsförordningen[69] utesluter förslaget inte genomsökning av ljudkommunikation i samband med spårning av gromning från sitt tillämpningsområde.[70] EDPB och EDPS anser att genomsökning av ljudkommunikation är särskilt inkräktande, eftersom det normalt skulle kräva aktiv, fortlöpande och direkt avlyssning. I vissa medlemsstater åtnjuter det talade ordet dessutom ett särskilt skydd.[71] Eftersom allt innehåll i ljudkommunikationen i princip skulle behöva analyseras kommer denna åtgärd dessutom sannolikt att påverka det väsentliga innehållet i de rättigheter som garanteras i artiklarna 7 och 8 i stadgan. Denna spårningsmetod bör därför inte omfattas av de spårningsskyldigheter som fastställs i den föreslagna förordningen, både när det gäller röstmeddelanden och direktkommunikation, särskilt mot bakgrund av att den konsekvensbedömningsrapport som åtföljde förslaget inte identifierade några specifika risker eller förändringar i hotbilden som skulle motivera dess användning.[72]

4.8.4 Ålderskontroll

92. I förslaget uppmuntras leverantörer att använda ålderskontroll och åldersbedömningsåtgärder för att identifiera barnanvändare på sina tjänster.[73] I detta avseende noterar EDPB och EDPS att det för närvarande inte finns någon teknisk lösning som med säkerhet kan bedöma en användares ålder i ett onlinesammanhang, utan att förlita sig på en officiell digital identitet, som inte är tillgänglig för alla EU-medborgare i detta skede.[74] Därför skulle förslagets planerade användning av ålderskontrollåtgärder eventuellt kunna leda till att t.ex. unga vuxna utestängs från att få tillgång till onlinetjänster, eller till att mycket inkräktande verktyg för ålderskontroll införs, vilket kan hindra eller avskräcka från legitim användning av de berörda tjänsterna.

93. I detta avseende, och även om det i skäl 16 i förslaget hänvisas till verktyg för föräldrakontroll som möjliga riskbegränsningsåtgärder, rekommenderar EDPB och EDPS att den föreslagna förordningen ändras för att uttryckligen tillåta leverantörer att förlita sig på föräldrakontrollmekanismer utöver eller som ett alternativ till ålderskontroll.

4.9 Presentation av information

94. I artikel 22 i förslaget begränsas de ändamål för vilka de leverantörer som omfattas av förslaget får lagra innehållsdata och andra uppgifter som behandlas i samband med de åtgärder som vidtas för att uppfylla de skyldigheter som anges i förslaget. I förslaget anges dock att leverantörer också får bevara denna information i syfte att förbättra effektiviteten och korrektheten i tekniken för att spåra sexuella övergrepp mot barn på nätet för att verkställa en spårningsorder, men de får inte lagra några personuppgifter för detta ändamål.[75]

---

[69] Jfr interimsförordningen, artikel 1.2.
[70] Jfr förslaget, artikel 1.
[71] Se t.ex. § 201 i den tyska strafflagen.
[72] Se konsekvensbedömningsrapporten.
[73] Se förslaget, artiklarna 4.3, 6.1 c och skäl 16.
[74] Se t.ex. National Commission for Informatics and Liberty (Commission Nationale de l'Informatique et des Libertés), rekommendation 7: Kontrollera barnets ålder och föräldrarnas samtycke med respekt för barnets privatliv (9 augusti 2021).
[75] Förslaget, artikel 22.1.

95. EDPB och EDPS anser att endast de leverantörer som använder sin egen spårningsteknik bör tillåtas lagra uppgifter för att förbättra teknikens effektivitet och exakthet, medan de som använder teknik som tillhandahålls av EU-centrumet inte bör dra nytta av denna möjlighet. EDPB och EDPS noterar dessutom att det i praktiken kan vara svårt att säkerställa att inga personuppgifter lagras för detta ändamål, eftersom de flesta innehållsdata och andra uppgifter som behandlas för spårningsändamål sannolikt kommer att betraktas som personuppgifter.

4.10 Inverkan på kryptering

96. Europeiska dataskyddsmyndigheter har konsekvent förespråkat en utbredd tillgång till starka krypteringsverktyg och argumenterat mot alla typer av bakdörrar.[76] Detta beror på att kryptering är viktig för att säkerställa åtnjutandet av alla mänskliga rättigheter både offline och online.[77] Krypteringstekniken bidrar dessutom på ett grundläggande sätt både till respekten för privatlivet och konfidentialiteten vid kommunikation samt till innovation och tillväxt i den digitala ekonomin, som är beroende av den höga graden av tillit och förtroende för sådan teknik.

97. När det gäller interpersonell kommunikation är totalsträckskryptering ett viktigt verktyg för att säkerställa konfidentialitet vid elektronisk kommunikation, eftersom den ger starka tekniska garantier mot tillgång till kommunikationsinnehållet för någon annan än avsändaren och mottagaren/mottagarna, inbegripet för leverantören. Att på något sätt förhindra eller avskräcka från användningen av totalsträckskryptering genom att ålägga tjänsteleverantörer en skyldighet att behandla data från elektronisk kommunikation för andra ändamål än att tillhandahålla sina tjänster, eller ålägga dem en skyldighet att proaktivt vidarebefordra elektronisk kommunikation till tredje part skulle medföra en risk för att leverantörer erbjuder mindre krypterade tjänster för att bättre uppfylla skyldigheterna, vilket försvagar krypteringens roll i allmänhet och undergräver respekten för EU-medborgarnas grundläggande rättigheter. Det bör noteras att även om totalsträckskryptering är en av de vanligaste säkerhetsåtgärderna i samband med elektronisk kommunikation, kan andra tekniska lösningar (t.ex. användning av andra kryptografiska system) vara eller bli lika viktiga för att säkra och skydda konfidentialiteten vid digital kommunikation. Användningen av dem bör därför inte heller förhindras eller motverkas.

98. Införandet av verktyg för avlyssning och analys av interpersonell elektronisk kommunikation står i direkt motsats till totalsträckskryptering, eftersom krypteringen syftar till att tekniskt garantera att kommunikationen mellan mottagare och avsändare förblir konfidentiell.

99. Även om det i förslaget inte införs någon systematisk avlyssningsskyldighet för leverantörer, är det därför sannolikt att blotta möjligheten att en spårningsorder utfärdas kommer att kraftigt påverka leverantörernas tekniska val, särskilt med tanke på den begränsade tidsram som de kommer att behöva för att följa en sådan order och de stränga påföljder som de skulle drabbas av om de inte gör det.[78] I praktiken kan detta leda till att vissa leverantörer slutar använda totalsträckskryptering.

---

[76] Se t.ex. uttalande från arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter (artikel 29-gruppen) om kryptering och dess inverkan på skyddet av enskilda med avseende på behandlingen av deras personuppgifter i EU (11 april 2018).
[77] Se FN:s råd för mänskliga rättigheter, resolution 47/16 om främjande, skydd och åtnjutande av mänskliga rättigheter på internet, UN Doc. A/HRC/RES/47/16 (26 juli 2021).
[78] Jfr förslaget, artikel 35.

100. Konsekvenserna av att användningen av totalsträckskryptering försämras eller motverkas, vilket kan bli följden av förslaget, måste bedömas ordentligt. Var och en av de tekniker för att kringgå totalsträckskrypteringens integritetsbevarande karaktär som presenteras i den konsekvensbedömningsrapport som åtföljde förslaget skulle medföra kryphål i säkerheten. [79] Till exempel skulle genomsökning på klientsidan[80] sannolikt leda till betydande, oriktad tillgång till och behandling av okrypterat innehåll på slutanvändarens enheter. En sådan betydande försämring av konfidentialiteten skulle särskilt drabba barn eftersom det är mer sannolikt att de tjänster de använder omfattas av spårningsorder, vilket gör dem sårbara för övervakning eller avlyssning. Samtidigt är genomsökning på *serversidan* i grunden oförenlig med paradigmet med totalsträckskryptering, eftersom den peer-to-peer-krypterade kommunikationskanalen skulle behöva brytas, vilket skulle leda till massbehandling av personuppgifter på leverantörernas servrar.

101. Även om det i förslaget anges att förordningen låter ”den berörda leverantören välja vilken teknik som ska användas för att följa en spårningsorder och bör inte tolkas som att den uppmuntrar eller avskräcker från användningen av en viss teknik”,[81] blir den strukturella inkompatibiliteten mellan en viss spårningsorder och totalsträckskryptering i praktiken ett starkt hinder för att använda totalsträckskryptering. Oförmågan att få tillgång till och använda tjänster med hjälp av totalsträckskryptering (som för närvarande är den senaste tekniken när det gäller tekniska garantier för konfidentialitet) skulle kunna få en dämpande effekt på yttrandefriheten och den legitima privata användningen av elektroniska kommunikationstjänster. Det negativa förhållandet mellan material med sexuella övergrepp mot barn eller gromning och totalsträckskryptering erkänns också av kommissionen när den i konsekvensbedömningsrapporten[82] konstaterade att det var sannolikt att Facebooks frivilliga genomsökning skulle upphöra när Facebook inför totalsträckskryptering 2023.

102. För att säkerställa att den föreslagna förordningen inte undergräver säkerheten eller konfidentialiteten för europeiska medborgares elektroniska kommunikation anser EDPB och EDPS att det i den normativa delen av förslaget tydligt bör anges att ingenting i den föreslagna förordningen bör tolkas som att kryptering förbjuds eller försvagas, i linje med vad som anges i skäl 25 i interimsförordningen.

4.11 Tillsyn, verkställighet och samarbete

4.11.1 De nationella tillsynsmyndigheternas roll enligt den allmänna dataskyddsförordningen

103. Enligt förslaget ska det inrättas ett nätverk av nationella samordnande myndigheter, som ska ansvara för tillämpningen och efterlevnaden av den föreslagna förordningen. [83] I skäl 54 i förslaget anges visserligen att ”[b]estämmelserna i denna förordning om tillsyn och genomförande [inte bör] tolkas som att de påverkar dataskyddsmyndigheternas befogenheter och behörigheter enligt förordning (EU) 2016/679”, men EDPB och EDPS anser att förhållandet mellan de samordnande myndigheternas

[79] Se avsnitt 4.2 i Abelson, Harold, Anderson, Ross J., Bellovin, Steven M., Benaloh, Josh, Blaze, Matt, Callas, John L., Diffie, Whitfield, Landau, Susan, Neumann, Peter G., Rivest, Ronald L., Schiller, Jeffrey I., Schneier, Bruce, Teague, Vanessa och Troncoso, Carmela, ”Bugs in our Pockets: Risks of clientside Scanning ”, ArXiv abs/2110.07450 (2021).
[80] Med genomsökning på klientsidan avses i princip system som söker igenom innehållet i meddelanden för matchningar mot en databas med tvivelaktigt innehåll innan meddelandet skickas till den avsedda mottagaren.
[81] Förslaget, skäl 26.
[82] Konsekvensbedömningsrapport s. 27.
[83] Förslaget, artikel 25.

och dataskyddsmyndigheternas uppgifter bör regleras bättre, och att dataskyddsmyndigheterna bör ges en mer framträdande roll i den föreslagna förordningen.

104. Leverantörer bör i synnerhet vara skyldiga att samråda med dataskyddsmyndigheter genom ett sådant föregående samrådsförfarande som avses i artikel 36 i den allmänna dataskyddsförordningen innan de inför några åtgärder för att spåra material med sexuella övergrepp mot barn eller gromning, och inte uteslutande i samband med användningen av åtgärder för att spåra kontaktsökning med barn, såsom för närvarande föreskrivs i förslaget.[84] Alla spårningsåtgärder bör anses leda till ”hög risk” som standard och bör därför genomgå ett föregående samrådsförfarande oavsett om de rör gromning eller material med sexuella övergrepp mot barn, vilket redan är fallet enligt interimsförordningen.[85] Dessutom bör de behöriga dataskyddsmyndigheter som utsetts enligt den allmänna dataskyddsförordningen alltid ha befogenhet att lämna synpunkter på de planerade spårningsåtgärderna, och inte bara under särskilda omständigheter.[86]

105. Dessutom bör det genom den föreslagna förordningen inrättas ett system för att hantera och lösa tvister mellan behöriga myndigheter och dataskyddsmyndigheter när det gäller spårningsorder. Dataskyddsmyndigheterna bör i synnerhet ges rätt att bestrida en spårningsorder vid domstolarna i den medlemsstat där den behöriga rättsliga myndighet eller oberoende administrativa myndighet som utfärdade spårningsordern är belägen. I detta avseende noterar EDPB och EDPS att den behöriga myndigheten, enligt den nuvarande versionen av förslaget, kan avvisa yttrandet från de behöriga dataskyddsmyndigheterna när den utfärdar en spårningsorder. Detta skulle kunna leda till motstridiga order, eftersom dataskyddsmyndigheterna, vilket bekräftas i artikel 36.2 i dataskyddsförordningen, skulle behålla hela spektrumet av sina korrigerande befogenheter enligt artikel 58 i dataskyddsförordningen, inbegripet befogenheten att beordra ett förbud mot behandling.

4.11.2 Europeiska dataskyddsstyrelsens roll

106. EDPB och EDPS noterar att enligt artikel 50.1 tredje meningen i förslaget ska ”EU-centrumet begära ett yttrande från sin tekniska kommitté och från Europeiska dataskyddsstyrelsen” innan det inkluderar en särskild teknik i förteckningarna över teknik som värdtjänstleverantörer och leverantörer av interpersonella kommunikationstjänster kan överväga att använda för att verkställa spårningsorder. Det föreskrivs vidare att EDPB ska avge sina yttranden inom åtta veckor, vilket vid behov kan förlängas med ytterligare sex veckor, med hänsyn till sakfrågans komplexitet. Slutligen krävs det att EDPB informerar EU-centrumet om en sådan förlängning inom en månad från mottagandet av begäran om samråd, tillsammans med skälen till förseningen.

107. EDPB:s befintliga uppgifter fastställs i artikel 70 i den allmänna dataskyddsförordningen och artikel 51 i direktiv (EU) 2016/680 (nedan kallat *dataskyddsdirektivet*)[87]. Enligt dessa uppgifter ska EDPB ge råd till kommissionen och avge yttranden på begäran av kommissionen, en nationell tillsynsmyndighet eller dess ordförande. Medan det i artikel 1.3 d i förslaget anges att de regler som fastställs i den allmänna dataskyddsförordningen och dataskyddsdirektivet inte ska påverkas av förslaget, går det att ge EU-centrumet befogenhet att begära yttranden från EDPB utöver de uppgifter som tilldelats EDPB

[84] Förslaget, artikel 7.3 andra stycket b.
[85] Interimsförordningen, artikel 3.1 c.
[86] Jfr förslaget, artikel 7.3 andra stycket c.
[87] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

enligt den allmänna dataskyddsförordningen och dataskyddsdirektivet. Det bör därför klargöras i den föreslagna förordningen – åtminstone i ett skäl – att förslaget utvidgar EDPB:s uppgifter. I detta avseende uppskattar EDPB och EDPS den viktiga roll som förslaget ger EDPB genom att kräva dess deltagande i det praktiska genomförandet av den föreslagna förordningen. I praktiken spelar EDPB:s sekretariat en viktig roll när det gäller att tillhandahålla det analytiska, administrativa och logistiska stöd som krävs för antagandet av EDPB:s yttranden. För att säkerställa att EDPB och dess ledamöter kan fullgöra sina uppgifter är det därför viktigt att anslå tillräckliga budgetmedel och tillräckligt med personal till EDPB. Tyvärr anges det dock inte i förslagets finansieringsöversikt att ytterligare resurser kommer att göras tillgängliga för utförandet av de ytterligare uppgifter som förslaget tilldelar EDPB.[88]

108. Vidare noterar EDPB och EDPS att artikel 50 i förslaget inte anger hur EU-centrumet kommer att gå vidare efter att ha mottagit ett yttrande från EDPB.[89] I skäl 27 i förslaget anges endast att råd från EDPB bör beaktas av EU-centrumet och Europeiska kommissionen. Det bör därför klargöras vilket syfte det begärda yttrandet kommer att tjäna i det förfarande som föreskrivs i artikel 50 i förslaget och hur EU-centrumet ska agera efter att ha mottagit ett yttrande från EDPB.

109. Dessutom anser EDPB och EDPS att även om alla riktlinjer från EDPB eller eventuella yttranden om användningen av spårningsteknik kommer att bedöma användningen av sådan teknik på allmän nivå, måste den nationella tillsynsmyndigheten för ett föregående samråd enligt artikel 36 i dataskyddsförordningen ta hänsyn till de särskilda omständigheterna och göra en bedömning från fall till fall av den berörda personuppgiftsansvariges avsedda behandling. EDPB och EDPS noterar att tillsynsmyndigheterna kommer att och bör tillämpa de kriterier som anges i artikel 36 i dataskyddsförordningen för att besluta om det är nödvändigt att förlänga den tidsfrist som anges i dataskyddsförordningen för att lämna sina yttranden som svar på ett föregående samråd, och det finns inget behov av att tillämpa andra standarder när ett föregående samråd gäller användningen av en spårningsteknik.[90]

110. Vid tillämpningen av artikel 11 (”Riktlinjer för spårningsskyldigheter”) föreskrivs slutligen i förslaget att kommissionen får utfärda riktlinjer för tillämpningen av artiklarna 7–10 i förslaget. Artikel 11 i förslaget bör ändras för att klargöra att EDPB, i tillägg till samordningsmyndigheterna och EU-centrumet, bör rådfrågas av kommissionen om utkastet till riktlinjer utanför det planerade offentliga samrådsförfarandet innan riktlinjer om spårningsskyldigheter utfärdas.

111. Därför kräver denna uppgift för EDPB, liksom dess roll inom den rättsliga ram som skulle införas genom förslaget, en ytterligare bedömning från lagstiftarens sida.

4.11.3 Rollen för EU-centrumet för bekämpande av sexuella övergrepp mot barn

112. Genom kapitel IV i förslaget inrättas EU-centrumet som en ny decentraliserad byrå för att möjliggöra genomförandet av förslaget. EU-centrumet bör bland annat underlätta leverantörernas tillgång till tillförlitlig spårningsteknik, tillgängliggöra indikatorer som inrättas baserat på sexuella övergrepp mot barn på nätet som har verifierats av domstolar eller oberoende administrativa myndigheter i medlemsstaterna för spårningsändamål, på begäran tillhandahålla visst stöd i samband med riskbedömningar och tillhandahålla stöd i kommunikationen med relevanta nationella myndigheter.[91]

[88] Jfr förslaget. s. 105 och följande.
[89] Kontrastera med artikel 51.4 i dataskyddsdirektivet.
[90] Jfr förslaget, skäl 24.
[91] Se COM(2022) 209 final, s. 7.

113. I detta avseende välkomnar EDPB och EDPS artikel 77.1 i förslaget som bekräftar att behandling av personuppgifter som utförs av EU-centrumet ska omfattas av Europeiska unionens dataskyddsförordning samt föreskriver att åtgärder för EU-centrumets tillämpning av den förordningen, inbegripet de som rör utnämningen av ett dataskyddsombud vid EU-centrumet, ska fastställas efter samråd med EDPS. EDPB och EDPS anser dock att flera bestämmelser i detta kapitel bör granskas närmare.

114. För det första noterar EDPB och EDPS att det i artikel 48 i förslaget föreskrivs att alla rapporter som inte är ”uppenbart ogrundade”[92] ska överlämnas till nationella brottsbekämpande myndigheter och Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol). Denna tröskel för att EU-centrumet ska vidarebefordra rapporter till nationella brottsbekämpande myndigheter och Europol (”inte uppenbart ogrundad”) förefaller alltför låg, särskilt med tanke på att syftet med att inrätta EU-centrumet, i enlighet med kommissionens konsekvensbedömning,[93] är att minska bördan för de brottsbekämpande myndigheterna och Europol när det gäller att filtrera innehåll som felaktigt markerats som material med sexuella övergrepp mot barn. I detta avseende är det oklart varför EU-centrumet, i egenskap av kompetenscentrum, inte skulle kunna göra en mer grundlig rättslig och faktisk bedömning för att begränsa risken för att oskyldiga personers uppgifter överförs till brottsbekämpande myndigheter.

115. För det andra förefaller bestämmelsen om varaktigheten för EU-centrumets lagring av personuppgifter vara relativt öppen med tanke på de berörda uppgifternas känslighet. Även om det inte skulle vara möjligt att fastställa en maximal lagringsperiod för lagring av dessa uppgifter rekommenderar EDPB och EDPS att det i förslaget fastställs åtminstone en maximal tidsfrist för att se över behovet av fortsatt lagring av uppgifter och kräva motivering för förlängd lagring efter den perioden.

116. Med tanke på den mycket höga känsligheten hos de personuppgifter som ska behandlas av EU-centrumet anser EDPB och EDPS dessutom att behandlingen bör omfattas av ytterligare skyddsåtgärder, särskilt för att säkerställa en effektiv tillsyn. Detta skulle kunna inbegripa en skyldighet för EU-centrumet att föra loggar över uppgiftsbehandling i automatiserade behandlingssystem (dvs. att återspegla kravet på operativa personuppgifter enligt kapitel IX i Europeiska unionens dataskyddsförordning), inbegripet registrering, ändring, åtkomst, läsning, utlämnande, kombination och radering av personuppgifter. Loggarna över läsning och utlämning ska göra det möjligt att fastställa motivering, datum och tidpunkt för sådana åtgärder, vem som har läst eller lämnat ut operativa personuppgifter samt, i möjligaste mån, vilka som har fått tillgång till de operativa personuppgifterna. Dessa loggar skulle användas för kontroll av behandlingens laglighet, egenkontroll och för att säkerställa dess integritet och säkerhet och skulle på begäran göras tillgängliga för EU-centrumets dataskyddsombud och EDPS.

117. I förslaget hänvisas dessutom till leverantörernas skyldighet att informera användarna om spårningen av material med sexuella övergrepp mot barn via spårningsorder samt rätten att lämna in ett klagomål till en samordnande myndighet.[94] I förslaget fastställs dock inga förfaranden för utövandet av registrerades rättigheter, även med beaktande av de många platser där personuppgifter kan överföras och lagras enligt förslaget (EU-centrumet, Europol, nationella brottsbekämpande organ). Kravet på att

[92] Begreppet ”uppenbart ogrundad” beskrivs i skäl 65 i förslaget som ”där det omedelbart är uppenbart, utan någon konkret rättslig eller faktisk analys, att de rapporterade verksamheterna inte utgör sexuella övergrepp mot barn på nätet”.

[93] Se t.ex. sidan 349 i konsekvensbedömningsrapporten.

[94] Se artikel 10.6 och, efter inlämnandet av en rapport till EU-centrumet, artikel 12.2 i förslaget.

informera användarna bör inbegripa en skyldighet att informera enskilda personer om att deras uppgifter har överförts och behandlas av olika enheter i tillämpliga fall (t.ex. av nationella brottsbekämpande organ och av Europol). Dessutom bör det finnas ett centraliserat förfarande för att ta emot och samordna begäranden om rätt till tillgång, rättelse och radering, eller alternativt en skyldighet som den enhet som tar emot en registrerads begäran samordnar med de andra berörda enheterna.

118. EDPB och EDPS noterar att EU-centrumet enligt artikel 50 i förslaget har till uppgift att specificera förteckningen över den teknik som får användas för att verkställa spårningsorder. Enligt artikel 12.1 i förslaget är leverantörer dock skyldiga att rapportera all information som tyder på potentiella sexuella övergrepp mot barn på nätet på sina tjänster, inte bara sådan information som härrör från verkställandet av en spårningsorder. Det är högst sannolikt att en betydande mängd sådan information skulle komma från leverantörernas riskbegränsningsåtgärder, i enlighet med artikel 4 i förslaget. Det förefaller därför avgörande att fastställa vilka dessa åtgärder kan vara, deras effektivitet, deras felfrekvens när det gäller att rapportera potentiella sexuella övergrepp mot barn och hur de påverkar enskilda personers rättigheter och friheter. Trots att det i artikel 4.5 i förslaget anges att kommissionen får utfärda relevanta riktlinjer, i samarbete med samordnande myndigheter och EU-centrumet och efter att ha genomfört ett offentligt samråd, anser EDPB och EDPS att det är viktigt att lagstiftaren i artikel 50 inkluderar en uppgift för EU-centrumet att även tillhandahålla en förteckning över rekommenderade riskbegränsningsåtgärder och relevant bästa praxis som är särskilt effektiv när det gäller att identifiera potentiella sexuella övergrepp mot barn på nätet. Eftersom sådana åtgärder kan inkräkta på de grundläggande rättigheterna till dataskydd och integritet rekommenderas det också att EU-centrumet begär ett yttrande från EDPB innan en sådan förteckning utfärdas.

119. Slutligen bör säkerhetskraven i artikel 51.4 i förslaget vara mer specifika. I detta avseende kan inspiration hämtas från de säkerhetskrav som fastställs i andra förordningar om storskaliga system som inbegriper högriskbehandling, såsom förordning (EG) nr 767/2008[95] (se artikel 32), förordning (EG) nr 1987/2006[96] (se artikel 16), förordning (EG) nr 2018/1862[97] (se artikel 16) och förordning (EG) nr 603/2013[98] (se artikel 34).

[95] Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) (EUT L 218, 13.8.2008, s. 60).

[96] Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II) (EUT L 381, 28.12.2006, s. 4).

[97] Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

[98] Europaparlamentets och rådets förordning (EU) nr 603/2013 av den 26 juni 2013 om inrättande av Eurodac för jämförelse av fingeravtryck för en effektiv tillämpning av förordning (EU) nr 604/2013 om kriterier och mekanismer för att avgöra vilken medlemsstat som är ansvarig för att pröva en ansökan om internationellt skydd som en tredjelandsmedborgare eller en statslös person har lämnat in i någon medlemsstat och för när medlemsstaternas brottsbekämpande myndigheter begär jämförelser med Eurodac-uppgifter för brottsbekämpande ändamål, samt om ändring av förordning (EU) nr 1077/2011 om inrättande av en Europeisk byrå för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa (EUT L 180, 29.6.2013, s. 1).

4.11.4 Europols roll

120. I förslaget föreskrivs ett nära samarbete mellan EU-centrumet och Europol. Enligt kapitel IV i förslaget ska EU-centrumet, efter att ha mottagit rapporter från leverantörer om misstänkta fall av material med sexuella övergrepp mot barn, kontrollera dem för att bedöma vilka rapporter som är användbara (som inte är uppenbart ogrundade) och vidarebefordra dem till Europol och till nationella brottsbekämpande myndigheter.[99] EU-centrumet ska bevilja Europol åtkomst till sina databaser med indikatorer och databaser över rapporter för att bistå Europols utredningar av misstänkta sexuella övergrepp mot barn.[100] Dessutom skulle EU-centrumet ”i största möjliga utsträckning” beviljas åtkomst till Europols informationssystem.[101] De båda byråerna kommer också att dela lokaler och viss (icke-operativ) infrastruktur.[102]

121. EDPB och EDPS noterar att flera aspekter som rör samarbetet mellan det föreslagna EU-centrumet och Europol ger anledning till oro eller kräver ytterligare specificering.

Om översändande av rapporter från EU-centrumet till Europol (artikel 48)

122. Enligt artikel 48 i förslaget till förordning ska EU-centrumet överlämna rapporter som inte anses vara uppenbart ogrundade, tillsammans med eventuell ytterligare relevant information, till Europol och till den eller de behöriga brottsbekämpande myndigheterna i den eller de medlemsstater som sannolikt har behörighet att utreda eller lagföra potentiella sexuella övergrepp mot barn. Även om denna artikel ger Europol rollen att identifiera den berörda brottsbekämpande myndigheten om den berörda medlemsstaten är oklar, föreskrivs det i bestämmelsen att alla rapporter ska översändas till Europol oavsett om den nationella myndigheten har identifierats och rapporten redan har översänts från EU-centrumet.

123. Förslaget klargör dock inte vilket mervärde Europols medverkan skulle tillföra eller dess förväntade roll vid mottagandet av rapporterna, särskilt i de fall där den nationella brottsbekämpande myndigheten har identifierats och underrättats parallellt.[103]

124. EDPB och EDPS erinrar om att Europols mandat är begränsat till att stödja åtgärder som vidtas av medlemsstaternas behöriga myndigheter och deras ömsesidiga samarbete för att förebygga och bekämpa allvarlig brottslighet som berör två eller flera medlemsstater.[104] I artikel 19 i förordning (EU) 2016/794 [105], ändrad genom förordning (EU) 2022/991 [106], (nedan kallad *den ändrade Europolförordningen*) föreskrivs att ett unionsorgan som lämnar information till Europol är skyldigt att

[99] Se artikel 48 i förslaget.
[100] Se artikel 46.4–5 i förslaget.
[101] Se artikel 53.2 i förslaget.
[102] Särskilt de som rör personalförvaltning, informationsteknik (IT), inbegripet cybersäkerhet, byggnader och kommunikation.
[103] Skäl 71 i förslaget innehåller endast en allmän hänvisning till Europols erfarenhet av att identifiera behöriga nationella myndigheter i oklara situationer och Europols databas över kriminalunderrättelser, som kan bidra till att identifiera kopplingar till utredningar i andra medlemsstater.
[104] Se artikel 3 i den ändrade Europolförordningen.
[105] Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF (EUT L 135, 24.5.2016, s. 53).
[106] Europaparlamentets och rådets förordning (EU) 2022/991 av den 8 juni 2022 om ändring av förordning (EU) 2016/794 vad gäller Europols samarbete med privata parter, Europols behandling av personuppgifter till stöd för brottsutredningar och Europols roll inom forskning och innovation (EUT L 169, 27.6.2022, s. 1).

fastställa för vilket eller vilka ändamål uppgifterna ska behandlas av Europol samt villkoren för behandlingen. Det ansvarar också för att säkerställa att de överförda personuppgifterna är korrekta.[107]

125. Ett generellt översändande av rapporter till Europol skulle därför strida mot den ändrade Europolförordningen och medföra ett antal dataskyddsrisker. Dubbleringen av behandlingen av personuppgifter skulle kunna leda till att flera kopior av samma mycket känsliga personuppgifter lagras parallellt (t.ex. hos EU-centrumet, Europol, nationella brottsbekämpande myndigheter), med risker för uppgifternas korrekthet till följd av en eventuell avsynkronisering av databaser och för utövandet av registrerades rättigheter. Det låga tröskelvärde som fastställs i förslaget för utbyte av rapporter med brottsbekämpande myndigheter (sådana som ”inte är uppenbart ogrundade”) innebär dessutom en stor sannolikhet för att falska positiva resultat (dvs. innehåll som felaktigt markerats som sexuella övergrepp mot barn) kommer att lagras i Europols informationssystem, eventuellt under längre perioder.[108]

126. EDPB och EDPS rekommenderar därför att förslaget specificerar och begränsar de omständigheter och syften under vilka EU-centrumet kan vidarebefordra rapporter till Europol, i enlighet med den ändrade Europolförordningen. Detta bör uttryckligen utesluta de omständigheter där rapporter har översänts till medlemsstatens berörda brottsbekämpande myndighet, som inte har någon gränsöverskridande dimension. Dessutom bör förslaget innehålla ett krav på att EU-centrumet endast ska överföra personuppgifter till Europol som är lämpliga, relevanta och begränsade till vad som är absolut nödvändigt. Särskilda skyddsåtgärder för att säkerställa uppgifternas kvalitet och tillförlitlighet måste också fastställas.

[107] Artikel 38.2 a i den ändrade Europolförordningen.

[108] Enligt kommissionens konsekvensbedömningsrapport har Europol endast kunnat granska 20 procent av de 50 miljoner unika bilder och videoklipp från material med sexuella övergrepp mot barn som finns i Europols databas, vilket innebär att det saknas resurser för att hantera de bidrag av material med sexuella övergrepp mot barn som byrån för närvarande tar emot. Se konsekvensbedömningsrapporten som åtföljer förslaget till förordning om fastställande av regler för att förebygga och bekämpa sexuella övergrepp mot barn, SWD(2022) 209, s. 47–48.

Artikel 53.2 om samarbete mellan EU-centrumet och Europol

127. Enligt artikel 53.2 i förslaget ska Europol och EU-centrumet ”i största möjliga utsträckning ge varandra åtkomst till relevant information och relevanta informationssystem, när så krävs för att de ska kunna utföra sina respektive uppgifter och i enlighet med de unionsrättsakter som reglerar denna åtkomst”.

128. I artiklarna 46.4 och 46.5 i förslaget anges vidare att Europol ska ha tillgång till EU-centrumets databas med indikatorer och databas med rapporter, och i artikel 46.6 fastställs förfarandet för beviljande av denna tillgång: Europol ska lämna in en begäran med angivande av syftet med och graden av den åtkomst som krävs för att uppnå detta syfte, och begäran ska vederbörligen bedömas av EU-centrumet.

129. De kriterier och skyddsåtgärder som krävs för Europols åtkomst och efterföljande användning av uppgifter från EU-centrumets informationssystem specificeras inte. Det förklaras inte heller varför det är nödvändigt att ge Europol direkt åtkomst till informationssystem hos en icke-brottsbekämpande myndighet som innehåller mycket känsliga personuppgifter, vars koppling till brottslig verksamhet och brottsförebyggande verksamhet kanske inte har fastställts. För att säkerställa en hög dataskyddsnivå och efterlevnad av principen om ändamålsbegränsning rekommenderar EDPB och EDPS att överföring av personuppgifter från EU-centrumet till Europol endast ska ske från fall till fall, efter en vederbörligen bedömd begäran, via ett säkert kommunikationsverktyg för utbyte, såsom Siena. [109]

130. Artikel 53.2 i förslaget innehåller den enda hänvisningen till EU-centrumets åtkomst till Europols informationssystem. Det är därför oklart för vilka syften och enligt vilka särskilda garantier sådan åtkomst skulle äga rum.

131. EDPB och EDPS erinrar om att Europol är en brottsbekämpande myndighet som har inrättats enligt EU-fördragen med ett centralt mandat att förebygga och bekämpa allvarlig brottslighet. De operativa personuppgifter som behandlas av Europol omfattas följaktligen av strikta regler och skyddsåtgärder för uppgiftsbehandling. Det föreslagna EU-centrumet är inte ett brottsbekämpande organ och bör under inga omständigheter beviljas direkt åtkomst till Europols informationssystem.

132. EDPB och EDPS noterar vidare att en stor del av informationen av gemensamt intresse för EU-centrumet och Europol kommer att avse personuppgifter om offer för påstådda brott, personuppgifter om minderåriga och personuppgifter om sexualliv, vilka klassificeras som särskilda kategorier av personuppgifter enligt den ändrade Europolförordningen. I den ändrade Europolförordningen fastställs strikta villkor för tillgång till särskilda kategorier av personuppgifter. I artikel 30.3 i den ändrade Europolförordningen föreskrivs att endast Europol ska ha direkt åtkomst till sådana personuppgifter, närmare bestämt endast ett begränsat antal Europoltjänstemän som vederbörligen har utsetts av den verkställande direktören. [110]

133. EDPB och EDPS rekommenderar därför att lydelsen i artikel 53.2 i förslaget förtydligas för att korrekt återspegla de restriktioner som gäller enligt den ändrade Europolförordningen och specificera villkoren för EU-centrumets åtkomst. I synnerhet bör åtkomst till personuppgifter som behandlas i Europols informationssystem, när den anses vara absolut nödvändig för att EU-centrumet ska kunna utföra sina uppgifter, endast beviljas från fall till fall, efter det att en uttrycklig begäran lämnats in, med angivande av det specifika syftet och motiveringen. Europol bör vara skyldigt att omsorgsfullt

[109] Nätapplikation för säkert informationsutbyte (Siena).

[110] Enligt den ändrade Europolförordningen görs undantag från detta förbud för unionsbyråer som inrättats på grundval av avdelning V i EUF-fördraget. Med tanke på förslagets rättsliga grund (artikel 114 i EUF-fördraget om harmonisering av den inre marknaden) skulle detta undantag dock inte omfatta det föreslagna EU-centrumet.

bedöma dessa begäranden och endast överföra personuppgifter till EU-centrumet om det är strikt nödvändigt och står i proportion till det eftersträvade syftet.

Artikel 10.6 om Europols roll när det gäller att informera användare efter genomförandet av en spårningsorder

134. EDPB och EDPS välkomnar kravet i artikel 10.6 i förslaget på att leverantörer ska informera användare vars personuppgifter kan beröras av verkställandet av en spårningsorder. Denna information ska lämnas till användarna först efter det att Europol eller den nationella brottsbekämpande myndigheten i en medlemsstat som tagit emot den rapport som avses i artikel 48 i förslaget har bekräftat att tillhandahållande av information till användare inte skulle påverka verksamhet för att förebygga, spåra, utreda och lagföra brott mot sexuella övergrepp mot barn.

135. Det finns dock en brist på precision när det gäller det praktiska genomförandet av denna bestämmelse. När rapporter vidarebefordras till både Europol och en brottsbekämpande myndighet i en medlemsstat anges inte i förslaget huruvida bekräftelse krävs från den ena eller båda mottagarna, och inte heller anges förfarandena/formerna för att erhålla denna bekräftelse i förslaget (t.ex. huruvida bekräftelser ska förmedlas via EU-centrumet). Med tanke på den stora mängd material med sexuella övergrepp mot barn som Europol och nationella brottsbekämpande myndigheter skulle kunna behöva behandla och avsaknaden av en exakt tidsfrist för att lämna denna bekräftelse (”utan onödigt dröjsmål”) rekommenderar EDPB och EDPS att de tillämpliga förfarandena förtydligas för att säkerställa att denna skyddsåtgärd genomförs i praktiken. Dessutom bör skyldigheten att informera användarna även omfatta information om mottagarna av de berörda personuppgifterna.

Om insamling av uppgifter och rapportering om öppenhet (artikel 83)

136. Enligt artikel 83.3 i förslaget ska EU-centrumet samla in uppgifter och ta fram statistik som rör ett antal av dess uppgifter enligt den föreslagna förordningen. För övervakningsändamål rekommenderar EDPB och EDPS att man i denna förteckning lägger till statistik om antalet rapporter som översänts till Europol i enlighet med artikel 48 samt antalet begäranden om åtkomst som mottagits av Europol enligt artikel 46.4 och 46.5, inklusive antalet begäranden som beviljats eller avslagits av EU-centrumet.

5. SLUTSATS

137. EDPB och EDPS välkomnar kommissionens insatser för att säkerställa effektiva åtgärder mot sexuella övergrepp mot barn på nätet, men anser att förslaget ger upphov till allvarliga dataskydds- och integritetsproblem. EDPB och EDPS uppmanar därför medlagstiftarna att ändra den föreslagna förordningen, särskilt för att säkerställa att de planerade spårningsskyldigheterna uppfyller de tillämpliga nödvändighets- och proportionalitetsstandarderna och inte leder till att krypteringen försvagas eller försämras på allmän nivå. EDPB och EDPS förblir tillgängliga för att erbjuda sitt stöd under lagstiftningsprocessen, om deras bidrag skulle anses nödvändiga för att ta itu med de problem som lyfts fram i detta gemensamma yttrande.

För Europeiska datatillsynsmannen	För Europeiska dataskyddsstyrelsen
Europeiska datatillsynsmannen	Ordförande
(Wojciech Wiewiorowski)	(Andrea Jelinek)