CEPD-AEPD

Avizul comun nr. 4/2022 privind Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor

Adoptat la 28 iulie 2022

CUPRINS

Rezumat

La 11 mai 2022, Comisia Europeană a publicat Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor.

Propunerea ar impune obligații specifice furnizorilor de servicii de găzduire, de servicii de comunicații interpersonale și de alte servicii în ceea ce privește detectarea, raportarea, eliminarea și blocarea materialelor online cunoscute și noi care conțin abuzuri sexuale asupra copiilor, precum și ademenirea copiilor. Propunerea prevede, de asemenea, înființarea unei noi agenții descentralizate a UE („Centrul UE") și a unei rețele de Autorități naționale de Coordonare pentru problemele legate de abuzul sexual asupra copiilor, pentru a permite punerea în aplicare a propunerii de Regulament. După cum se recunoaște în Expunerea de Motive a Propunerii, măsurile cuprinse în Propunere ar afecta exercitarea drepturilor fundamentale ale utilizatorilor serviciilor în cauză.

Abuzul sexual asupra copiilor este o infracțiune deosebit de gravă și odioasă, iar obiectivul de a permite o acțiune eficientă pentru a-l combate reprezintă un obiectiv de interes general recunoscut de Uniune și urmărește să protejeze drepturile și libertățile victimelor. În același timp, CEPD și AEPD reamintesc că orice limitare a drepturilor fundamentale, precum cele avute în vedere de propunere, trebuie să respecte cerințele prevăzute la articolul 52 alineatul (1) din Carta Drepturilor Fundamentale a Uniunii Europene.

CEPD și AEPD subliniază că Propunerea ridică serioase îngrijorări în ceea ce privește proporționalitatea interferențelor și a limitărilor avute în vedere în raport cu protecția drepturilor fundamentale la viață privată și cu protecția datelor cu caracter personal. În această privință, CEPD și AEPD subliniază că garanțiile procedurale nu pot înlocui niciodată pe deplin garanțiile de fond. Un sistem complex de escaladare de la evaluarea riscurilor și măsurile de atenuare a acestora la un ordin de detectare nu poate înlocui claritatea necesară a obligațiilor de fond.

CEPD și AEPD consideră că Propunerea nu este clară în privința unor elemente-cheie, cum ar fi noțiunea de „risc semnificativ". În plus, entitățile însărcinate cu aplicarea acestor garanții, începând cu operatorii privați și terminând cu autoritățile administrative și/sau judiciare, se bucură de o marjă de apreciere foarte largă, ceea ce duce la insecuritate juridică privind modul de stabilire a echilibrului între drepturile în discuție în fiecare caz în parte. CEPD și AEPD subliniază că legiuitorul trebuie, atunci când permite interferențe deosebit de grave cu drepturile fundamentale, să ofere claritate juridică cu privire la momentul și locul în care sunt permise interferențele. Deși recunosc faptul că legislația nu poate fi prea prescriptivă și trebuie să lase o anumită flexibilitate în aplicarea sa practică, CEPD și AEPD consideră că Propunerea lasă prea mult loc pentru potențiale abuzuri din cauza lipsei unor norme de fond clare.

În ceea ce privește necesitatea și proporționalitatea măsurilor de detectare avute în vedere, CEPD și AEPD sunt deosebit de preocupate de măsurile avute în vedere pentru detectarea materialelor necunoscute care conțin abuzuri sexuale asupra copiilor („MASC") și a cazurilor de ademenire a copiilor („grooming") în cadrul serviciilor de comunicații interpersonale. Din cauza caracterului lor intruziv, a naturii lor probabilistice și a ratelor de eroare asociate cu astfel de tehnologii, CEPD și AEPD consideră că interferența provocată de aceste măsuri depășește ceea ce este necesar și proporțional. În plus, măsurile care permit autorităților publice să aibă acces în mod generalizat la conținutul unei comunicări pentru a detecta cazurile de ademenire a copiilor sunt mai susceptibile de a afecta esența drepturilor garantate la articolele 7 și 8 din Cartă. Prin urmare, dispozițiile relevante referitoare la „grooming" ar trebui eliminate din Propunere. În plus, Propunerea nu exclude din domeniul său de aplicare scanarea comunicațiilor audio. CEPD și AEPD consideră că scanarea

comunicațiilor audio este deosebit de intruzivă și, ca atare, trebuie să rămână în afara domeniului de aplicare al obligațiilor de detectare stabilite în propunerea de Regulament, atât pentru mesajele vocale, cât și pentru comunicațiile în direct.

De asemenea, CEPD și AEPD își exprimă îndoielile cu privire la eficiența măsurilor de blocare și consideră că solicitarea adresată furnizorilor de servicii de internet de a decripta comunicațiile online pentru a le bloca pe cele referitoare la MASC ar fi disproporționată.

În plus, CEPD și AEPD subliniază că tehnologiile de criptare contribuie în mod fundamental la respectarea vieții private și a confidențialității comunicațiilor, la libertatea de exprimare, precum și la inovare și la creșterea economiei digitale, care se bazează pe nivelul ridicat de încredere pe care îl oferă aceste tehnologii. Considerentul 26 din Propunere se referă nu numai la alegerea tehnologiilor de detectare, ci și a măsurilor tehnice de protejare a confidențialității comunicațiilor, cum ar fi criptarea, cu atenționarea că această alegere tehnologică trebuie să îndeplinească cerințele propunerii de Regulament, și anume trebuie să permită detectarea. Acest lucru susține ideea rezultată din articolul 8 alineatul (3) și din articolul 10 alineatul (2) din Propunere, conform căreia un furnizor nu poate refuza executarea unui ordin de detectare pe baza imposibilității tehnice. CEPD și AEPD consideră că ar trebui să existe un echilibru mai bun între nevoia societății de a avea canale de comunicare sigure și confidențiale și de a combate utilizarea abuzivă a acestora. Ar trebui să se precizeze în mod clar în Propunere că niciun element din propunerea de Regulament nu ar trebui interpretat ca fiind o interzicere sau o slăbire a criptării.

Deși CEPD și AEPD salută faptul că în Propunere se stipulează că aceasta nu afectează prerogativele și competențele autorităților pentru protecția datelor în temeiul RGPD, CEPD și AEPD sunt de părere că relația dintre sarcinile Autorităților de Coordonare și cele ale autorităților pentru protecția datelor ar trebui totuși să fie mai bine reglementată. În acest sens, CEPD și AEPD apreciază rolul pe care Propunerea îl atribuie CEPD, solicitând implicarea acestuia în punerea în aplicare practică a Propunerii, în special necesitatea ca CEPD să emită un aviz cu privire la tehnologiile pe care Centrul UE le va pune la dispoziție pentru a executa ordinele de detectare. Cu toate acestea, ar trebui să se clarifice care ar fi scopul avizului în cadrul acestui proces și cum ar acționa Centrul UE după ce a primit un aviz din partea CEPD.

În cele din urmă, CEPD și AEPD iau act de faptul că Propunerea are în vedere o cooperare strânsă între Centrul UE și Europol, care ar trebui să își ofere reciproc „cel mai larg acces posibil la sistemele informatice relevante”. Deși, în principiu, CEPD și AEPD sprijină cooperarea dintre cele două agenții, având în vedere că Centrul UE nu este o autoritate de aplicare a legii, CEPD și AEPD fac totuși câteva recomandări pentru îmbunătățirea dispozițiilor relevante, inclusiv aceea ca transmiterea de date cu caracter personal între Centrul UE și Europol să aibă loc numai de la caz la caz, în urma unei cereri evaluate în mod corespunzător, prin intermediul unui instrument de comunicare securizat pentru schimburi, cum ar fi rețeaua SIENA.

Comitetul European pentru Protecția Datelor și Autoritatea Europeană pentru Protecția Datelor,

având în vedere articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725 din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE („RPDUE"),[1]

având în vedere Acordul privind SEE și, în special, anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018,[2]

având în vedere solicitarea Comisiei Europene de emitere a unui aviz comun al Comitetului European pentru Protecția Datelor și al Autorității Europene pentru Protecția Datelor din 12 mai 2022 privind Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor,[3]

A ADOPTAT PREZENTUL AVIZ COMUN

1. CONTEXT

1. La 11 mai 2022, Comisia Europeană („Comisia") a publicat Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor (denumită în continuare „Propunerea" sau „propunerea de Regulament").[4]

2. Propunerea a fost elaborată ca urmare a adoptării Regulamentului (UE) 2021/1232 privind o derogare temporară de la anumite dispoziții ale Directivei 2002/58/CE în ceea ce privește utilizarea tehnologiilor de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere pentru prelucrarea datelor cu caracter personal și a altor date în scopul combaterii abuzului sexual online asupra copiilor („Regulamentul Provizoriu")[5]. Regulamentul Provizoriu nu impune furnizorilor de servicii relevanți să instituie măsuri de detectare a materialelor care conțin abuzuri sexuale asupra copiilor („MASC") (de exemplu, imagini, videoclipuri etc.) sau a cazurilor de ademenire a copiilor (cunoscută și sub denumirea de „grooming") în cadrul serviciilor lor, dar permite acestor furnizori să facă acest lucru în mod voluntar, în conformitate cu condițiile stabilite în Regulamentul respectiv.[6]

---

[1] JO L 295, 21.11.2018, p. 39.
[2] Trimiterile la „statele membre" din acest document trebuie înțelese ca trimiteri la „statele membre ale SEE".
[3] Propunerea de Regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor, COM(2022) 209 final.
[4] Ibid.
[5] Regulamentul (UE) 2021/1232 al Parlamentului European și al Consiliului din 14 iulie 2021 privind o derogare temporară de la anumite dispoziții ale Directivei 2002/58/CE în ceea ce privește utilizarea tehnologiilor de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere pentru prelucrarea datelor cu caracter personal și a altor date în scopul combaterii abuzului sexual online asupra copiilor, JO [2021] L 274/41.
[6] A se vedea, de asemenea, Avizul AEPD nr. 7/2020 privind Propunerea de derogare temporară de la Directiva 2002/58/CE în scopul combaterii abuzului sexual online asupra copiilor (10 noiembrie 2020).

3. Propunerea este formată din două componente principale. În primul rând, propunerea impune obligații specifice furnizorilor de servicii de găzduire, de servicii de comunicații interpersonale și de alte servicii în ceea ce privește detectarea, raportarea, eliminarea și blocarea materialelor online cunoscute și noi care conțin abuzuri sexuale asupra copiilor, precum și a cazurilor de ademenire a copiilor. În al doilea rând, Propunerea prevede înființarea unei noi agenții descentralizate a UE („Centrul UE privind abuzul sexual asupra copiilor" sau „Centrul UE") și a unei rețele de Autorități naționale de Coordonare pentru problemele legate de abuzul sexual asupra copiilor, pentru a permite punerea în aplicare a propunerii de Regulament.[7]

4. După cum se recunoaște în Expunerea de Motive a Propunerii, măsurile cuprinse în Propunere ar afecta exercitarea drepturilor fundamentale ale utilizatorilor serviciilor în cauză. Aceste drepturi includ, în special, drepturile fundamentale la respectarea vieții private (inclusiv confidențialitatea comunicațiilor, ca parte a dreptului mai larg la respectarea vieții private și de familie), protecția datelor cu caracter personal și libertatea de exprimare și de informare.[8]

5. În plus, aceste măsuri propuse sunt menite să se bazeze pe legislația UE existentă în materie de protecție a datelor și a vieții private și, într-o anumită măsură, să o completeze. În acest context, în Expunerea de Motive se menționează că:

> „Propunerea se bazează pe Regulamentul General privind Protecția Datelor (RGPD). În practică, furnizorii tind să invoce diverse motive ale prelucrării prevăzute în RGPD pentru a efectua prelucrarea datelor cu caracter personal pe care o implică detectarea și raportarea în mod voluntar a abuzului sexual online asupra copiilor. Propunerea stabilește un sistem de ordine de detectare specifice și precizează condițiile de detectare, asigurând un grad sporit de securitate juridică pentru aceste activități. În ceea ce privește activitățile obligatorii de detectare care implică prelucrarea datelor cu caracter personal, propunerea, în special ordinele de detectare emise pe baza acesteia, stabilește, prin urmare, motivul unei astfel de prelucrări menționate la articolul 6 alineatul (1) litera (c) din RGPD, care prevede prelucrarea datelor cu caracter personal ce este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului în temeiul dreptului Uniunii sau al dreptului intern.
>
> Propunerea vizează, printre altele, furnizorii care oferă servicii de comunicații electronice interpersonale și care, prin urmare, fac obiectul dispozițiilor naționale de punere în aplicare a Directivei asupra confidențialității și comunicațiilor electronice și a propunerii de revizuire a acesteia, pentru care se desfășoară negocieri. Măsurile prevăzute în propunere limitează în anumite privințe domeniul de aplicare al drepturilor și obligațiilor care decurg din dispozițiile relevante ale Directivei menționate, și anume în ceea ce privește activitățile care sunt strict necesare pentru executarea ordinelor de detectare. În acest sens, propunerea implică aplicarea, prin analogie, a articolului 15 alineatul (1) din Directiva menționată."[9]

6. Având în vedere gravitatea interferențelor preconizate cu drepturile fundamentale, Propunerea are o importanță deosebită pentru protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Astfel, la 12 mai 2022, Comisia a decis să consulte Comitetul European pentru Protecția Datelor („CEPD") și Autoritatea Europeană pentru Protecția Datelor („AEPD"), în conformitate cu articolul 42 alineatul (2) din RPDUE.

---

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

2. DOMENIUL DE APLICARE AL AVIZULUI

7. Prezentul aviz comun prezintă opiniile comune ale CEPD și ale AEPD cu privire la Propunere. Acesta se limitează la aspectele Propunerii referitoare la protecția vieții private și a datelor cu caracter personal. În special, avizul comun evidențiază domeniile în care Propunerea nu asigură o protecție suficientă a drepturilor fundamentale la viață privată și la protecția datelor sau necesită o aliniere suplimentară la cadrul juridic al UE privind protecția vieții private și a datelor cu caracter personal.

8. După cum se explică în continuare în prezentul aviz comun, Propunerea ridică serioase îngrijorări cu privire la necesitatea și proporționalitatea interferențelor și a limitărilor avute în vedere în raport cu protecția drepturilor fundamentale la viață privată și la protecția datelor cu caracter personal. Cu toate acestea, scopul prezentului aviz comun nu este nici de a furniza o listă exhaustivă a tuturor problemelor legate de protecția vieții private și a datelor ridicate de Propunere, nici de a oferi sugestii specifice pentru îmbunătățirea formulării propunerii. În schimb, prezentul aviz comun face observații la nivel înalt cu privire la principalele probleme ridicate de Propunere identificate de către CEPD și AEPD. Cu toate acestea, CEPD și AEPD rămân disponibile pentru a furniza observații și recomandări suplimentare colegiuitorilor pe parcursul procesului legislativ privind Propunerea.

3. OBSERVAȚII GENERALE PRIVIND DREPTUL LA CONFIDENȚIALITATEA COMUNICAȚIILOR ȘI LA PROTECȚIA DATELOR CU CARACTER PERSONAL

9. Confidențialitatea comunicațiilor este un element esențial al dreptului fundamental la respectarea vieții private și de familie, astfel cum este consacrat la articolul 7 din Carta Drepturilor Fundamentale a Uniunii Europene („Carta”).[10] În plus, articolul 8 din Cartă recunoaște dreptul fundamental la protecția datelor cu caracter personal. Dreptul la confidențialitatea comunicațiilor și dreptul la viața privată și de familie sunt, de asemenea, garantate la articolul 8 din Convenția Europeană a Drepturilor Omului („CEDO”) și fac parte din tradițiile constituționale comune ale statelor membre.[11]

10. CEPD și AEPD reamintesc că drepturile consacrate la articolele 7 și 8 din Cartă nu sunt drepturi absolute, ci trebuie luate în considerare în raport cu funcția lor în societate.[12] Abuzul sexual asupra copiilor este o infracțiune deosebit de gravă și odioasă, iar obiectivul de a permite o acțiune eficientă pentru a-l combate reprezintă un obiectiv de interes general recunoscut de Uniune și urmărește să protejeze drepturile și libertățile victimelor. În ceea ce privește acțiunile eficiente de combatere a infracțiunilor comise împotriva minorilor și a altor persoane vulnerabile, Curtea de Justiție a Uniunii Europene („CJUE”) a subliniat că din articolul 7 din Cartă pot rezulta obligații pozitive, care impun

[10] A se vedea, de exemplu, Declarația CEPD referitoare la revizuirea Regulamentului privind viața privată și comunicațiile electronice și la impactul acestuia asupra protecției persoanelor în ceea ce privește viața privată și confidențialitatea comunicațiilor acestora (25 mai 2018).
[11] Aproape toate constituțiile europene includ un drept care protejează confidențialitatea comunicațiilor. A se vedea, de exemplu, articolul 15 din Constituția Republicii Italiene; articolul 10 din Legea fundamentală a Republicii Federale Germania; articolul 22 din Constituția Belgiei; și articolul 13 din Constituția Regatului Țărilor de Jos.
[12] A se vedea, printre altele, Hotărârea CJUE pronunțată în cauza Facebook Ireland și Schrems, C-311/18, punctul 172 și jurisprudența citată în cadrul acesteia. A se vedea, de asemenea, considerentul 4 din RGPD.

autorităților publice să adopte măsuri legale pentru a proteja viața privată și de familie, domiciliul și comunicațiile. Astfel de obligații pot rezulta, de asemenea, din articolele 3 și 4 din Cartă, în ceea ce privește protecția integrității fizice și psihice a unei persoane și interzicerea torturii și a tratamentelor inumane și degradante.[13]

11. În același timp, orice restrângere a drepturilor garantate prin Cartă, precum cele avute în vedere de Propunere[14], trebuie să respecte cerințele prevăzute la articolul 52 alineatul (1) din Cartă. Orice măsură care interferează cu dreptul la confidențialitatea comunicațiilor și cu dreptul la viața privată și de familie trebuie să respecte în primul rând esența drepturilor în cauză.[15] Esența unui drept este afectată în cazul în care dreptul este golit de conținutul său de bază, iar persoana respectivă nu îl poate exercita[16]. Interferența nu poate constitui, în raport cu scopul urmărit, o situație atât de disproporționată și intolerabilă, care să afecteze însăși substanța dreptului astfel garantat.[17] Aceasta înseamnă că până și un drept fundamental care nu are un caracter absolut, cum ar fi dreptul la confidențialitatea comunicațiilor și dreptul la protecția datelor cu caracter personal, are unele componente de bază care nu pot fi limitate.

12. CJUE a aplicat în mai multe rânduri testul privind „conținutul esențial al unui drept" în domeniul confidențialității comunicațiilor electronice. În cauza Tele2 Sverige și Watson, Curtea a hotărât că o reglementare care nu permite păstrarea conținutului unei comunicări nu este de natură să aducă atingere conținutului esențial al dreptului la viață privată și la protecția datelor cu caracter personal.[18] În cauza Schrems, Curtea a considerat că o reglementare care permite autorităților publice să aibă acces în mod generalizat la conținutul comunicațiilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din Cartă[19]. În cauza Digital Rights Ireland și Seitlinger și alții, Curtea a constatat că, deși păstrarea datelor impusă de Directiva 2006/24 a constituit o interferență deosebit de gravă cu dreptul fundamental la viață privată și cu celelalte drepturi prevăzute la articolul 7 din Cartă, aceasta nu a fost de natură să aducă atingere substanței acestor drepturi, întrucât Directiva nu permitea cunoașterea conținutului comunicațiilor electronice ca atare.[20] Din această jurisprudență se poate deduce că măsurile care permit autorităților publice să aibă acces în mod generalizat la conținutul unei comunicații sunt mai susceptibile de a afecta esența drepturilor garantate la articolele 7 și 8 din Cartă. Aceste considerații sunt la fel de relevante și în ceea ce privește măsurile de detectare a MASC și a cazurilor de ademenire a copiilor, precum cele avute în vedere de Propunere.

13. În plus, CJUE a constatat că măsurile privind securitatea datelor joacă un rol esențial pentru a asigura că substanța dreptului fundamental la protecția datelor cu caracter personal prevăzut la articolul 8

---

[13] CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, punctele 126-128. A se vedea, de asemenea, Avizul AEPD nr. 7/2020 privind Propunerea de derogare temporară de la Directiva 2002/58/CE în scopul combaterii abuzului sexual online asupra copiilor (10 noiembrie 2020), punctul 12.

[14] A se vedea COM(2022) 209 final, p. 12 și 13.

[15] Articolul 52 alineatul (1) din Cartă.

[16] A se vedea „ Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal (19 decembrie 2019), p. 8, document disponibil la adresa https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[17] CJUE, cauza C-393/19, OM, punctul 53.

[18] CJUE, cauzele conexate C-203/15 și C-698/15, Tele2 Sverige și Watson, punctul 101.

[19] CJUE, cauza C-362/14, Schrems, punctul 94.

[20] CJUE, cauzele conexate C- 293/12 și C- 594/12, Digital Rights Ireland și Seitlinger și alții, punctul 39.

din Cartă nu este afectată în mod negativ.[21] În era digitală, soluțiile tehnice de securizare și de protecție a confidențialității comunicațiilor electronice, inclusiv măsurile de criptare, sunt esențiale pentru a asigura exercitarea tuturor drepturilor fundamentale.[22] Acest lucru ar trebui să fie avut în vedere în mod corespunzător atunci când se evaluează măsurile de detectare obligatorie a MASC sau a cazurilor de ademenire a copiilor, în special dacă acestea ar avea ca rezultat slăbirea sau degradarea criptării.[23]

14. Articolul 52 alineatul (1) din Cartă prevede, de asemenea, că orice restrângere a exercițiului unui drept fundamental garantat de Cartă trebuie să fie prevăzută de lege. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.[24] Pentru a îndeplini cerința proporționalității, legislația trebuie să prevadă norme clare și precise care să reglementeze domeniul de aplicare și aplicarea măsurilor în cauză și să impună garanții minime, pentru ca persoanele ale căror date cu caracter personal sunt afectate să aibă suficiente garanții că datele lor vor fi protejate în mod eficient împotriva riscului de abuz.[25] Respectiva reglementare trebuie să indice în ce împrejurări și în ce condiții o măsură care prevede prelucrarea unor asemenea date poate fi luată, garantând în acest mod că o ingerință este limitată la strictul necesar.[26] După cum a clarificat CJUE, necesitatea unor astfel de garanții este cu atât mai mare atunci când datele cu caracter personal sunt supuse unei prelucrări automate și atunci când este în joc protecția unei categorii particulare de date cu caracter personal, care sunt date sensibile.[27]

15. Propunerea ar limita exercitarea drepturilor și obligațiilor prevăzute la articolul 5 alineatele (1) și (3) și la articolul 6 alineatul (1) din Directiva 2002/58/CE („Directiva asupra confidențialității și comunicațiilor electronice")[28] în măsura în care acest lucru este necesar pentru executarea ordinelor de detectare emise în conformitate cu secțiunea 2 din capitolul 1 al Propunerii. CEPD și AEPD consideră că este, prin urmare, necesar să se evalueze Propunerea nu numai în lumina Cartei și a RGPD, ci și în lumina articolelor 5 și 6 și al articolului 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.

[21] Ibid., punctul 40.
[22] A se vedea Rezoluția 47/16 a Consiliului pentru Drepturile Omului privind promovarea, protecția și exercitarea drepturilor omului pe internet, documentul ONU A/HRC/RES/47/16 (26 iulie 2021).
[23] A se vedea și Considerentul 25 din Regulamentul Provizoriu.
[24] A se vedea Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente, 11 aprilie 2019, disponibilă la adresa https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] CJUE, cauzele conexate C-511/18, C-512/18 și C-520/18, La Quadrature du Net și alții, punctul 132.
[26] Ibid.
[27] Ibid.
[28] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), astfel cum a fost modificată prin Directiva 2006/24/CE și Directiva 2009/136/CE.

4. OBSERVAȚII SPECIFICE

4.1 Relația cu legislația în vigoare

4.1.1 Relația cu RGPD și cu Directiva asupra confidențialității și comunicațiilor electronice

16. Propunerea precizează că nu aduce atingere normelor care rezultă din alte acte ale Uniunii, în special RGPD [29] și Directiva asupra confidențialității și comunicațiilor electronice. Spre deosebire de Regulamentul Provizoriu, Propunerea nu prevede o derogare temporară explicită de la exercitarea drepturilor și obligațiilor prevăzute la articolul 5 alineatul (1), articolul 5 alineatul (3) și articolul 6 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, ci o restrângere a exercitării acestora. În plus, ar trebui remarcat că Regulamentul Provizoriu prevede o derogare exclusiv de la dispozițiile articolului 5 alineatul (1) și ale articolului 6 alineatul (1), și nu de la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice.

17. Propunerea se referă, de asemenea, la articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, care permite statelor membre să adopte măsuri legislative pentru a restrânge domeniul de aplicare al drepturilor și obligațiilor prevăzute la articolele 5 și 6 din Directiva respectivă, atunci când o astfel de restrângere constituie o măsură necesară, corespunzătoare și proporțională într-o societate democratică, printre altele, pentru prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor. În conformitate cu Propunerea, articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice se aplică prin analogie în cazul în care Propunerea limitează exercitarea drepturilor și obligațiilor prevăzute la articolul 5 alineatul (1), la articolul 5 alineatul (3) și la articolul 6 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice.

18. CEPD și AEPD reamintesc că CJUE a precizat că articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice trebuie interpretat în sens strict, ceea ce înseamnă că excepția de la principiul confidențialității comunicațiilor pe care o permite articolul 15 alineatul (1) trebuie să rămână o excepție și nu trebuie să devină o regulă. [30] După cum se subliniază în continuare în prezentul aviz comun, CEPD și AEPD consideră că Propunerea nu îndeplinește cerințele de (strictă) necesitate, eficacitate și proporționalitate. În plus, CEPD și AEPD concluzionează că Propunerea ar implica faptul că interferența cu confidențialitatea comunicațiilor ar putea deveni, de fapt, regula, în loc să rămână o excepție.

4.1.2 Relația cu Regulamentul (UE) 2021/1232 și impactul asupra detectării voluntare a abuzurilor sexuale online asupra copiilor

19. În conformitate cu articolul 88 din Propunere, aceasta din urmă ar urma să abroge Regulamentul Provizoriu, care prevede o derogare temporară de la anumite dispoziții ale Directivei asupra confidențialității și comunicațiilor electronice pentru a permite utilizarea voluntară de către furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere a tehnologiilor de detectare a

[29] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) (JO L 119, 4.5.2016, p. 1–88).
[30] Hotărârea din 21 decembrie 2016, Tele2 Sverige AB and Watson, cauzele conexate C-203/15 și C-698/15, punctul 89.

MASC și a cazurilor de ademenire a copiilor. Astfel, de la data aplicării propunerii de Regulament, nu ar exista nicio derogare de la Directiva asupra confidențialității și comunicațiilor electronice care să permită detectarea voluntară de către respectivii furnizori a abuzurilor sexuale online asupra copiilor.

20. Având în vedere că obligațiile de detectare introduse prin Propunere s-ar aplica numai destinatarilor ordinelor de detectare, ar fi important să se precizeze în textul propunerii de Regulament că utilizarea voluntară a tehnologiilor pentru detectarea MASC și a cazurilor de ademenire a copiilor rămâne permisă numai în măsura în care este permisă în temeiul Directivei asupra confidențialității și comunicațiilor electronice și al RGPD. Acest lucru ar implica, de exemplu, faptul că furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere nu ar putea să utilizeze astfel de tehnologii în mod voluntar, cu excepția cazului în care acest lucru ar fi permis de legislația națională care transpune Directiva asupra confidențialității și comunicațiilor electronice, în conformitate cu articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice și cu Carta.

21. În general, propunerea de Regulament ar beneficia de o mai mare claritate în ceea ce privește statutul detectării voluntare a abuzurilor sexuale online asupra copiilor după data aplicării propunerii de Regulament, precum și în ceea ce privește tranziția de la regimul de detectare voluntară prevăzut în Regulamentul Provizoriu la obligațiile de detectare prevăzute în propunerea de Regulament. De exemplu, CEPD și AEPD recomandă să se precizeze că propunerea de Regulament nu prevede un temei legal pentru prelucrarea datelor cu caracter personal în scopul exclusiv al detectării pe bază voluntară a abuzurilor sexuale online asupra copiilor.

4.2 Temeiul juridic în conformitate cu RGPD

22. Propunerea vizează stabilirea unui temei legal, în sensul RGPD, pentru prelucrarea datelor cu caracter personal în vederea detectării MASC și a „groomingului". În consecință, în Expunerea de Motive se menționează: „În ceea ce privește activitățile obligatorii de detectare care implică prelucrarea datelor cu caracter personal, propunerea, în special ordinul de detectare emis pe baza acesteia, stabilește, prin urmare, temeiul unei astfel de prelucrări menționate la articolul 6 alineatul (1) litera (c) din RGPD, care prevede prelucrarea datelor cu caracter personal ce este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului în temeiul dreptului Uniunii sau al dreptului intern."[31]

23. CEPD și AEPD salută decizia Comisiei de a elimina insecuritatea juridică cu privire la temeiul juridic al prelucrării datelor cu caracter personal, care a apărut în Regulamentul Provizoriu. De asemenea, CEPD și AEPD sunt de acord cu concluzia Comisiei potrivit căreia consecințele punerii în aplicare a măsurilor de detectare sunt prea profunde și prea grave pentru a lăsa la latitudinea furnizorilor de servicii decizia de a pune sau nu în aplicare astfel de măsuri.[32] În același timp, CEPD și AEPD remarcă faptul că orice temei juridic care îi obligă pe furnizorii de servicii să intervină asupra drepturilor fundamentale la protecția datelor și a vieții private va fi valabil numai în măsura în care respectă condițiile prevăzute la articolul 52 alineatul (1) din Cartă, astfel cum se analizează în secțiunile următoare.

4.3 Obligațiile de evaluare și atenuare a riscurilor

24. În conformitate cu capitolul II secțiunea 1 din Propunere, furnizorii de servicii de găzduire și furnizorii de servicii de comunicații interpersonale trebuie să identifice, să analizeze și să evalueze, pentru fiecare astfel de serviciu pe care îl oferă, riscul utilizării serviciului în scopul abuzului sexual online

[31] Ibid., p. 4.
[32] A se vedea Propunerea, COM(2022) 209 final, p. 14.

asupra copiilor, iar apoi să încerce să reducă la minimum riscul identificat prin aplicarea unor „măsuri de atenuare rezonabile, adaptate la riscul identificat”.

25. CEPD și AEPD menționează că, atunci când efectuează o evaluare a riscurilor, furnizorul ar trebui să ia în considerare în special elementele enumerate la articolul 3 alineatul (2) literele (a)-(e) din Propunere, inclusiv: interdicțiile și restricțiile prevăzute în condițiile generale de utilizare ale furnizorului; modul în care utilizatorii utilizează serviciul și impactul acestuia asupra riscului respectiv; modul în care furnizorul a conceput și prestează serviciul, inclusiv modelul de afaceri, guvernanța și sistemele și procesele relevante, precum și impactul acestora asupra riscului respectiv. În ceea ce privește riscul de ademenire a copiilor, elementele propuse pentru a fi luate în considerare sunt: măsura în care serviciul este utilizat sau este susceptibil de a fi utilizat de către copii; grupele de vârstă și riscul de ademenire în funcție de grupa de vârstă; disponibilitatea unor funcționalități care permit căutarea de către utilizator, funcționalități care permit utilizatorilor să stabilească contacte directe cu alți utilizatori, în special prin intermediul comunicării private și funcționalități care permit utilizatorilor să partajeze imagini sau videoclipuri cu alți utilizatori.

26. Deși CEPD și AEPD recunosc că aceste criterii par relevante, CEPD și AEPD sunt totuși îngrijorate că aceste criterii lasă o marjă destul de largă de interpretare și apreciere. Mai multe criterii sunt descrise în termeni extrem de generici (de exemplu, „modul în care utilizatorii folosesc serviciul și impactul acestuia asupra respectivului risc”) sau se referă la funcționalități de bază care sunt comune multor servicii online (de exemplu, „utilizatorii pot partaja imagini sau materiale video cu alți utilizatori”). Ca atare, criteriile pot fi evaluate subiectiv (mai degrabă decât obiectiv).

27. În opinia CEPD și AEPD, același lucru este valabil și pentru măsurile de atenuare a riscurilor care trebuie luate în conformitate cu articolul 4 din Propunere. Măsuri cum ar fi adaptarea, prin măsuri tehnice și operaționale adecvate și prin dotarea cu personal, a sistemelor de moderare a conținutului sau de recomandare ale furnizorului par relevante pentru a reduce riscul identificat. Cu toate acestea, dacă sunt aplicate în cadrul unui proces complex de evaluare a riscurilor și combinate cu termeni abstracți și vagi pentru a descrie gradul acceptabil de risc (de exemplu, „măsură apreciabilă”), aceste criterii nu îndeplinesc criteriile de securitate juridică și de previzibilitate necesare pentru a justifica o interferență cu confidențialitatea comunicațiilor între persoane private, ceea ce constituie o interferență clară cu drepturile fundamentale la viață privată și la libertatea de exprimare.

28. Deși furnizorii nu sunt autorizați să intervină în confidențialitatea comunicațiilor ca parte a strategiilor lor de evaluare și de atenuare a riscurilor înainte de a primi un ordin de detectare, există o legătură directă între obligațiile de evaluare și de atenuare a riscurilor și obligațiile de detectare care decurg din acestea. Articolul 7 alineatul (4) din Propunere face ca emiterea unui ordin de detectare să depindă de existența dovezilor unui risc semnificativ ca serviciul în cauză să poată fi utilizat în scopul abuzului sexual online asupra copiilor. Înainte de emiterea unui ordin de detectare, trebuie urmat un proces complex care implică furnizorii, Autoritatea de Coordonare și autoritatea judiciară sau altă autoritate administrativă independentă responsabilă cu emiterea ordinului. În primul rând, furnizorii trebuie să evalueze riscul de utilizare a serviciilor lor în scopul abuzului sexual online asupra copiilor (articolul 3 din Propunere) și să evalueze posibilele măsuri de atenuare a riscurilor (articolul 4 din Propunere) pentru a reduce acest risc. Rezultatele acestui exercițiu urmează să fie apoi raportate Autorității de Coordonare competente (articolul 5 din Propunere). În cazul în care evaluarea riscurilor arată că, în ciuda eforturilor de atenuare a acestora, rămâne un risc semnificativ, Autoritatea de Coordonare îl audiază pe furnizor cu privire la un proiect de cerere de emitere a unui ordin de detectare și îi oferă acestuia posibilitatea de a formula observații. Furnizorul este obligat, de asemenea, să prezinte un plan de punere în aplicare, inclusiv un aviz din partea autorității competente pentru protecția datelor în cazul detectării unor situații de „grooming”. În cazul în care Autoritatea de Coordonare urmărește

cazul, se solicită și, în cele din urmă, se emite un ordin de detectare de către o instanță sau o altă autoritate administrativă independentă. Prin urmare, evaluarea inițială a riscurilor și măsurile alese pentru a reduce riscul identificat reprezintă un temei decisiv pentru evaluarea de către Autoritatea de Coordonare, precum și de către autoritatea judiciară sau administrativă competentă, a necesității unui ordin de detectare.

29. CEPD și AEPD iau act de etapele complexe care conduc la emiterea unui ordin de detectare, care includ o evaluare inițială a riscurilor de către furnizor și propunerea de măsuri de atenuare a riscurilor de către acesta, precum și interacțiunea ulterioară a furnizorului cu Autoritatea de Coordonare competentă. CEPD și AEPD consideră că există o posibilitate substanțială ca furnizorul să influențeze rezultatul procesului. În acest sens, CEPD și AEPD iau act de faptul că considerentul 17 din Propunere prevede că furnizorii ar trebui să poată indica, ca parte a raportării riscurilor, că „doresc și sunt pregătiți" să execute un eventual ordin de detectare emis. Prin urmare, nu se poate presupune că fiecare furnizor va încerca să evite emiterea unui ordin de detectare pentru a păstra confidențialitatea comunicațiilor utilizatorilor săi prin aplicarea celor mai eficiente, dar și a celor mai puțin intruzive măsuri de atenuare, în special în cazul în care astfel de măsuri de atenuare interferează cu libertatea furnizorului de a-și desfășura activitatea în conformitate cu articolul 16 din Cartă.

30. CEPD și AEPD ar dori să sublinieze că garanțiile procedurale nu pot înlocui niciodată în totalitate garanțiile de fond. Astfel, procesul complex care duce la posibila emitere a unui ordin de detectare descris mai sus ar trebui să fie însoțit de obligații de fond clare. CEPD și AEPD consideră că Propunerea nu este clară în ceea ce privește mai multe elemente-cheie (de exemplu, noțiunile de „risc semnificativ", „măsură apreciabilă" etc.), care nu pot fi remediate prin prezența mai multor niveluri de garanții procedurale. Acest lucru este cu atât mai relevant cu cât entitățile însărcinate cu aplicarea acestor garanții (de exemplu, furnizorii, autoritățile judiciare etc.) se bucură de o marjă largă de apreciere în ceea ce privește modul de stabilire a echilibrului între drepturile în discuție în fiecare caz în parte. Având în vedere interferențele extinse cu drepturile fundamentale care ar decurge din adoptarea Propunerii, legiuitorul ar trebui să se asigure că Propunerea oferă mai multă claritate cu privire la situațiile în care sunt permise astfel de interferențe. Deși recunosc că măsurile legislative nu pot fi prea prescriptive și trebuie să lase o anumită flexibilitate în aplicarea lor practică, CEPD și AEPD consideră că textul actual al Propunerii lasă prea mult loc pentru posibile abuzuri din cauza lipsei unor norme de fond clare.

31. Având în vedere potențialul impact semnificativ asupra unui număr foarte mare de persoane vizate (și anume potențial toți utilizatorii de servicii de comunicații interpersonale), CEPD și AEPD subliniază necesitatea unui nivel ridicat de securitate juridică, claritate și previzibilitate a legislației pentru a se asigura că măsurile propuse sunt cu adevărat eficiente în atingerea obiectivului pe care îl urmăresc și, în același timp, sunt cât mai puțin dăunătoare pentru drepturile fundamentale în discuție.

4.4 Condiții pentru emiterea ordinelor de detectare

32. Articolul 7 din Propunere prevede că Autoritatea de Coordonare din statul membru de stabilire va avea competența de a solicita autorității judiciare competente sau unei alte autorități administrative independente din statul membru respectiv să emită un ordin de detectare prin care să solicite unui furnizor de servicii de găzduire sau unui furnizor de servicii de comunicații interpersonale să ia măsurile specificate la articolul 10 pentru a detecta abuzurile sexuale online asupra copiilor pe un anumit serviciu.

33. CEPD și AEPD țin seama în mod corespunzător de următoarele elemente care trebuie îndeplinite înainte de emiterea unui ordin de detectare:

a. există dovezi ale unui risc semnificativ ca serviciul să fie utilizat în scopul abuzului sexual online asupra copiilor, în sensul articolului 7 alineatele (5), (6) sau (7), după caz;

b. motivele pentru emiterea ordinului de detectare depășesc consecințele negative pentru drepturile și interesele legitime ale tuturor părților afectate, având în vedere în special necesitatea de a asigura un echilibru echitabil între drepturile fundamentale ale acestor părți.

34. Semnificația conceptului de risc semnificativ este specificată la articolul 7 alineatul (5) și următoarele, în funcție de tipul de ordin de detectare în cauză. Riscul semnificativ este asumat în cazul ordinelor de detectare privind detectarea MASC cunoscute dacă:

a. în pofida oricăror măsuri de atenuare pe care furnizorul le-a luat sau le va lua, este probabil ca serviciul să fie utilizat, într-o măsură apreciabilă, pentru difuzarea de materiale cunoscute care conțin abuzuri sexuale asupra copiilor; și

b. există dovezi că serviciul sau un serviciu comparabil, în cazul în care serviciul nu a fost încă oferit în Uniune la data cererii de emitere a ordinului de detectare, a fost utilizat în ultimele 12 luni și într-o măsură apreciabilă pentru difuzarea de materiale cunoscute conținând abuzuri sexuale asupra copiilor.

35. Pentru a emite un ordin de detectare pentru MASC necunoscute, probabilitatea și dovezile factuale trebuie să se refere la MASC necunoscute, iar un ordin de detectare prealabil pentru MASC cunoscute trebuie să fi fost emis și să fi condus la un număr semnificativ de rapoarte privind MASC prezentate de către furnizor [articolul 7 alineatul (6) din Propunere]. În ceea ce privește un ordin de detectare referitor la ademenirea copiilor, se va considera că există un risc semnificativ atunci când furnizorul se califică drept furnizor de servicii de comunicații interpersonale, este probabil ca serviciul să fie utilizat într-o măsură apreciabilă pentru ademenirea copiilor și există dovezi că serviciul a fost utilizat într-o măsură apreciabilă pentru ademenirea copiilor [articolul 7 alineatul (7) din Propunere].

36. CEPD și AEPD observă că, în pofida specificațiilor de la articolul 7 alineatele (5)-(7) din Propunere, condițiile pentru emiterea unui ordin de detectare sunt dominate de termeni juridici vagi, cum ar fi „măsură apreciabilă", „număr semnificativ", și sunt parțial repetitive, deoarece dovezile de abuzuri anterioare vor contribui adesea la stabilirea probabilității de abuzuri viitoare.

37. Propunerea are în vedere un sistem prin care, atunci când se decide dacă este necesar un ordin de detectare, trebuie să se ia o decizie predictivă cu privire la utilizarea viitoare a unui serviciu în scopul abuzului sexual online asupra copiilor. Prin urmare, este de înțeles că elementele prevăzute la articolul 7 au un caracter de prognoză. Cu toate acestea, noțiunile vagi utilizate în cadrul Propunerii fac dificilă pentru furnizori, precum și pentru autoritatea judiciară competentă sau altă autoritate administrativă independentă abilitată aplicarea cerințelor legale introduse de Propunere într-un mod previzibil și nearbitrar. CEPD și AEPD sunt îngrijorate de faptul că aceste noțiuni largi și vagi vor duce la o lipsă de securitate juridică și vor conduce, de asemenea, la divergențe considerabile în punerea în aplicare concretă a Propunerii în întreaga Uniune, în funcție de interpretările care vor fi date unor noțiuni precum „probabilitate" și „măsură apreciabilă" de către autoritățile judiciare sau alte autorități administrative independente din statele membre. Un astfel de rezultat nu ar fi acceptabil, având în vedere faptul că dispozițiile privind ordinele de detectare pentru furnizorii de servicii de comunicații interpersonale vor constitui „restrângeri" ale principiului confidențialității comunicațiilor prevăzut la articolul 5 din Directiva asupra confidențialității și comunicațiilor electronice, iar claritatea și previzibilitatea acestora sunt, prin urmare, de o importanță majoră pentru a se asigura că aceste restrângeri sunt aplicate în mod uniform în întreaga Uniune.

4.5 Analiza necesității și proporționalității măsurilor preconizate[33]

38. După cum s-a indicat mai sus, pot fi emise trei tipuri de ordine de detectare: ordine de detectare privind diseminarea de materiale cunoscute care conțin abuzuri sexuale asupra copiilor [articolul 7 alineatul (5) din Propunere], ordine de detectare privind diseminarea de materiale noi care conțin abuzuri sexuale asupra copiilor [articolul 7 alineatul (6) din Propunere] și ordine de detectare privind ademenirea copiilor [articolul 7 alineatul (7) din Propunere]. Fiecare ordin de detectare ar necesita, în mod normal, o tehnologie diferită pentru punerea sa în practică. În consecință, acestea au un nivel diferit de intruziune și, prin urmare, un impact diferit asupra dreptului la viață privată și la protecția datelor cu caracter personal.

39. Tehnologiile de detectare a materialelor cunoscute care conțin abuzuri sexuale asupra copiilor sunt, de obicei, tehnologii de potrivire, în sensul că acestea se bazează pe o bază de date existentă cu materiale cunoscute care conțin abuzuri sexuale asupra copiilor cu care pot compara imagini (inclusiv imagini statice din videoclipuri). Pentru a permite potrivirea, imaginile prelucrate de furnizor, precum și imaginile din baza de date trebuie să fie digitalizate, de obicei prin conversia lor în valori de dispersie. Acest tip de tehnologie de dispersie are o rată estimată de rezultate fals pozitive de cel mult 1 la 50 de miliarde (adică o rată de rezultate fals pozitive de 0,000000002 %). [34]

40. Pentru detectarea de noi MASC, se utilizează de obicei un alt tip de tehnologie, inclusiv clasificatori și inteligența artificială (IA). [35] Cu toate acestea, ratele de eroare ale acestora sunt, în general, semnificativ mai mari. De exemplu, Raportul de Evaluare a Impactului indică faptul că există tehnologii de detectare a noilor MASC a căror rată de precizie poate fi stabilită la 99,9 % (adică o rată de 0,1 % a rezultatelor fals pozitive), dar cu această rată de precizie acestea sunt capabile să identifice doar 80 % din totalul MASC din setul de date relevant. [36]

41. În ceea ce privește detectarea cazurilor de ademenire a copiilor în comunicațiile bazate pe text, Raportul de Evaluare a Impactului explică faptul că aceasta se bazează în mod obișnuit pe detectarea tiparelor. Raportul de Evaluare a Impactului observă că unele dintre tehnologiile existente pentru detectarea cazurilor de „grooming" au o „rată de precizie" de 88 %.[37]. Potrivit Comisiei, acest lucru înseamnă că „din cele 100 de conversații semnalate ca eventuale infracțiuni de ademenire a copiilor, 12 pot fi excluse în urma analizei [conform propunerii, de către Centrul UE] și nu vor fi raportate autorităților de aplicare a legii". [38] Cu toate acestea, chiar dacă – spre deosebire de Regulamentul Provizoriu – Propunerea s-ar aplica și comunicațiilor audio, Raportul de Evaluare a Impactului nu detaliază soluțiile tehnologice care ar putea fi utilizate pentru a detecta cazurile de „grooming" într-un astfel de cadru.

---

[33] A se vedea și Ghidul rapid al AEPD privind necesitatea și proporționalitatea, disponibil la adresa: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

[34] A se vedea Comisia Europeană, Document de lucru al serviciilor Comisiei, Raport de evaluare a impactului care însoțește documentul intitulat „Propunere de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor, SWD(2022) 209 final" [denumit în continuare „raport de evaluare a impactului" sau „SWD(2022) 209 final"], p. 281, nota de subsol 511.

[35] Raportul de Evaluare a Impactului, p. 281.

[36] Ibid., p. 282.

[37] Ibid., p. 283.

[38] Propunere, COM(2022) 209 final, p. 14, nota de subsol 32.

4.5.1 Eficacitatea detectării

42. Necesitatea implică nevoia unei evaluări bazate pe fapte a eficacității măsurilor avute în vedere pentru atingerea obiectivului urmărit și a faptului dacă acestea sunt mai puțin intruzive decât alte opțiuni pentru atingerea aceluiași obiectiv.[39] Un alt factor care trebuie luat în considerare în evaluarea proporționalității unei măsuri propuse este eficacitatea măsurilor existente pe lângă cea propusă.[40] În cazul în care există deja măsuri pentru același scop sau pentru un scop similar, eficacitatea acestora ar trebui să fie evaluată ca parte a evaluării proporționalității. Fără o astfel de evaluare a eficacității măsurilor existente care urmăresc același scop sau un scop similar, nu se poate considera că testul de proporționalitate pentru o nouă măsură a fost efectuat în mod corespunzător.

43. Detectarea MASC sau a cazurilor de „grooming" de către furnizorii de servicii de găzduire și furnizorii de servicii de comunicații interpersonale poate contribui la obiectivul general de prevenire și combatere a abuzului sexual asupra copiilor și a difuzării online a materialelor care conțin abuzuri sexuale asupra copiilor. În același timp, necesitatea de a evalua eficacitatea măsurilor prevăzute în Propunere generează trei întrebări-cheie:

- Măsurile de detectare a abuzurilor sexuale online asupra copiilor pot fi ușor de eludat?
- Care este efectul pe care activitățile de detectare îl vor avea asupra acțiunilor întreprinse de autoritățile de aplicare a legii?[41]
- Cum ar reduce Propunerea insecuritatea juridică?

44. Nu este de competența CEPD și AEPD să răspundă în detaliu la aceste întrebări. Cu toate acestea, CEPD și AEPD constată că nici Raportul de Evaluare a Impactului, nici Propunerea nu răspund pe deplin la aceste întrebări.

45. În ceea ce privește posibilitatea de a eluda detectarea MASC, trebuie remarcat că, în prezent, nu pare să existe nicio soluție tehnologică pentru a detecta MASC care sunt partajate în formă criptată. Prin urmare, orice activitate de detectare – chiar și scanarea la nivelul clientului menită să eludeze criptarea de la un capăt la altul oferită de furnizor[42] – poate fi ușor eludată prin criptarea conținutului cu ajutorul unei aplicații separate înainte de a-l trimite sau de a-l încărca. Astfel, măsurile de detectare avute în vedere de Propunere ar putea avea un impact mai redus asupra diseminării MASC pe internet decât s-ar putea spera.

46. În plus, Comisia se așteaptă la o creștere a numărului de raportări ale abuzurilor sexuale asupra copiilor către autoritățile de aplicare a legii, odată cu adoptarea obligațiilor de detectare introduse prin Propunere.[43] Cu toate acestea, nici Propunerea, nici Raportul de Evaluare a Impactului nu explică modul în care se vor remedia deficiențele situației actuale. Având în vedere resursele limitate ale autorităților de aplicare a legii, pare necesar să se înțeleagă mai bine dacă creșterea numărului de

---

[39] AEPD, Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente, 11 aprilie 2017, p. 5; AEPD, Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, (19 decembrie 2019), p. 8.

[40] AEPD, „Orientările AEPD privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal, (19 decembrie 2019), p. 11.

[41] Conform Raportului de Evaluare a Impactului, anexa II, p. 132, 85,71 % dintre respondenții la sondajul privind aplicarea legii și-au exprimat îngrijorarea cu privire la creșterea, în ultimul deceniu, a numărului de materiale care conțin abuzuri sexuale asupra copiilor și la lipsa de resurse (adică umane, tehnice).

[42] A se vedea și secțiunea 4.10 de mai jos.

[43] A se vedea, printre altele, Raportul de Evaluare a Impactului, anexa 3, SWD(2022) 209 final, p. 176.

rapoarte ar avea un impact semnificativ asupra activităților de aplicare a legii împotriva abuzurilor sexuale asupra copiilor. În orice caz, CEPD și AEPD doresc să sublinieze că astfel de rapoarte ar trebui evaluate în timp util pentru a se asigura că se ia o decizie privind relevanța penală a materialului raportat cât mai curând posibil și pentru a limita, pe cât posibil, reținerea de date irelevante.

4.5.2 Nicio măsură mai puțin intruzivă

47. Presupunând că efectele pozitive ale detectării MASC și ale cazurilor de „grooming", preconizate de Comisie, ar putea fi realizate, detectarea trebuie să fie cea mai puțin intruzivă dintre măsurile la fel de eficiente. Articolul 4 din Propunere prevede că, într-o primă etapă, furnizorii ar trebui să ia în considerare adoptarea de măsuri de atenuare pentru a reduce riscul de utilizare a serviciului lor în scopul abuzului sexual online asupra copiilor sub pragul care justifică emiterea unui ordin de detectare. În cazul în care există măsuri de atenuare care ar putea duce la o reducere substanțială a numărului de cazuri de „grooming" sau de MASC care fac obiectul schimburilor în cadrul serviciului în cauză, aceste măsuri ar fi adesea mai puțin intruzive în comparație cu un ordin de detectare[44]. Prin urmare, în cazul în care furnizorul relevant nu reușește să adopte astfel de măsuri în mod voluntar, ar trebui să fie posibil ca autoritatea administrativă independentă competentă sau autoritatea judiciară să facă obligatorie și executorie punerea în aplicare a măsurilor de atenuare, în loc să emită un ordin de detectare. În opinia CEPD și AEPD, faptul că articolul 5 alineatul (4) din Propunere permite Autorității de Coordonare să „solicite" furnizorului să introducă, să revizuiască, să întrerupă sau să extindă măsurile de atenuare nu este suficient, deoarece o astfel de cerință nu ar fi aplicabilă în mod independent, iar nerespectarea ar fi „sancționată" doar prin emiterea unui ordin de detectare.

48. Prin urmare, CEPD și AEPD consideră că Autoritatea de Coordonare sau autoritatea administrativă independentă competentă sau autoritatea judiciară ar trebui să fie împuternicită în mod explicit să impună măsuri de atenuare mai puțin intruzive înainte de emiterea unui ordin de detectare sau în locul acesteia.

4.5.3 Proporționalitatea în sens strict

49. Pentru ca o măsură să respecte principiul proporționalității consacrat la articolul 52 alineatul (1) din Cartă, avantajele care rezultă din măsură nu ar trebui să fie depășite de dezavantajele pe care măsura le provoacă în ceea ce privește exercitarea drepturilor fundamentale. Prin urmare, principiul proporționalității „limitează autoritățile în exercitarea competențelor lor, impunând stabilirea unui echilibru între mijloacele utilizate și scopul urmărit (sau rezultatul obținut)".[45]

50. Pentru a putea evalua impactul unei măsuri asupra drepturilor fundamentale la viața privată și la protecția datelor cu caracter personal, este deosebit de important să se identifice cu precizie: [46]

---

[44] De exemplu, ar putea fi avute în vedere măsuri precum blocarea la nivelul clientului a transmiterii de MASC prin împiedicarea încărcării și transmiterii conținutului comunicațiilor electronice, deoarece acestea ar putea ajuta în anumite contexte la prevenirea circulării MASC cunoscute.

[45] A se vedea cauza C-343/09, Afton Chemical, punctul 45; cauzele conexate C-92/09 și C-93/09, Volker und Markus Schecke și Hartmut Eifert, punctul 74; cauzele C-581/10 și C-629/10, Nelson și alții, punctul 71; cauza C-283/11, Sky Österreich, punctul 50; și cauza C-101/12, Schaible, punctul 29. A se vedea, de asemenea, AEPD, Evaluarea necesității măsurilor care limitează dreptul fundamental la protecția datelor cu caracter personal: un set de instrumente (11 aprilie 2017).

[46] AEPD, Orientări privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal) (19 decembrie 2019, p. 23.

- **domeniul de aplicare al măsurii**, inclusiv numărul de persoane afectate și dacă aceasta provoacă „intruziuni colaterale” (și anume interferența cu viața privată a altor persoane decât persoanele vizate de măsură);
- **amploarea măsurii**, inclusiv cantitatea de informații colectate; pentru cât timp; dacă măsura analizată necesită colectarea și prelucrarea unor categorii speciale de date;
- **nivelul de intruziune**, luând în considerare: natura activității care face obiectul măsurii (dacă aceasta afectează sau nu activitățile care fac obiectul obligației de confidențialitate, relația avocat-client; activitatea medicală); contextul; dacă acesta echivalează sau nu cu crearea de profiluri ale persoanelor în cauză; dacă prelucrarea implică utilizarea unui sistem automatizat de luare a deciziilor (parțial sau integral) cu o „marjă de eroare”;
- dacă este vorba de **persoane vulnerabile** sau nu;
- dacă afectează și **alte drepturi fundamentale** (de exemplu, dreptul la libertatea de exprimare, ca în cauzele Digital Rights Ireland și Seitlinger și alții și Tele2 Sverige și Watson).[47]

51. În acest context, este, de asemenea, important de remarcat că impactul poate fi minor în ceea ce privește persoana în cauză, dar totuși semnificativ sau foarte semnificativ la nivel colectiv/pentru societate în ansamblu.[48]

52. În cazul tuturor celor trei tipuri de ordine de detectare (detectarea MASC cunoscute, a MASC noi și a cazurilor de „grooming”), tehnologiile disponibile în prezent se bazează pe prelucrarea automată a datelor referitoare la conținut ale tuturor utilizatorilor afectați. Tehnologiile utilizate pentru a analiza conținutul sunt adesea complexe, implicând de obicei utilizarea inteligenței artificiale. Prin urmare, comportamentul acestei tehnologii este posibil să nu fie pe deplin inteligibil pentru utilizatorul serviciului. În plus, se știe că tehnologiile disponibile în prezent, în special cele pentru detectarea noilor MASC sau a cazurilor de „grooming”, au rate de eroare relativ ridicate.[49] Mai mult, există riscul de a fi raportat la Centrul UE în conformitate cu articolul 12 alineatul (1) și cu articolul 48 alineatul (1) din Propunere, pe baza detectării unui „potențial” MASC.

53. În plus, condițiile generale pentru emiterea unui ordin de detectare în temeiul Propunerii, și anume aplicarea acestuia la un întreg serviciu și nu doar la comunicări selectate[50], durata de până la 24 de luni pentru MASC cunoscute sau noi și de până la 12 luni pentru „grooming”[51] etc., pot duce la un domeniu de aplicare foarte larg al ordinului în practică. Ca urmare, monitorizarea ar fi de fapt generală și fără discriminare, și nu ar fi direcționată în practică.

54. Având în vedere cele de mai sus, CEPD și AEPD sunt, de asemenea, preocupate de posibilele efecte de intimidare a exercitării libertății de exprimare. CEPD și AEPD reamintesc că un astfel de efect de intimidare este considerat cu atât mai probabil cu cât legea este mai puțin clară.

---

[47] A se vedea, de asemenea, Avizul AEPD nr. 7/2020 privind Propunerea de derogare temporară de la Directiva 2002/58/CE în scopul combaterii abuzului sexual online asupra copiilor (10 noiembrie 2020), p. 9 și următoarele.

[48] AEPD, Orientări privind evaluarea proporționalității măsurilor care limitează drepturile fundamentale la viață privată și la protecția datelor cu caracter personal) (19 decembrie 2019, p. 20.

[49] A se vedea detaliile de mai sus, secțiunea 4.5, și de mai jos, subsecțiunea 4.8.2.

[50] A se vedea articolul 7 alineatul (1) din Propunere.

[51] A se vedea articolul 7 alineatul (9) al treilea paragraf din Propunere.

55. În lipsa specificității, a preciziei și a clarității necesare pentru a satisface cerința de securitate juridică[52] și având în vedere domeniul său larg de aplicare, și anume toți furnizorii de servicii relevante ale societății informaționale care oferă astfel de servicii în Uniune,[53] Propunerea nu garantează că va exista efectiv doar o abordare țintită a detectării MASC și a cazurilor de „grooming". Prin urmare, CEPD și AEPD consideră că, în practică, propunerea ar putea deveni baza unei scanări *de facto* generalizate și nediscriminatorii a conținutului tuturor tipurilor de comunicații electronice ale tuturor utilizatorilor din UE/SEE. În consecință, legislația ar putea determina oamenii să se abțină de la a partaja conținut legal de teamă că ar putea fi vizați pe baza acțiunii lor.

56. Acestea fiind spuse, CEPD și AEPD recunosc că diferite măsuri de combatere a abuzului sexual online asupra copiilor pot implica diferite niveluri de intruziune. Ca o chestiune preliminară, CEPD și AEPD observă că analiza automată a discursului sau a textului în vederea identificării unor potențiale cazuri de ademenire a copiilor este susceptibilă de a constitui o interferență mai semnificativă decât compararea imaginilor sau a videoclipurilor pe baza unor cazuri confirmate anterior de MASC în vederea detectării diseminării MASC. În plus, ar trebui să se facă o distincție între detectarea „MASC cunoscute" și a „noilor MASC". În plus, impactul ar trebui să fie diferențiat în continuare între măsurile adresate furnizorilor de servicii de găzduire și cele impuse furnizorilor de servicii de comunicații interpersonale.

4.5.4 Detectarea materialelor cunoscute care conțin abuzuri sexuale asupra copiilor

57. Deși, conform considerentului 4, Propunerea ar fi „neutră din punct de vedere tehnologic", atât eficacitatea măsurilor de detectare propuse, cât și impactul acestora asupra persoanelor fizice vor depinde în mare măsură de alegerea tehnologiei aplicate și de indicatorii selectați. Acest fapt este recunoscut de Comisie în Raportul de Evaluare a Impactului, anexa 8[54], și confirmat de alte studii, cum ar fi evaluarea de impact înlocuitoare specifică din februarie 2021 a Serviciului de cercetare al Parlamentului European privind Propunerea Comisiei de derogare temporară de la Directiva asupra confidențialității și comunicațiilor electronice în scopul combaterii abuzului sexual online asupra copiilor.[55]

58. Articolul 10 din Propunere stabilește o serie de cerințe pentru tehnologiile care urmează să fie utilizate în scopul detectării, în special privind eficacitatea, fiabilitatea și caracterul cât mai puțin intruziv al acestora în ceea ce privește impactul asupra drepturilor utilizatorilor la viața privată și de familie, inclusiv la confidențialitatea comunicațiilor, și la protecția datelor cu caracter personal.

59. În acest context, CEPD și AEPD constată că, în prezent, singurele tehnologii care par a fi în măsură să îndeplinească în general aceste standarde sunt cele utilizate pentru a detecta MASC cunoscute, și anume tehnologiile de potrivire care se bazează pe o bază de date a valorilor de dispersie ca referință.

---

[52] A se vedea CJUE, cauza C-197/96, Comisia Comunităților Europene/Republica Franceză, punctul 15.
[53] A se vedea articolul 1 alineatul (2) din Propunere.
[54] A se vedea informațiile privind ratele rezultatelor fals pozitive din raportul de evaluare a impactului, anexa 8, p. 279 și următoarele.
[55] A se vedea Propunerea Comisiei privind derogarea temporară de la Directiva asupra confidențialității și comunicațiilor electronice în scopul combaterii abuzurilor sexuale online asupra copiilor: o evaluare de impact înlocuitoare specifică (Serviciul de cercetare al Parlamentului European, februarie 2021), p. 14 și următoarele.

4.5.5 Detectarea materialelor necunoscute anterior care conțin abuzuri sexuale asupra copiilor

60. Evaluarea măsurilor care vizează detectarea MASC necunoscute anterior (noi) conduce la concluzii diferite în ceea ce privește eficacitatea, fiabilitatea și limitarea impactului asupra drepturilor fundamentale la viață privată și la protecția datelor.

61. În primul rând, după cum se explică în Raportul de Evaluare a Impactului ce însoțește Propunerea, tehnologiile utilizate în prezent pentru detectarea MASC necunoscute anterior includ clasificatorii și IA. Un clasificator este orice algoritm care sortează datele în clase etichetate sau categorii de informații, prin recunoașterea tiparelor.[56] Astfel, aceste tehnologii au rezultate și un impact diferite în ceea ce privește acuratețea, eficacitatea și nivelul de intruziune. În același timp, acestea sunt, de asemenea, mai predispuse la erori.

62. Tehnicile utilizate pentru a detecta MASC necunoscute anterior sunt similare cu cele utilizate pentru a detecta cazurile de ademenire a copiilor, deoarece ambele se bazează nu pe simple tehnologii de potrivire, ci pe modele predictive, utilizând tehnologii din domeniul inteligenței artificiale. CEPD și AEPD consideră că ar trebui să existe un nivel ridicat de precauție atunci când se detectează MASC necunoscute anterior, deoarece o eroare a sistemului ar avea consecințe grave pentru persoanele vizate, care ar fi semnalate în mod automat ca fiind posibil să fi comis o infracțiune foarte gravă, iar datele cu caracter personal și detaliile comunicațiilor lor ar fi raportate.

63. În al doilea rând, indicatorii de performanță găsiți în literatura de specialitate, dintre care unii sunt evidențiați în Raportul de Evaluare a Impactului care a însoțit Propunerea,[57] oferă foarte puține informații despre condițiile care au fost utilizate pentru calcularea lor și despre caracterul lor adecvat pentru condițiile din viața reală, ceea ce înseamnă că performanța lor în lumea reală ar putea fi semnificativ mai mică decât cea preconizată, ceea ce ar duce la o acuratețe mai scăzută și la un procent mai mare de rezultate fals pozitive.

64. În al treilea rând, indicatorii de performanță ar trebui să fie luați în considerare în contextul specific de utilizare a instrumentelor de detectare relevante și să ofere o perspectivă exhaustivă asupra comportamentului instrumentelor de detectare. Atunci când se utilizează algoritmi de inteligență artificială pe imagini sau texte, este bine documentat faptul că pot apărea prejudecăți și discriminări din cauza lipsei de reprezentativitate a anumitor grupuri de populație în datele utilizate pentru antrenarea algoritmului. Aceste prejudecăți ar trebui identificate, măsurate și reduse la un nivel acceptabil pentru ca sistemele de detectare să fie cu adevărat benefice pentru întreaga societate.

65. Deși a fost realizat un studiu al tehnologiilor utilizate pentru detectare,[58] CEPD și AEPD consideră că este necesară o analiză suplimentară pentru a evalua fiabilitatea instrumentelor existente. Această analiză ar trebui să se bazeze pe indicatori de performanță exhaustivi și să evalueze impactul potențialelor erori în condiții reale pentru toate persoanele vizate de Propunere.

66. După cum s-a menționat mai sus, CEPD și AEPD au îndoieli serioase cu privire la măsura în care garanțiile procedurale prevăzute la articolul 7 alineatul (6) din Propunere sunt suficiente pentru a compensa aceste riscuri. În plus, după cum s-a menționat anterior, acestea observă că Propunerea

[56] Raportul de Evaluare a Impactului, anexa 8, p. 281.
[57] Raportul de Evaluare a Impactului, anexa 8, p. 281-283.
[58] Raportul de Evaluare a Impactului, p. 279 și urm.

utilizează termeni destul de abstracți și vagi pentru a descrie valoarea acceptabilă a riscului (de exemplu, „măsură apreciabilă”).

67. CEPD și AEPD sunt îngrijorate de faptul că aceste noțiuni largi și vagi vor duce la o lipsă de securitate juridică și vor provoca, de asemenea, divergențe puternice în punerea în aplicare concretă a Propunerii în întreaga Uniune, în funcție de interpretările care vor fi date unor noțiuni precum „probabilitate” și „măsură apreciabilă” de către autoritățile judiciare sau alte autorități administrative independente din statele membre. Acest lucru este îngrijorător și având în vedere că dispozițiile privind ordinele de detectare vor constitui „restrângeri” ale principiului confidențialității prevăzut la articolul 5 din Directiva asupra confidențialității și comunicațiilor electronice. Prin urmare, claritatea și previzibilitatea acestora trebuie îmbunătățite în propunerea de Regulament.

4.5.6 Detectarea cazurilor de ademenire a copiilor („grooming”)

68. CEPD și AEPD observă că măsurile propuse privind detectarea ademenirii copiilor („grooming”), care implică analiza automată a discursului sau a textului, ar putea constitui cea mai semnificativă interferență cu drepturile utilizatorilor la viața privată și de familie, inclusiv la confidențialitatea comunicațiilor, și la protecția datelor cu caracter personal.

69. Deși detectarea MASC cunoscute și chiar noi poate fi limitată la analiza imaginilor și a videoclipurilor, detectarea fenomenului de „grooming” s-ar extinde, prin definiție, la toate comunicările de tip text (și, eventual, audio) care intră în sfera de aplicare a unui ordin de detectare. Prin urmare, intensitatea interferenței cu confidențialitatea comunicațiilor în cauză este mult mai mare.

70. CEPD și AEPD consideră că analiza automată generală și nediscriminatorie *de facto* a comunicațiilor bazate pe text transmise prin intermediul serviciilor de comunicații interpersonale, în vederea identificării unei potențiale ademeniri a copiilor, nu respectă cerințele de necesitate și proporționalitate. Chiar dacă tehnologia utilizată se limitează la utilizarea indicatorilor, CEPD și AEPD consideră că desfășurarea unei astfel de analize generale și nediscriminatorii este excesivă și poate afecta chiar esența dreptului fundamental la viață privată consacrat la articolul 7 din Cartă.

71. După cum s-a afirmat deja, lipsa garanțiilor de fond în contextul măsurilor de detectare a cazurilor de ademenire a copiilor nu poate fi compensată doar prin garanții procedurale. În plus, problema clarității și securității juridice insuficiente (de exemplu, utilizarea unui limbaj juridic vag, cum ar fi „măsură apreciabilă”) este și mai gravă în cazul analizei automate a comunicațiilor personale bazate pe text, față de compararea fotografiilor bazată pe tehnologia cu valori de dispersie.

72. În plus, CEPD și AEPD consideră că „efectul de intimidare” asupra libertății de exprimare este deosebit de semnificativ atunci când comunicările text (sau audio) ale persoanelor sunt scanate și analizate pe scară largă. CEPD și AEPD reamintesc că acest efect de intimidare este cu atât mai grav cu cât legea este mai puțin clară.

73. În plus, după cum se indică în Raportul de Evaluare a Impactului[59] și în studiul Serviciului de Cercetare al Parlamentului European[60], rata de precizie a tehnologiilor de detectare a cazurilor de „grooming” bazate pe text este mult mai mică decât rata de precizie a tehnologiilor de detectare a MASC cunoscute[61]. Tehnicile de detectare a cazurilor de „grooming” sunt concepute pentru a analiza și a

[59] Raportul de Evaluare a Impactului, anexa 8, p. 281-283.
[60] p. 15-18.
[61] A se vedea punctul 40 de mai sus.

atribui grade de probabilitate fiecărui aspect al conversației, prin urmare, CEPD și AEPD le consideră, de asemenea, predispuse la erori și vulnerabile la abuzuri.

4.5.7 Concluzii privind necesitatea și proporționalitatea măsurilor preconizate

74. În ceea ce privește necesitatea și proporționalitatea măsurilor de detectare avute în vedere, CEPD și AEPD sunt deosebit de îngrijorate în legătură cu măsurile luate în considerare pentru detectarea MASC necunoscute și a cazurilor de ademenire a copiilor („grooming"), întrucât acestea au un caracter intruziv din cauza posibilității de a acorda acces la conținutul comunicațiilor în mod generalizat, a naturii lor probabilistice și a ratelor de eroare asociate cu astfel de tehnologii.

75. În plus, din jurisprudența CJUE se poate deduce că măsurile care permit autorităților publice să aibă acces în mod generalizat la conținutul unei comunicații sunt mai susceptibile de a afecta esența drepturilor garantate la articolele 7 și 8 din Cartă. Aceste considerații sunt relevante în special în ceea ce privește măsurile de detectare a cazurilor de ademenire a copiilor prevăzute în Propunere.

76. În orice caz, CEPD și AEPD consideră că interferența creată în special de măsurile de detectare a cazurilor de ademenire a copiilor depășește ceea ce este strict necesar și proporțional. Prin urmare, aceste măsuri ar trebui să fie eliminate din Propunere.

4.6 Obligații de raportare

77. CEPD și AEPD recomandă completarea listei de cerințe specifice de raportare de la articolul 13 din Propunere cu o cerință de a include în raport informații privind tehnologia specifică care a permis furnizorului să ia cunoștință de conținutul abuziv relevant, în cazul în care furnizorul a luat cunoștință de potențialul abuz sexual asupra copiilor ca urmare a măsurilor luate pentru a executa un ordin de detectare emis în conformitate cu articolul 7 din Propunere.

4.7 Obligațiile de eliminare și blocare

78. Una dintre măsurile avute în vedere de Propunere pentru atenuarea riscurilor de diseminare a MASC este emiterea de ordine de eliminare și de blocare, care ar obliga furnizorii să elimine sau să dezactiveze accesul la materiale online care conțin abuzuri sexuale asupra copiilor sau să blocheze aceste materiale.[62]

79. Deși impactul ordinelor de eliminare asupra protecției datelor și a confidențialității comunicațiilor este relativ limitat, ca observație generală, CEPD și AEPD reamintesc principiul general care trebuie respectat, și anume că orice astfel de măsură ar trebui să fie cât mai bine direcționată posibil.

80. În același timp, CEPD și AEPD atrag atenția că furnizorii de servicii de acces la internet au acces la URL-ul exact al conținutului doar dacă acest conținut este disponibil în text clar. De fiecare dată când conținutul este accesibil prin HTTPS, furnizorul de servicii de acces la internet nu va avea acces la URL-ul exact, cu excepția cazului în care decriptează comunicația. Prin urmare, CEPD și AEPD au îndoieli cu privire la eficiența măsurilor de blocare și consideră că solicitarea adresată furnizorilor de servicii de acces la internet de a decripta comunicațiile online pentru a le bloca pe cele referitoare la MASC ar fi disproporționată.

[62] Propunere, articolele 14 și 16.

81. În plus și în general, ar trebui remarcat că blocarea (sau dezactivarea) accesului la un element digital este o operațiune care are loc la nivelul rețelei, iar punerea sa în aplicare se poate dovedi ineficientă în cazul unor copii multiple (eventual similare, și nu identice) ale aceluiași element. Mai mult, o astfel de operațiune se poate dovedi disproporționată, în cazul în care blocarea afectează și alte elemente digitale, care nu sunt ilegale, atunci când acestea sunt stocate pe același server făcut inaccesibil cu ajutorul comenzilor de rețea (de exemplu, includerea în lista neagră a adreselor IP sau a DNS-urilor). În plus, nu toate abordările privind blocarea la nivel de rețea sunt la fel de eficiente, iar unele pot fi ușor de eludat, având competențe tehnice destul de elementare.

82. În cele din urmă, competențele Autorităților de Coordonare în ceea ce privește emiterea ordinelor de blocare ar trebui să fie clarificate în propunerea de Regulament. De exemplu, din formularea actuală a articolului 16 alineatul (1) și a articolului 17 alineatul (1), nu este clar dacă Autoritățile de Coordonare sunt împuternicite să emită sau doar să solicite emiterea ordinelor de blocare.[63]

4.8 Tehnologii și măsuri de protecție relevante

4.8.1 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

83. Cerințele propunerii care se aplică tehnologiilor care urmează să fie implementate pentru detectarea MASC și a cazurilor de ademenire a copiilor nu par a fi suficient de stricte. În special, CEPD și AEPD au remarcat că – spre deosebire de dispozițiile similare din Regulamentul Provizoriu[64] – propunerea nu face nicio referire expresă la principiul protecției datelor începând cu momentul conceperii și în mod implicit și nu prevede că tehnologiile care sunt utilizate pentru a scana textul din comunicații nu trebuie să fie în măsură să deducă substanța conținutului comunicațiilor. Propunerea prevede pur și simplu, la articolul 10 alineatul (3) litera (b), că tehnologiile nu trebuie să fie în măsură să „extragă" alte informații din comunicațiile relevante decât cele strict necesare pentru detectare. Cu toate acestea, acest standard nu pare a fi suficient de strict, deoarece ar putea fi posibil să se *deducă* alte informații din substanța conținutului unei comunicații fără a *extrage* informații din aceasta ca atare.

84. În consecință, CEPD și AEPD recomandă introducerea în Propunere a unui Considerent care să stipuleze că principiul protecției datelor începând cu momentul conceperii și în mod implicit prevăzut la articolul 25 din Regulamentul (UE) 2016/679 se aplică tehnologiilor reglementate de articolul 10 din Propunere în temeiul legii și, prin urmare, nu trebuia repetat în textul juridic. În plus, articolul 10 alineatul (3) litera (b) ar trebui modificat pentru a se asigura că nu sunt extrase alte informații și că nici nu sunt deduse, așa cum prevede în prezent articolul 3 alineatul (1) litera (b) din Regulamentul Provizoriu.

[63] Articolul 16 alineatul (1) din Propunere prevede: „Autoritatea de Coordonare din statul membru de stabilire are competența de a solicita autorității judiciare competente a statului membru care a desemnat-o sau unei autorități administrative independente a respectivului stat membru să emită un ordin de blocare […]", în timp ce articolul 17 alineatul (1) prevede: „Autoritatea de coordonare din statul membru de stabilire emite ordinele de blocare menționate la articolul 16 […]" (sublinierea noastră).
[64] Regulamentul Provizoriu, articolul 3 alineatul (1) litera (b).

4.8.2 Fiabilitatea tehnologiilor

85. Propunerea presupune că furnizorii de servicii pot utiliza mai multe tipuri de soluții tehnologice pentru a executa ordinele de detectare. În special, Propunerea presupune că sistemele de inteligență artificială sunt disponibile și funcționale pentru detectarea MASC necunoscute și pentru detectarea cazurilor de ademenire a copiilor[65] și ar putea fi considerate ca fiind de ultimă generație de către unele Autorități de Coordonare. În timp ce eficacitatea Propunerii depinde de fiabilitatea acestor soluții tehnologice, sunt disponibile foarte puține informații cu privire la utilizarea generalizată și sistematică a acestor tehnici, ceea ce necesită o analiză atentă.

86. În plus, chiar dacă CEPD și AEPD au fost nevoite să le utilizeze în evaluarea proporționalității, din cauza lipsei de alternative, trebuie remarcat faptul că indicatorii de performanță ai tehnologiilor de detectare menționați în Raportul de Evaluare a Impactului care a însoțit Propunerea oferă foarte puține informații despre modul în care au fost evaluați și dacă reflectă performanța în lumea reală a tehnologiilor relevante. Nu există informații despre testele sau criteriile de referință utilizate de furnizorii de tehnologii pentru a măsura aceste performanțe. În lipsa unor astfel de informații, nu este posibil să se reproducă testele sau să se evalueze valabilitatea declarațiilor de performanță. În această privință, ar trebui remarcat că, deși indicatorii de performanță ar putea fi interpretați ca sugerând că unele instrumente de detectare au un nivel ridicat de acuratețe (de exemplu, acuratețea anumitor instrumente de detectare a ademenirii copiilor este de 88 %),[66] acești indicatori ar trebui analizați în lumina utilizării practice preconizate a instrumentelor de detectare și a gravității riscurilor pe care o evaluare incorectă a unui anumit material le-ar implica pentru persoanele vizate relevante. În plus, CEPD și AEPD consideră că, în cazul unei prelucrări cu un risc atât de ridicat, rata de eșec de 12 % prezintă un risc ridicat pentru persoanele vizate care au fost supuse unor rezultate fals pozitive, chiar și atunci când există garanții pentru a preveni raportările false către autoritățile de aplicare a legii. Este foarte puțin probabil ca furnizorii de servicii să poată angaja suficiente resurse pentru a examina un astfel de procent de rezultate fals pozitive.

87. După cum s-a menționat anterior,[67] indicatorii de performanță ar trebui să ofere o perspectivă exhaustivă asupra comportamentului instrumentelor de detectare. Atunci când se utilizează algoritmi de inteligență artificială pe imagini sau texte, este bine documentat faptul că pot apărea prejudecăți și discriminări din cauza lipsei de reprezentativitate a anumitor grupuri de populație în datele utilizate pentru antrenarea algoritmului. Aceste prejudecăți ar trebui identificate, măsurate și reduse la un nivel acceptabil pentru ca sistemele de detectare să fie cu adevărat benefice pentru întreaga societate.

88. Deși a fost realizat un studiu al tehnologiilor utilizate pentru detectare[68], CEPD și AEPD consideră că este necesară o analiză suplimentară pentru a evalua în mod independent fiabilitatea instrumentelor existente în cazuri de utilizare în lumea reală. Această analiză ar trebui să se bazeze pe indicatori de performanță exhaustivi și să evalueze impactul potențialelor erori în condiții reale pentru toate persoanele vizate de propunere. Având în vedere că aceste tehnologii reprezintă temeiul pe care se bazează propunerea, CEPD și AEPD consideră că această analiză este de o importanță capitală pentru evaluarea caracterului adecvat al propunerii.

89. De asemenea, CEPD și AEPD remarcă faptul că Propunerea nu definește cerințe specifice tehnologiei, fie în ceea ce privește ratele de eroare, fie în ceea ce privește utilizarea clasificatorilor și validarea

[65] A se vedea Raportul de Evaluare a Impactului, p. 281 și 282.
[66] Ibid., p. 283.
[67] A se vedea punctele 63 și 64 de mai sus.
[68] A se vedea Raportul de Evaluare a Impactului, p. 279 și urm.

acestora sau în ceea ce privește alte restricții. Rămâne să se elaboreze astfel de criterii în practică atunci când se evaluează proporționalitatea utilizării unei tehnologii specifice, ceea ce contribuie și mai mult la lipsa de precizie și de claritate.

90. Având în vedere importanța consecințelor pentru persoanele vizate în cazurile de rezultate fals pozitive, CEPD și AEPD consideră că ratele rezultatelor fals pozitive trebuie reduse la minimum și că aceste sisteme trebuie concepute ținând cont de faptul că marea majoritate a comunicațiilor electronice nu includ nici MASC, nici cazuri de ademenire a copiilor și că, de asemenea, chiar și o rată de rezultate fals pozitive foarte scăzută va implica un număr foarte mare de rezultate fals pozitive, având în vedere volumul de date care vor fi supuse detectării. În mod mai general, CEPD și AEPD sunt, de asemenea, preocupate de faptul că performanța instrumentelor disponibile indicate în Raportul de Evaluare a Impactului nu reflectă indicatori preciși și comparabili în ceea ce privește ratele rezultatelor fals pozitive și fals negative și consideră că ar trebui să se emită indicatori de performanță comparabili și semnificativi pentru aceste tehnologii înainte de a le considera disponibile și eficiente.

4.8.3 Scanarea comunicațiilor audio

91. Spre deosebire de Regulamentul Provizoriu,[69] Propunerea nu exclude din domeniul său de aplicare scanarea comunicațiilor audio în contextul detectării cazurilor de „grooming”.[70] CEPD și AEPD consideră că scanarea comunicațiilor audio este deosebit de intruzivă, deoarece ar necesita în mod normal o interceptare activă, continuă și „în direct”. În plus, în unele state membre, confidențialitatea cuvintelor vorbite se bucură de o protecție specială.[71] În plus, din cauza faptului că, în principiu, ar trebui analizat întregul conținut al comunicațiilor audio, această măsură ar putea să afecteze esența drepturilor garantate la articolele 7 și 8 din Cartă. Prin urmare, această metodă de detectare ar trebui să rămână în afara domeniului de aplicare al obligațiilor de detectare prevăzute în propunerea de Regulament, atât în ceea ce privește mesajele vocale, cât și comunicațiile în direct, cu atât mai mult cu cât Raportul de Evaluare a Impactului care a însoțit Propunerea nu a identificat riscuri specifice sau schimbări în peisajul amenințărilor care să justifice utilizarea acesteia.[72]

4.8.4 Verificarea vârstei

92. Propunerea încurajează furnizorii să utilizeze măsuri de verificare și de evaluare a vârstei pentru a identifica utilizatorii minori în cadrul serviciilor lor.[73] În acest sens, CEPD și AEPD constată că, în prezent, nu există nicio soluție tehnologică în măsură să evalueze cu certitudine vârsta unui utilizator într-un context online, fără a se baza pe o identitate digitală oficială, care nu este disponibilă pentru fiecare cetățean european în acest moment.[74] Prin urmare, utilizarea măsurilor de verificare a vârstei prevăzută în Propunere ar putea duce la excluderea, de exemplu, a adulților care par foarte tineri de la accesarea serviciilor online sau la implementarea unor instrumente de verificare a vârstei foarte intruzive, care ar putea inhiba sau descuraja utilizarea legitimă a serviciilor afectate.

93. În această privință și chiar dacă Considerentul 16 din Propunere se referă la instrumentele de control parental ca posibile măsuri de atenuare, CEPD și AEPD recomandă ca propunerea de Regulament să

[69] A se vedea Regulamentul Provizoriu, articolul 1 alineatul (2).
[70] A se vedea Propunerea, articolul 1.
[71] A se vedea, de exemplu, Codul penal german, articolul 201.
[72] A se vedea Raportul de Evaluare a Impactului.
[73] A se vedea Propunerea, articolul 4 alineatul (3), articolul 6 alineatul (1) litera (c) și considerentul 16.
[74] A se vedea, de exemplu, CNIL, Recomandarea 7: Verificarea vârstei copilului și a consimțământului părinților, respectând în același timp viața privată a copilului (9 august 2021).

fie modificată pentru a permite în mod expres furnizorilor să se bazeze pe mecanismele de control parental pe lângă verificarea vârstei sau ca alternativă la aceasta.

4.9 Păstrarea informațiilor

94. Articolul 22 din Propunere limitează scopurile în care furnizorii care fac obiectul Propunerii pot păstra datele privind conținutul și alte date prelucrate în legătură cu măsurile luate pentru a se conforma obligațiilor prevăzute în Propunere. Cu toate acestea, Propunerea indică faptul că furnizorii pot, de asemenea, să păstreze aceste informații în scopul îmbunătățirii eficacității și acurateței tehnologiilor de detectare a abuzurilor sexuale online asupra copiilor în vederea executării unui ordin de detectare, dar nu trebuie să stocheze date cu caracter personal în acest scop.[75]

95. CEPD și AEPD consideră că numai acei furnizori care utilizează propriile tehnologii de detectare ar trebui să aibă dreptul de a păstra datele pentru a îmbunătăți eficacitatea și acuratețea tehnologiilor, în timp ce aceia care utilizează tehnologii furnizate de Centrul UE nu ar trebui să beneficieze de această posibilitate. În plus, CEPD și AEPD observă că ar putea fi dificil să se asigure în practică că nu se stochează date cu caracter personal în acest scop, deoarece majoritatea datelor referitoare la conținut și a altor date prelucrate în scopuri de detectare sunt susceptibile de a fi considerate date cu caracter personal.

4.10 Impactul asupra criptării

96. Autoritățile europene pentru protecția datelor au pledat în mod constant pentru disponibilitatea pe scară largă a unor instrumente de criptare puternice și împotriva oricărui tip de backdoor.[76] Motivul pentru aceasta este importanța criptării pentru a asigura exercitarea tuturor drepturilor omului atât offline, cât și online.[77] În plus, tehnologiile de criptare contribuie în mod fundamental atât la respectarea vieții private, cât și a confidențialității comunicațiilor, precum și la inovare și la creșterea economiei digitale, care se bazează pe nivelul ridicat de încredere pe care îl oferă aceste tehnologii.

97. În contextul comunicațiilor interpersonale, criptarea de la un capăt la altul (end-to-end – E2EE) este un instrument esențial pentru asigurarea confidențialității comunicațiilor electronice, deoarece oferă garanții tehnice puternice împotriva accesării conținutului comunicațiilor de către oricine altcineva în afară de expeditor și destinatar (destinatari), inclusiv de către furnizor. Împiedicând sau descurajând în orice fel utilizarea E2EE, impunând furnizorilor de servicii obligația de a prelucra datele de comunicații electronice în alte scopuri decât furnizarea serviciilor lor sau impunându-le obligația de a transmite în mod proactiv comunicațiile electronice către terți ar implica riscul ca furnizorii să ofere servicii mai slab criptate pentru a se conforma mai bine obligațiilor, slăbind astfel rolul criptării în general și subminând respectarea drepturilor fundamentale ale cetățenilor europeni. Trebuie remarcat că, deși E2EE este una dintre cel mai frecvent utilizate măsuri de securitate în contextul comunicațiilor electronice, alte soluții tehnice (de exemplu, utilizarea altor sisteme criptografice) pot fi sau pot deveni la fel de importante pentru a securiza și a proteja confidențialitatea comunicațiilor digitale. Astfel, utilizarea acestora nu ar trebui împiedicată sau descurajată.

---

[75] Propunerea, articolul 22 alineatul (1).
[76] A se vedea, de exemplu, Grupul de lucru instituit prin articolul 29, Declarația Grupului de lucru instituit prin articolul 29 privind criptarea și impactul său asupra protecției persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal în UE (11 aprilie 2018).
[77] A se vedea Rezoluția 47/16 a Consiliului pentru Drepturile Omului privind promovarea, protecția și exercitarea drepturilor omului pe internet, documentul ONU A/HRC/RES/47/16 (26 iulie 2021).

98. Implementarea de instrumente de interceptare și analiză a comunicațiilor electronice interpersonale este în mod fundamental în contradicție cu E2EE, deoarece aceasta din urmă are ca scop garantarea din punct de vedere tehnic a confidențialității unei comunicații între expeditor și destinatar.

99. Prin urmare, chiar dacă Propunerea nu stabilește o obligație de interceptare sistematică pentru furnizori, simpla posibilitate ca un ordin de detectare să fie emis ar putea să influențeze puternic opțiunile tehnice ale furnizorilor, mai ales având în vedere termenul limitat pe care îl vor avea la dispoziție pentru a se conforma unui astfel de ordin și sancțiunile grele pe care le-ar suporta în caz de nerespectare a acestuia.[78] În practică, acest lucru ar putea determina anumiți furnizori să nu mai utilizeze E2EE.

100. Impactul degradării sau al descurajării utilizării E2EE, care ar putea rezulta din Propunere, trebuie evaluat în mod corespunzător. Fiecare dintre tehnicile de eludare a caracterului de protecție a vieții private al E2EE prezentate în Raportul de Evaluare a Impactului care a însoțit propunerea ar introduce lacune de securitate.[79] De exemplu, scanarea la nivelul clientului[80] ar duce probabil la accesarea și prelucrarea substanțială și fără o țintă precisă a conținutului necriptat pe dispozitivele utilizatorilor finali. O astfel de degradare substanțială a confidențialității ar afecta în special copiii, deoarece serviciile pe care le utilizează sunt mai susceptibile de a fi vizate de ordine de detectare, ceea ce îi face vulnerabili la monitorizare sau ascultare. În același timp, scanarea la nivelul serverului este, de asemenea, fundamental incompatibilă cu paradigma E2EE, deoarece ar trebui să se decripteze canalul de comunicații, criptat peer-to-peer, ceea ce ar duce la prelucrarea în masă a datelor cu caracter personal pe serverele furnizorilor.

101. În timp ce Propunerea afirmă că „lasă la latitudinea furnizorului în cauză alegerea tehnologiilor care urmează să fie utilizate pentru a respecta în mod eficace ordinele de detectare și nu ar trebui să fie înțeles ca stimulând sau descurajând utilizarea unei anumite tehnologii”, [81] incompatibilitatea structurală a unor ordine de detectare cu E2EE devine, de fapt, un puternic factor de descurajare a utilizării E2EE. Imposibilitatea de a accesa și de a utiliza serviciile care utilizează E2EE (care reprezintă stadiul actual al tehnologiei în ceea ce privește garanția tehnică a confidențialității) ar putea avea un efect de intimidare asupra libertății de exprimare și asupra utilizării private legitime a serviciilor de comunicații electronice. Relația nefavorabilă dintre detectarea MASC sau a cazurilor de „grooming” și E2EE este, de asemenea, recunoscută de Comisie atunci când constată, în Raportul de Evaluare a Impactului[82], probabilitatea ca implementarea E2EE de către Facebook în 2023 să pună capăt scanării voluntare a Facebook.

102. Pentru a asigura că propunerea de Regulament nu subminează securitatea sau confidențialitatea comunicațiilor electronice ale cetățenilor europeni, CEPD și AEPD consideră că partea dispozitivă a Propunerii ar trebui să precizeze în mod clar că nicio dispoziție din propunerea de Regulament nu ar

[78] A se vedea Propunerea, articolul 35.

[79] A se vedea secțiunea 4.2 din Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague și Carmela Troncoso, „The Risks of Client-Side Scanning”, ArXiv abs/2110.07450 (2021).

[80] Scanarea la nivelul clientului se referă, în general, la sistemele care scanează conținutul mesajelor pentru a căuta corespondențe cu o bază de date de conținut inacceptabil înainte ca mesajul să fie trimis destinatarului.

[81] Propunere, considerentul 26.

[82] Raportul de Evaluare a Impactului, p. 27.

trebui interpretată în sensul că interzice sau slăbește criptarea, în conformitate cu ceea ce se precizează în Considerentul 25 din Regulamentul Provizoriu.

4.11 Supraveghere, aplicare și cooperare

4.11.1 Rolul autorităților naționale de supraveghere în temeiul RGPD

103. Propunerea prevede înființarea unei rețele de Autorități naționale de Coordonare, care vor răspunde de aplicarea și executarea propunerii de Regulament.[83] În timp ce considerentul 54 din Propunere prevede că „[n]ormele prezentului Regulament privind supravegherea și asigurarea respectării dispozițiilor nu ar trebui înțelese ca afectând prerogativele și competențele autorităților pentru protecția datelor în temeiul Regulamentului (UE) 2016/679", CEPD și AEPD sunt de părere că relația dintre sarcinile Autorităților de Coordonare și cele ale autorităților pentru protecția datelor ar trebui să fie mai bine reglementată și că autorităților pentru protecția datelor ar trebui să li se acorde un rol mai important în cadrul propunerii de Regulament.

104. În special, furnizorii ar trebui să fie obligați să consulte autoritățile pentru protecția datelor prin intermediul unei proceduri de consultare prealabilă, astfel cum se menționează la articolul 36 din RGPD, înainte de a pune în aplicare orice măsură de detectare a MASC sau a cazurilor de „grooming", și nu exclusiv în legătură cu utilizarea măsurilor de detectare a cazurilor de ademenire a copiilor, așa cum se prevede în prezent în Propunere.[84] Toate măsurile de detectare ar trebui să fie considerate ca având ca rezultat implicit un „risc ridicat" și, prin urmare, ar trebui supuse unei proceduri de consultare prealabilă, indiferent dacă se referă la „grooming" sau MASC, așa cum se întâmplă deja în temeiul Regulamentului Provizoriu.[85] În plus, autoritățile competente pentru protecția datelor desemnate în temeiul RGPD ar trebui să fie întotdeauna împuternicite să își exprime punctul de vedere cu privire la măsurile de detectare avute în vedere, și nu doar în circumstanțe specifice.[86]

105. În plus, propunerea de Regulament ar trebui să stabilească un sistem de abordare și de soluționare a dezacordurilor dintre autoritățile competente și autoritățile pentru protecția datelor în ceea ce privește ordinele de detectare. În special, autorităților pentru protecția datelor ar trebui să li se acorde dreptul de a contesta un ordin de detectare în fața instanțelor din statul membru al autorității judiciare competente sau al autorității administrative independente care a emis ordinul de detectare. În această privință, CEPD și AEPD iau act de faptul că, în conformitate cu versiunea actuală a Propunerii, avizul autorităților competente în materie de protecție a datelor poate fi respins de autoritatea competentă atunci când emite un ordin de detectare. Acest lucru ar putea duce la decizii contradictorii, întrucât autoritățile pentru protecția datelor, așa cum se confirmă la articolul 36 alineatul (2) din RGPD, și-ar păstra toate competențele corective în temeiul articolului 58 din RGPD, inclusiv competența de a dispune interzicerea prelucrării.

4.11.2 Rolul CEPD

106. CEPD și AEPD observă că Propunerea prevede la articolul 50 alineatul (1) a treia teză că „Centrul UE solicită avizele Comitetului pentru tehnologie și Comitetului European pentru Protecția Datelor" înainte de a adăuga o tehnologie specifică pe listele de tehnologii a căror utilizare furnizorii de servicii de găzduire și furnizorii de servicii de comunicații interpersonale o pot lua în considerare pentru

[83] Propunere, articolul 25.
[84] Propunere, articolul 7 alineatul (3) al doilea paragraf litera (b).
[85] Regulamentul provizoriu, articolul 3 alineatul (1) litera (c).
[86] A se vedea Propunerea, articolul 7 alineatul (3) al doilea paragraf litera (c).

executarea ordinelor de detectare. De asemenea, aceasta prevede că CEPD emite avizele sale într-un termen de opt săptămâni, care poate fi prelungit cu încă șase săptămâni, dacă este necesar, ținând seama de complexitatea chestiunii. În cele din urmă, aceasta impune CEPD să informeze Centrul UE cu privire la o astfel de prelungire în termen de o lună de la primirea cererii de consultare, prezentând motivele întârzierii.

107. Sarcinile existente ale CEPD sunt stabilite la articolul 70 din RGPD și la articolul 51 din Directiva (UE) 2016/680 (denumită în continuare „Directiva privind protecția datelor în materie de asigurare a respectării legii")[87]. În cadrul acestor sarcini, se prevede că CEPD oferă consultanță Comisiei și emite avize la cererea Comisiei, a unei autorități naționale de supraveghere sau a Președintelui acesteia. Deși articolul 1 alineatul (3) litera (d) din Propunere prevede că normele stabilite în RGPD și în Directiva privind protecția datelor în materie de asigurare a respectării legii nu sunt afectate de Propunere, împuternicirea Centrului UE de a solicita avize din partea CEPD depășește sarcinile atribuite CEPD în temeiul RGPD și al Directivei privind protecția datelor în materie de asigurare a respectării legii. Astfel, ar trebui să se precizeze în propunerea de Regulament – cel puțin într-un Considerent – că Propunerea extinde sarcinile CEPD. În această privință, CEPD și AEPD apreciază rolul important pe care Propunerea îl atribuie CEPD, solicitând implicarea sa în punerea în aplicare practică a propunerii de Regulament. În practică, secretariatul CEPD joacă un rol esențial în furnizarea sprijinului analitic, administrativ și logistic necesar pentru adoptarea avizelor CEPD. Prin urmare, pentru a se asigura că CEPD și membrii săi își pot îndeplini sarcinile, este esențială alocarea unui buget și a unui personal suficient pentru CEPD. Din păcate, însă, fișa financiară legislativă a Propunerii nu indică faptul că vor fi puse la dispoziție resurse suplimentare pentru îndeplinirea sarcinilor suplimentare pe care Propunerea le atribuie CEPD.[88]

108. În plus, CEPD și AEPD constată că articolul 50 din Propunere nu indică modul în care Centrul UE va proceda după primirea unui aviz din partea CEPD.[89] Considerentul 27 din Propunere prevede doar că avizul emis de CEPD ar trebui luat în considerare de către Centrul UE și Comisia Europeană. Prin urmare, ar trebui să se clarifice care va fi scopul avizului solicitat în cadrul procesului prevăzut la articolul 50 din Propunere și cum va acționa Centrul UE după primirea unui aviz din partea CEPD.

109. În plus, CEPD și AEPD consideră că, deși orice orientare sau eventual aviz al CEPD privind utilizarea tehnologiilor de detectare va evalua utilizarea acestor tehnologii la nivel general, pentru o consultare prealabilă în temeiul articolului 36 din RGPD, autoritatea națională de supraveghere va trebui să țină seama de circumstanțele specifice și să efectueze o evaluare de la caz la caz a prelucrării planificate de către operatorul relevant. CEPD și AEPD remarcă faptul că autoritățile de supraveghere vor aplica și ar trebui să aplice criteriile prevăzute la articolul 36 din RGPD pentru a decide dacă este necesar să prelungească perioada stabilită în RGPD pentru a-și prezenta opiniile ca răspuns la o consultare prealabilă și nu este necesar să aplice standarde diferite atunci când o consultare prealabilă se referă la utilizarea unei tehnologii de detectare.[90]

---

[87] Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89-131).

[88] A se vedea Propunerea, p. 105 și urm.

[89] A se vedea, în schimb, articolul 51 alineatul (4) din Directiva privind protecția datelor în materie de asigurare a respectării legii.

[90] A se vedea Propunerea, considerentul 24.

110. În cele din urmă, în aplicarea articolului 11 („Orientări privind obligațiile de detectare”), Propunerea stipulează că Comisia poate emite orientări privind aplicarea articolelor 7-10 din propunere. Articolul 11 din Propunere ar trebui modificat pentru a clarifica faptul că, pe lângă autoritățile de coordonare și Centrul UE, Comisia ar trebui să consulte CEPD cu privire la proiectul de orientări, în afara procesului de consultare publică prevăzut, înainte de emiterea orientărilor privind obligațiile de detectare.

111. Prin urmare, această sarcină a CEPD, precum și rolul său în cadrul juridic care ar fi introdus prin Propunere, necesită o evaluare suplimentară din partea legiuitorului.

4.11.3 Rolul Centrului UE privind abuzul sexual asupra copiilor

112. Capitolul IV din Propunere prevede înființarea Centrului UE, în calitate de nouă agenție descentralizată care să permită punerea în aplicare a Propunerii. Printre alte sarcini, Centrul UE ar trebui să faciliteze accesul furnizorilor la tehnologii de detectare fiabile; să pună la dispoziție indicatori creați pe baza abuzurilor sexuale online asupra copiilor, verificați de instanțele judecătorești sau de autoritățile administrative independente din statele membre, în scopul detectării; să ofere asistență, la cerere, în legătură cu efectuarea evaluărilor de risc; și să ofere sprijin în comunicarea cu autoritățile naționale relevante.[91]

113. În această privință, CEPD și AEPD salută articolul 77 alineatul (1) din Propunere, care confirmă că prelucrarea datelor cu caracter personal de către Centrul UE face obiectul RPDUE și care prevede că măsurile de aplicare a Regulamentului respectiv de către Centrul UE, inclusiv cele referitoare la numirea unui Responsabil cu Protecția Datelor în cadrul Centrului UE, se stabilesc după consultarea AEPD. Cu toate acestea, CEPD și AEPD sunt de părere că mai multe dispoziții din acest capitol merită o examinare mai atentă.

114. În primul rând, CEPD și AEPD iau act de faptul că articolul 48 din Propunere prevede transmiterea tuturor rapoartelor care „nu sunt în mod vădit nefondate”[92] către autoritățile naționale de aplicare a legii și către Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii („Europol”). Acest prag pentru ca Centrul UE să transmită rapoartele (care „nu sunt în mod vădit nefondate”) către autoritățile naționale de aplicare a legii și Europol pare prea redus, mai ales dacă se ține seama de faptul că scopul înființării Centrului UE, astfel cum se prevede în Raportul de Evaluare a Impactului al Comisiei[93], este de a ușura sarcina autorităților de aplicare a legii și a Europol de a filtra conținutul semnalat în mod eronat ca fiind MASC. În această privință, nu este clar de ce Centrul UE, în calitate de centru de expertiză, nu ar putea efectua o evaluare juridică și factuală mai amănunțită pentru a limita riscurile ca datele unor persoane nevinovate să fie transmise autorităților de aplicare a legii.

115. În al doilea rând, dispoziția privind durata de stocare a datelor cu caracter personal de către Centrul UE pare relativ deschisă, având în vedere caracterul sensibil al datelor în cauză. Chiar dacă nu ar fi posibil să se stabilească o perioadă maximă de păstrare pentru stocarea acestor date, CEPD și AEPD recomandă ca în propunere să se stabilească cel puțin o limită maximă de timp pentru analizarea

[91] A se vedea COM(2022) 209 final, p. 7.
[92] Termenul „în mod vădit nefondate” este descris în considerentul 65 din propunere ca fiind „imediat evident, fără o analiză juridică sau factuală de fond, că activitățile raportate nu constituie un abuz sexual online asupra copiilor”.
[93] A se vedea, de exemplu, pagina 349 din Raportul de Evaluare a Impactului.

necesității de a continua stocarea datelor și să se solicite o justificare pentru păstrarea prelungită după această perioadă.

116. În plus, având în vedere gradul foarte ridicat de sensibilitate a datelor cu caracter personal care urmează să fie prelucrate de Centrul UE, CEPD și AEPD sunt de părere că prelucrarea ar trebui să facă obiectul unor garanții suplimentare, în special pentru a asigura o supraveghere eficientă. Aceasta ar putea include obligația Centrului UE de a păstra jurnale pentru operațiunile de prelucrare în cadrul sistemelor de prelucrare automată care privesc datele (și anume reflectând cerința privind datele operaționale cu caracter personal în temeiul capitolului IX din RPDUE), inclusiv înregistrarea introducerii, modificării, accesului, consultării, divulgării, combinării și ștergerii datelor cu caracter personal. Înregistrările consultărilor și ale dezvăluirilor fac posibilă determinarea motivelor, a datei și a orei efectuării acestor operațiuni, identificarea persoanei care a consultat sau a dezvăluit date operaționale cu caracter personal și, în măsura în care este posibil, identitatea destinatarilor. Aceste înregistrări vor fi utilizate pentru verificarea legalității prelucrării, pentru automonitorizare și pentru asigurarea integrității și securității și vor fi puse la dispoziția responsabilului cu protecția datelor din cadrul Centrului UE și a AEPD, la cerere.

117. În plus, Propunerea face referire la obligația furnizorilor de a informa utilizatorii cu privire la detectarea MASC prin intermediul ordinelor de detectare, precum și la dreptul de a depune o plângere la o autoritate de coordonare.[94] Cu toate acestea, Propunerea nu stabilește proceduri pentru exercitarea drepturilor persoanelor vizate, ținând seama, de asemenea, de multiplele locuri în care datele cu caracter personal pot fi transmise și stocate în temeiul Propunerii (Centrul UE, Europol, agențiile naționale de aplicare a legii). Cerința de a informa utilizatorii ar trebui să includă obligația de a informa persoanele fizice cu privire la faptul că datele lor au fost transmise și sunt prelucrate de diferite entități, dacă este cazul (de exemplu, de agențiile naționale de aplicare a legii și de Europol). În plus, ar trebui să existe o procedură centralizată pentru primirea și coordonarea cererilor privind dreptul de acces, rectificare și ștergere sau, alternativ, o obligație ca entitatea care primește o cerere din partea persoanei vizate să colaboreze cu celelalte entități în cauză.

118. CEPD și AEPD constată că, în temeiul articolului 50 din Propunere, Centrul UE are sarcina de a specifica lista tehnologiilor care pot fi utilizate pentru executarea ordinelor de detectare. Cu toate acestea, în conformitate cu articolul 12 alineatul (1) din Propunere, furnizorii sunt obligați să raporteze toate informațiile care indică un potențial abuz sexual online asupra copiilor în cadrul serviciilor lor, nu numai pe cele care provin din executarea unui ordin de detectare. Este foarte probabil ca un volum semnificativ de astfel de informații să provină din funcționarea măsurilor de atenuare ale furnizorilor, în conformitate cu articolul 4 din Propunere. Prin urmare, pare esențial să se determine care ar putea fi aceste măsuri, eficiența lor, rata de eroare în raportarea potențialelor abuzuri sexuale asupra copiilor și care este impactul lor asupra drepturilor și libertăților persoanelor fizice. În ciuda faptului că articolul 4 alineatul (5) din Propunere prevede că Comisia, în cooperare cu Autoritățile de Coordonare și cu Centrul UE și după ce a efectuat o consultare publică, poate emite orientări relevante, CEPD și AEPD consideră că este important ca legiuitorul să includă la articolul 50 o sarcină pentru Centrul UE de a furniza și o listă de măsuri de atenuare recomandate și de bune practici relevante care sunt deosebit de eficiente în identificarea potențialelor abuzuri sexuale online asupra copiilor. Întrucât astfel de măsuri pot interfera cu drepturile fundamentale la protecția datelor și a

[94] A se vedea articolul 10 alineatul (6) și, în urma prezentării unui raport către Centrul UE, articolul 12 alineatul (2) din Propunere.

vieții private, se recomandă, de asemenea, ca Centrul UE să solicite avizul CEPD înainte de a publica o astfel de listă.

119. În cele din urmă, cerințele de securitate prevăzute la articolul 51 alineatul (4) din Propunere ar trebui să fie mai specifice. În această privință, pot fi folosite ca surse de inspirație cerințele de securitate stabilite în alte Regulamente privind sistemele la scară largă care implică o prelucrare cu risc ridicat, cum ar fi Regulamentul (CE) nr. 767/2008 [95] (a se vedea articolul 32), Regulamentul (CE) nr. 1987/2006[96] (a se vedea articolul 16), Regulamentul (UE) 2018/1862[97] (a se vedea articolul 16) și Regulamentul (UE) nr. 603/2013[98] (a se vedea articolul 34).

4.11.4 Rolul Europol

120. Propunerea prevede o cooperare strânsă între Centrul UE și Europol. În temeiul capitolului IV din Propunere, la primirea rapoartelor de la furnizori privind suspiciunile de MASC, Centrul UE le verifică pentru a evalua care rapoarte pot conduce la o acțiune (care nu sunt în mod vădit nefondate) și le transmite Europol, precum și autorităților naționale de aplicare a legii. [99] Centrul UE acordă Europol acces la bazele sale de date cu indicatori și la bazele sale de date cu rapoarte pentru a sprijini investigațiile Europol privind suspiciunile de infracțiuni de abuz sexual asupra copiilor. [100] În plus, Centrului UE i se va acorda „cel mai larg acces posibil" la sistemele de informații ale Europol. [101] Cele două agenții vor împărți, de asemenea, sediile și anumite infrastructuri (non-operaționale). [102]

121. CEPD și AEPD constată că mai multe aspecte legate de cooperarea dintre Centrul UE propus și Europol suscită îngrijorare sau necesită precizări suplimentare.

Cu privire la transmiterea de rapoarte de către Centrul UE către Europol (articolul 48)

---

[95] Regulamentul (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere (Regulamentul VIS), JO L 218, 13.8.2008, p. 60-81.

[96] Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), (JO L 381, 28.12.2006, p. 4-23).

[97] Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56-106).

[98] Regulamentul (UE) nr. 603/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor și mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecție internațională prezentate într-unul dintre statele membre de către un resortisant al unei țări terțe sau de către un apatrid și privind cererile autorităților de aplicare a legii din statele membre și a Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii și de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenției europene pentru gestionarea operațională a sistemelor informatice la scară largă, în spațiul de libertate, securitate și justiție (reformare) (JO L 180, 29.6.2013, p. 1-30).

[99] A se vedea articolul 48 din Propunere.

[100] A se vedea articolul 46 alineatele (4) și (5) din Propunere.

[101] A se vedea articolul 53 alineatul (2) din Propunere.

[102] În special cele referitoare la gestionarea resurselor umane, tehnologia informației (IT), inclusiv securitatea cibernetică, clădirea și comunicațiile.

122. Articolul 48 din propunerea de Regulament prevede ca Centrul UE să transmită rapoartele care nu sunt considerate în mod vădit nefondate, împreună cu orice informații suplimentare relevante, către Europol și către autoritatea sau autoritățile competente de aplicare a legii din statul membru (statele membre) care ar putea avea competența de a investiga sau de a urmări penal potențialul abuz sexual asupra copiilor. Deși acest articol acordă Europol rolul de a identifica autoritatea relevantă de aplicare a legii în cazul în care statul membru în cauză nu este clar, dispoziția prevede, de fapt, că toate rapoartele sunt transmise către Europol, indiferent dacă autoritatea națională a fost identificată, iar raportul a fost deja transmis de către Centrul UE.

123. Cu toate acestea, Propunerea nu clarifică care ar fi valoarea adăugată a implicării Europol sau care ar fi rolul preconizat al acestuia la primirea rapoartelor, în special în cazurile în care autoritatea națională de aplicare a legii a fost identificată și notificată în paralel.[103]

124. CEPD și AEPD reamintesc că mandatul Europol se limitează la sprijinirea acțiunilor autorităților competente ale statelor membre și la cooperarea reciprocă a acestora în prevenirea și combaterea infracțiunilor grave care afectează două sau mai multe state membre.[104] Articolul 19 din Regulamentul (UE) 2016/794[105], astfel cum a fost modificat prin Regulamentul (UE) 2022/991[106] („Regulamentul modificat privind Europol"), prevede că un organism al Uniunii care furnizează informații către Europol este obligat să stabilească scopul sau scopurile în care acestea urmează să fie prelucrate de Europol, precum și condițiile de prelucrare. De asemenea, acesta este responsabil de asigurarea exactității datelor cu caracter personal transferate.[107]

125. Prin urmare, o transmitere generalizată a rapoartelor către Europol ar contraveni Regulamentului modificat privind Europol și ar implica o serie de riscuri legate de protecția datelor. Dublarea prelucrării datelor cu caracter personal ar putea duce la stocarea în paralel a mai multor copii ale acelorași date cu caracter personal extrem de sensibile (de exemplu, la Centrul UE, la Europol, la autoritatea națională de aplicare a legii), prezentând riscuri pentru acuratețea datelor, ca urmare a posibilei desincronizări a bazelor de date, precum și pentru exercitarea drepturilor persoanelor vizate. În plus, pragul scăzut stabilit în Propunere pentru schimbul de rapoarte cu autoritățile de aplicare a legii (cele care nu sunt „în mod vădit nefondate") implică o probabilitate ridicată ca rapoartele fals pozitive (și anume conținuturile semnalate în mod eronat ca fiind abuzuri sexuale asupra copiilor) să fie stocate în sistemele de informații ale Europol, potențial pentru perioade prelungite.[108]

---

[103] Considerentul 71 din Propunere face doar o referire generală la experiența Europol în identificarea autorităților naționale competente într-o situație neclară și la baza sa de date operative în materie penală care pot contribui la identificarea legăturilor cu investigații din alte state membre.

[104] A se vedea articolul 3 din Regulamentul modificat privind Europol.

[105] Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 24.5.2016, p. 53-114).

[106] Regulamentul (UE) 2022/991 al Parlamentului European și al Consiliului din 8 iunie 2022 de modificare a Regulamentului (UE) 2016/794 în ceea ce privește cooperarea Europol cu părțile private, prelucrarea datelor cu caracter personal de către Europol în sprijinul anchetelor penale și rolul Europol în materie de cercetare și inovare (JO L 169, 27.6.2022, p. 1-42).

[107] Articolul 38 alineatul (2) litera (a) din Regulamentul privind Europol.

[108] Conform raportului Comisiei privind evaluarea impactului, Europol a putut să examineze doar 20 % din cele 50 de milioane de imagini și clipuri video unice considerate MASC din baza sa de date, ceea ce implică o lipsă de resurse pentru a acționa asupra contribuțiilor referitoare la MASC pe care le primește în prezent. A se vedea Raportul de evaluare a impactului care însoțește Propunerea de regulament de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor, SWD(2022)209, p. 47 și 48.

126. Prin urmare, CEPD și AEPD recomandă ca Propunerea să specifice și să limiteze circumstanțele și scopurile în care Centrul UE ar putea transmite rapoarte către Europol, în conformitate cu Regulamentul modificat privind Europol. Acest lucru ar trebui să excludă în mod explicit acele circumstanțe în care rapoartele au fost transmise autorității de aplicare a legii relevante din statul membru, care nu implică nicio dimensiune transfrontalieră. În plus, Propunerea ar trebui să includă cerința ca Centrul UE să transfere către Europol numai date cu caracter personal care sunt adecvate, relevante și limitate la ceea ce este strict necesar. De asemenea, trebuie prevăzute garanții specifice pentru asigurarea calității și fiabilității datelor.

Articolul 53 alineatul (2) privind cooperarea dintre Centrul UE și Europol

127. Articolul 53 alineatul (2) din Propunere prevede că Europol și Centrul UE își acordă reciproc „cel mai larg acces posibil la informațiile și sistemele informatice relevante, în cazul în care acest lucru este necesar pentru îndeplinirea sarcinilor care le revin și în conformitate cu actele dreptului Uniunii care reglementează acest acces".

128. Articolul 46 alineatele (4) și (5) din Propunere precizează, de asemenea, că Europol are acces la baza de date a Centrului UE privind indicatorii și la baza de date a rapoartelor, iar articolul 46 alineatul (6) stabilește procedura de acordare a acestui acces: Europol depune o cerere, precizând scopul și gradul de acces necesar pentru îndeplinirea scopului respectiv, care este evaluată în mod corespunzător de către Centrul UE.

129. Criteriile și garanțiile care condiționează accesul Europol și utilizarea ulterioară a datelor obținute din sistemele informatice ale Centrului UE nu sunt specificate. În plus, nu se explică de ce este necesar să se acorde Europol acces direct la sistemele de informații ale unei agenții care nu se ocupă cu aplicarea legii, conținând date cu caracter personal extrem de sensibile, a căror legătură cu activitatea infracțională și cu prevenirea infracțiunilor poate să nu fi fost stabilită. Pentru a asigura un nivel ridicat de protecție a datelor și respectarea principiului colectării datelor cu caracter personal numai în scopurile prevăzute, CEPD și AEPD recomandă ca transmiterea de date cu caracter personal de la Centrul UE către Europol să aibă loc numai de la caz la caz, în urma unei cereri evaluate în mod corespunzător, prin intermediul unui instrument de comunicare securizat pentru schimburi, cum ar fi SIENA.[109]

130. Articolul 53 alineatul (2) reprezintă singura referire din Propunere la accesul Centrului UE la sistemele de informații ale Europol. Prin urmare, nu este clar în ce scopuri și conform căror garanții specifice ar avea loc un astfel de acces.

131. CEPD și AEPD reamintesc că Europol este o agenție de aplicare a legii, înființată în temeiul Tratatelor UE, cu un mandat principal de prevenire și combatere a infracțiunilor grave. Datele operaționale cu caracter personal prelucrate de Europol fac, prin urmare, obiectul unor norme și garanții stricte privind prelucrarea datelor. Centrul UE propus nu este un organism de aplicare a legii și în niciun caz nu ar trebui să i se acorde acces direct la sistemele de informații ale Europol.

132. De asemenea, CEPD și AEPD iau act de faptul că o mare parte din informațiile de interes comun pentru Centrul UE și Europol se vor referi la datele cu caracter personal referitoare la victimele unor presupuse infracțiuni, la datele cu caracter personal ale minorilor și la datele cu caracter personal privind viața sexuală, care se califică drept categorii speciale de date cu caracter personal în temeiul

[109] Secure Information Exchange Network Application (aplicație de rețea pentru schimbul securizat de informații – SIENA).

Regulamentului modificat privind Europol. Regulamentul modificat privind Europol impune condiții stricte în ceea ce privește accesul la categoriile speciale de date cu caracter personal. Articolul 30 alineatul (3) din Regulamentul modificat privind Europol prevede că numai Europol are acces direct la aceste date cu caracter personal, mai precis numai un număr limitat de funcționari Europol autorizați în mod corespunzător de către directorul executiv.[110]

133. Prin urmare, CEPD și AEPD recomandă să se clarifice formularea articolului 53 alineatul (2) din Propunere pentru a reflecta în mod corespunzător restricțiile în vigoare în temeiul Regulamentului modificat privind Europol și pentru a preciza modalitățile de acces al Centrului UE. În special, orice acces la datele cu caracter personal prelucrate în sistemele de informații ale Europol, în cazul în care este considerat strict necesar pentru îndeplinirea sarcinilor Centrului UE, ar trebui să fie acordat numai de la caz la caz, la prezentarea unei cereri explicite, care să documenteze scopul specific, și a unei justificări. Europol ar trebui să fie obligat să evalueze riguros aceste cereri și să transmită date cu caracter personal către Centrul UE numai în cazul în care acest lucru este strict necesar și proporțional cu scopul solicitat.

Articolul 10 alineatul (6) privind rolul Europol în informarea utilizatorilor în urma punerii în aplicare a unui ordin de detectare

134. CEPD și AEPD salută cerința, prevăzută la articolul 10 alineatul (6) din Propunere, ca furnizorii să informeze utilizatorii ale căror date cu caracter personal pot fi vizate de executarea unui ordin de detectare. Aceste informații urmează să fie furnizate utilizatorilor numai după obținerea confirmării din partea Europol sau a autorității naționale de aplicare a legii dintr-un stat membru care a primit raportul în conformitate cu articolul 48 din Propunere că furnizarea de informații utilizatorilor nu ar interfera cu activitățile de prevenire, detectare, investigare și urmărire penală a infracțiunilor de abuz sexual asupra copiilor.

135. Cu toate acestea, există o lipsă de specificitate în ceea ce privește punerea în aplicare practică a acestei dispoziții. În cazul în care rapoartele sunt transmise atât către Europol, cât și către o autoritate de aplicare a legii dintr-un stat membru, Propunerea nu precizează dacă este necesară o confirmare din partea unuia sau a ambilor destinatari și nici procedurile/modalitățile de obținere a acestei confirmări nu sunt precizate în Propunere (de exemplu, dacă confirmările trebuie să fie transmise prin intermediul Centrului UE). Având în vedere volumul mare de MASC pe care Europol și autoritățile naționale de aplicare a legii ar putea fi obligate să le prelucreze, precum și lipsa unui termen precis pentru furnizarea confirmării („fără întârzieri nejustificate"), CEPD și AEPD recomandă să se clarifice procedurile aplicabile pentru a asigura realizarea acestei garanții în practică. În plus, obligația de informare a utilizatorilor ar trebui să includă și informații privind destinatarii datelor cu caracter personal în cauză.

Cu privire la colectarea de date și raportarea în materie de transparență (articolul 83)

136. Articolul 83 alineatul (3) din Propunere prevede că Centrul UE colectează date și generează statistici referitoare la o serie de sarcini care îi revin în temeiul propunerii de Regulament. În scopul monitorizării, CEPD și AEPD recomandă adăugarea la această listă a statisticilor privind numărul de rapoarte transmise către Europol în conformitate cu articolul 48, precum și numărul de cereri de acces

[110] În temeiul Regulamentului modificat privind Europol, se fac excepții de la această interdicție pentru agențiile Uniunii instituite în temeiul titlului V din TFUE. Cu toate acestea, având în vedere temeiul juridic al propunerii (articolul 114 din TFUE referitor la armonizarea pieței interne), această excepție nu ar include Centrul UE propus.

primite de Europol în temeiul articolului 46 alineatele (4) și (5), inclusiv numărul de cereri aprobate și refuzate de Centrul UE.

5. CONCLUZIE

137. Deși CEPD și AEPD salută eforturile Comisiei de a asigura o acțiune eficientă împotriva abuzului sexual online asupra copiilor, acestea consideră că Propunerea ridică probleme serioase în ceea ce privește protecția datelor și a confidențialității. Prin urmare, CEPD și AEPD invită colegiuitorii să modifice propunerea de Regulament, în special pentru a se asigura că obligațiile de detectare preconizate îndeplinesc standardele aplicabile de necesitate și proporționalitate și nu au ca rezultat slăbirea sau degradarea criptării la nivel general. CEPD și AEPD rămân disponibile pentru a-și oferi sprijinul pe parcursul procesului legislativ, în cazul în care contribuția lor este considerată necesară pentru a discuta preocupările evidențiate în prezentul aviz comun.

Pentru Autoritatea Europeană pentru Protecția Datelor	Pentru Comitetul european pentru protecția datelor
Autoritatea Europeană pentru Protecția Datelor	Președinte
(Wojciech Wiewiorowski)	(Andrea Jelinek)