



Bruxelles, 7 iunie 2024
(OR. en)

10666/24

**Dosar interinstituțional:
2022/0155 (COD)**

JAI 939
ENFOPOL 276
CRIMORG 90
IXIM 149
DATAPROTECT 231
CYBER 182
COPEN 296
FREMP 284
TELECOM 202
COMPET 616
MI 572
CONSOM 209
DIGIT 151
CODEC 1431

NOTĂ

Sursă:	Președinția
Destinatar:	Comitetul Reprezentanților Permanenți / Consiliul
Subiect:	Propunerea de regulament al Parlamentului European și al Consiliului de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor – Raport intermediar

I. INTRODUCERE

1. La 11 mai 2022, Comisia a adoptat propunerea sus-menționată¹, însoțită de o evaluare a impactului și de o comunicare. Propunerea se bazează pe articolul 114 din TFUE și are două componente principale. În primul rând, furnizorii de servicii online, cum ar fi furnizorii de servicii de găzduire și de comunicații interpersonale, ar urma să fie obligați să prevină diseminarea, să detecteze, să raporteze și să elimine materialele care conțin abuzuri sexuale asupra copiilor (CSAM), precum și să prevină, să detecteze și să raporteze ademenirea copiilor („grooming”). În al doilea rând, ar urma să fie înființată o nouă agenție

¹ Doc. 9068/22.

descentralizată a UE („Centrul UE”)² pentru a sprijini punerea în aplicare a regulamentului propus, în colaborare cu o rețea de autorități naționale de coordonare și cu alte autorități competente.

2. În cadrul Consiliului, propunerea a fost examinată până în prezent în cadrul a 31 de reuniuni ale Grupului de lucru pentru asigurarea respectării legii – Poliție (LEWP-P), în vederea pregătirii unui mandat de negociere cu Parlamentul European.
3. Serviciul juridic al Consiliului a emis un aviz scris la 26 aprilie 2023³.
4. Comitetul Reprezentanților Permanenți a desfășurat dezbateri de orientare cu privire la propunerea sus-menționată la 31 mai și 13 octombrie 2023, concentrându-se asupra domeniului de aplicare al ordinului de detectare și asupra aspectelor legate de comunicațiile criptate și securitatea cibernetică. De asemenea, Consiliul a discutat chestiunea în sesiune publică la 19 octombrie și 5 decembrie 2023.
5. În cadrul Parlamentului European, Comisia pentru libertăți civile, justiție și afaceri interne (LIBE) este comisia competentă pentru negocierile care vizează propunerea. În octombrie 2022, aceasta l-a numit ca raportor pe Javier Zarzalejos (PPE, ES), deputat în Parlamentul European. Comisia LIBE și-a adoptat raportul la 14 noiembrie 2023, iar poziția Parlamentului European a fost considerată adoptată la 22 noiembrie 2023.
6. Regulamentul (UE) 2024/1307 al Parlamentului European și al Consiliului din 29 aprilie 2024 prelungește până la 3 aprilie 2026 perioada de aplicare a cadrului juridic temporar privind abuzul sexual asupra copiilor prevăzut în Regulamentul (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.

² Alegerea sediului Centrului UE va face obiectul unei proceduri interinstituționale, urmând exemplul alegerii sediului Autorității pentru Combaterea Spălării Banilor.

³ Doc. 8787/23.

II. PROGRESELE ÎNREGISTRATE ÎN CURSUL PREȘEDINȚIEI BELGIENE

7. În timpul președinției belgiene, LEWP-P a alocat mult timp și eforturi considerabile pentru a lua în considerare noi abordări ale regulamentului propus și pentru a elabora texte de compromis în cadrul reuniunilor din 1 martie⁴, 19 martie⁵, 3 aprilie⁶, 15 aprilie⁷, 8 mai, 24 mai și 4 iunie 2024⁸.
8. Președinția și-a concentrat eforturile asupra răspunsului la preocupările exprimate de unele delegații în ceea ce privește proporționalitatea și direcționarea ordinelor de detectare, precum și în ceea ce privește securitatea cibernetică:
- Președinția a propus două componente interconectate: (1) îmbunătățirea evaluării riscurilor și a clasificării riscurilor serviciilor, pentru ca ordinele de detectare să fie mai bine direcționate și (2) protejarea securității cibernetică și a datelor criptate, menținând în același timp serviciile care utilizează criptarea de la un capăt la altul în domeniul de aplicare al ordinelor de detectare.
 - Ulterior, delegațiile au lucrat la elaborarea unei metodologii de determinare a riscurilor unor servicii specifice pe baza unui set de criterii obiective (referitoare la dimensiunea, tipul și arhitectura de bază a serviciului, politicile furnizorului și funcționalitățile de siguranță din faza de proiectare, precum și o cartografiere a tendințelor utilizatorilor).
 - În urma rezultatului acestui proces de clasificare a riscurilor, sistemele sau părți ale acestora ar urma să fie clasificate drept „risc ridicat”, „risc mediu” sau „risc scăzut”. Pe baza acestei clasificări, ar putea fi impuse măsuri suplimentare de atenuare a riscurilor furnizorilor clasificați în categoriile cu risc mediu și ridicat. În cazul în care încă predomină riscuri semnificative după punerea în aplicare a măsurilor suplimentare de atenuare a riscurilor, autoritatea de coordonare ar putea lua în considerare solicitarea emiterii unui ordin de detectare ca măsură de ultimă instanță pentru serviciile care sunt clasificate ca prezentând un risc ridicat. Furnizorii ar putea, de asemenea, să semnaleze în mod voluntar autorității de coordonare din statul membru de stabilire dacă au suspiciuni că serviciile lor sunt utilizate pentru abuzuri sexuale asupra copiilor, ceea ce ar putea necesita emiterea de ordine de detectare.

⁴ Doc. 6850/24.

⁵ Doc. 7462/24.

⁶ Doc. 8019/24.

⁷ Doc. 8579/24.

⁸ Doc. 9093/24.

- Președinția a propus menținerea serviciilor care utilizează criptarea de la un capăt la altul în domeniul de aplicare al ordinelor de detectare emise către servicii cu grad ridicat de risc, cu condiția ca acest lucru să nu oblige furnizorii să creeze acces la datele criptate de la un capăt la altul și ca tehnologiile utilizate pentru detectare să fie verificate în ceea ce privește eficacitatea lor, impactul lor asupra drepturilor fundamentale și riscurile la adresa securității cibernetice.
 - În urma discuțiilor la nivel tehnic, președinția și-a adaptat abordarea și a sugerat adăugarea unor garanții suplimentare pentru a asigura proporționalitatea și respectarea drepturilor fundamentale, și anume limitarea domeniului de aplicare al ordinelor de detectare la conținutul vizual și URL-uri, raportarea întârziată după două rezultate pozitive constând în materiale noi care conțin abuzuri sexuale asupra copiilor pentru a reduce rezultatele fals pozitive, pseudonimizarea noilor materiale detectate care conțin abuzuri sexuale asupra copiilor înainte de verificarea umană și protecția datelor criptate de la un capăt la altul, permițând în același timp detectarea în comunicarea interpersonală prin moderarea încărcării, care să necesite consimțământul utilizatorilor.
 - De asemenea, președinția s-a străduit să clarifice faptul că detectarea nu ar trebui să se aplice conturilor utilizate de stat în scopuri de securitate națională, pentru menținerea ordinii publice sau în scopuri militare.
9. În cadrul reuniunii LEWP-P din 4 iunie 2024, președinția a remarcat că nu este necesar să se continue examinarea la nivel tehnic, întrucât toate chestiunile tehnice au fost abordate în mod cuprinzător.
10. Președinția se angajează să ajungă la un compromis și intenționează, în urma prezentării progreselor în cadrul Consiliului din 13 iunie 2024, să emită un text de compromis și, ulterior, să invite Comitetul Reprezentanților Permanenți să convină asupra unui mandat de negociere parțial⁹.

III. CONCLUZIE

11. Comitetul Reprezentanților Permanenți/Consiliul este invitat să ia act de progresele înregistrate de președinție cu privire la Regulamentul de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor.

⁹ „Parțial” deoarece alegerea sediului Centrului UE este exclusă.