COMISIA
EUROPEANĂ

Bruxelles, 11.12.2025
COM(2025) 752 final

# RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

**privind evaluarea și analizarea impactului operațional al punerii în aplicare a atribuțiilor prevăzute în Regulamentul (UE) 2022/991, în special la articolul 4 alineatul (1) litera (t), la articolul 18 alineatul (2) litera (e), la articolul 18 alineatul (6a) și la articolele 18a, 26, 26a, 26b, în ceea ce privește obiectivele Europol, precum și a impactului atribuțiilor respective asupra drepturilor și libertăților fundamentale, astfel cum sunt prevăzute în Cartă, în temeiul articolului 68 alineatul (3) din Regulamentul (UE) 2016/794**

{SWD(2025) 404 final}

## 1. Domeniul de aplicare al evaluării

De la începerea activității sale în 1999, **Agenția UE pentru Cooperare în Materie de Aplicare a Legii (Europol)** a jucat **un rol central în combaterea criminalității transfrontaliere grave și a terorismului**, devenind un factor-cheie al cooperării în materie de asigurarea respectării legii în Europa. Situația în materie de securitate a suferit schimbări drastice în ultimii 30 de ani, cu o schimbare corespunzătoare în ceea ce privește formele grave de criminalitate și criminalitatea organizată[1]. Statele membre au noi nevoi operaționale în ceea ce privește abordarea eficace a amenințărilor emergente; totodată, **așteptările lor cu privire la sprijinul Europol au evoluat**. Prin urmare, mandatul Europol a fost înlocuit sau modificat de mai multe ori pentru a menține și a spori relevanța agenției.

Mandatul Europol, astfel cum este definit în Regulamentul (UE) 2016/794[2] (denumit în continuare „Regulamentul privind Europol" sau „RE"), a fost modificat ultima dată în 2022 prin Regulamentul (UE) 2022/991[3] pentru a răspunde noilor amenințări la adresa securității. Regulamentul privind Europol nu mai era adecvat scopului în noua realitate, în care infractorii profită de avantajele **transformării digitale**, **ale noilor tehnologii**, **ale globalizării** și **ale mobilității**[4].

**Obiectivele specifice** ale Regulamentului (UE) 2022/991[5] erau:

- asigurarea unei cooperări eficace între **părțile private** și autoritățile de aplicare a legii pentru a combate utilizarea abuzivă a serviciilor transfrontaliere de către infractori;
- abilitarea autorităților de aplicare a legii să analizeze **seturi de date mari și complexe** pentru a detecta legături transfrontaliere, cu respectarea deplină a **drepturilor fundamentale**;
- abilitarea statelor membre să utilizeze **noile tehnologii** pentru asigurarea respectării legii.

În plus, Regulamentul (UE) 2022/991 a modificat normele de protecție a datelor aplicabile Europol pentru a menține **un nivel ridicat de protecție a datelor**, asigurând un echilibru între noile competențe ale agenției de prelucrare a datelor cu caracter personal și protecția vieții private și a datelor cu caracter personal ale persoanelor fizice. Acesta a aliniat în mare măsură normele privind protecția datelor aplicabile Europol la cele aplicabile altor agenții și organisme ale UE din domeniul justiției și afacerilor interne (JAI) în temeiul capitolului IX din Regulamentul (UE) 2018/1875 („Regulamentul UE privind protecția datelor" sau „RPDUE") și la cele aplicabile autorităților de aplicare a legii din statele membre („autoritățile competente") în temeiul dreptului lor intern de transpunere a Directivei (UE) 2016/680

---

1 Europol, 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) – The changing DNA of serious and organised crime („Evaluarea din 2025 a amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în Uniunea Europeană – Formele grave de criminalitate și criminalitatea organizată își schimbă caracterul"), disponibilă online la adresa https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf („EU SOCTA 2025"). A se vedea, de asemenea, evaluarea amenințărilor în domeniul vamal (*Customs threat assessment* – CTA) 2025, disponibilă online la adresa https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 JO L 135, 24.5.2016, p. 53, ELI: https://eur-lex.europa.eu/eli/reg/2016/794/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

3 JO L 169, 27.6.2022, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/991/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

4 SWD(2020) 543 final din 9 decembrie 2020, p. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Ibidem.*

(„Directiva privind protecția datelor în materie de asigurare a respectării legii” sau „LED”)[6] pentru a **facilita fluxul de informații**.

Prezentul raport a fost adoptat în conformitate cu obligația care îi revine Comisiei, în temeiul **articolului 68 alineatul (3) din RE**, de a evalua[7] și de a examinat impactul operațional al sarcinilor Europol, astfel cum sunt prevăzute în Regulamentul (UE) 2022/991, la trei ani de la intrarea sa în vigoare. Conform mandatului acordat de colegiuitori, Comisia: în primul rând, a evaluat și a examinat **impactul operațional** al unora dintre noile norme privind prelucrarea datelor cu caracter personal, în raport cu obiectivele Europol, în temeiul articolului 3 din RE (și anume: sprijinirea și consolidarea acțiunii autorităților competente ale statelor membre și a cooperării lor reciproce în ceea ce privește prevenirea și combaterea infracțiunilor care intră sub incidența mandatului Europol); în al doilea rând, a evaluat impactul acestor norme asupra **drepturilor și libertăților fundamentale** (denumite în continuare „drepturile fundamentale”), astfel cum sunt consacrate în cartă[8], și, în al treilea rând, a efectuat o **analiză cost-beneficiu** a sarcinilor de prelucrare a datelor aferente.

Pentru a pregăti revizuirea, serviciile Comisiei au colectat informații și feedback din diferite surse și au organizat consultări ad-hoc cu Europol și cu statele membre. **Documentul de lucru al serviciilor Comisiei** care însoțește prezentul raport oferă o descriere detaliată a contextului general și a metodologiei de revizuire, precum și o prezentare cuprinzătoare a surselor de dovezi și a consultărilor care confirmă principalele constatări rezumate în prezentul raport.

## 2. Contextul general

În conformitate cu articolul 68 alineatul (3) din RE, prezentul raport al Comisiei acoperă anumite dispoziții din Regulamentul (UE) 2022/991, concentrându-se asupra cinci aspecte-cheie ale activității Europol.

### (1) Dimensiunea externă: articolul 4 alineatul (1) litera (t) din RE privind semnalările privind existența de informații referitoare la resortisanți ai țărilor terțe în Sistemul de informații Schengen (SIS), la propunerea Europol

Având în vedere **caracterul global al infracțiunilor grave și al terorismului**, informațiile deținute de țările terțe și de organizațiile internaționale cu privire la autorii și la persoanele suspectate de astfel de infracțiuni sunt din ce în ce mai relevante pentru securitatea internă a UE. Dimensiunea externă a cooperării UE în materie de asigurare a respectării legii a devenit, prin urmare, esențială pentru statele membre, la fel ca **rolul Europol în sprijinirea statelor membre în parteneriatele lor cu țări terțe** sau cu entități situate în țările respective. În viitor vor fi necesare **eforturi suplimentare pentru consolidarea** pentru consolidarea securității mondiale[9].

Regulamentul (UE) 2022/991 a introdus deja modificări substanțiale în Regulamentul privind Europol pentru a consolida **dimensiunea externă a activităților Europol**, în special facilitând

---

[6] JO L 119, 4.5.2016, p. 89, ELI: https://eur-lex.europa.eu/eli/dir/2016/680/oj?eliuri=eli%3Adir%3A2016%3A680%3Aoj&locale=ro.

[7] Această evaluare efectuată în conformitate cu articolul 68 alineatul (3) din RE nu este evaluarea care trebuie efectuată în conformitate cu Orientările privind o mai bună legiferare în vederea unei posibile propuneri de revizuire a Regulamentului privind Europol. Vezi și secțiunea 4 de mai jos.

[8] Carta drepturilor fundamentale a Uniunii Europene, JO C 326, 26.10.2012, p. 391, ELI: https://eur-lex.europa.eu/eli/treaty/char_2012/oj?eliuri=eli%3Atreaty%3Achar_2012%3Aoj&locale=ro.

[9] A se vedea ProtectEU: o strategie europeană de securitate internă COM(2025) 148 final din 1 aprilie 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0148.

schimbul de informații cu țările terțe[10] și solicitând Europol să includă o strategie pentru relațiile cu țările terțe și cu organizațiile internaționale în programarea sa multianuală și în programele sale de lucru anuale[11].

**Articolul 4 alineatul (1) litera (t)** din RE a atribuit Europol o nouă sarcină: sprijinirea statelor membre în prelucrarea datelor privind persoanele implicate în acte de terorism sau în infracțiuni grave furnizate de țări terțe sau de organizații internaționale. Sarcina include **propunerea adresată statelor membre de a introduce, eventual, semnalări privind existența unor informații referitoare la resortisanți ai țărilor terțe în interesul Uniunii în Sistemul de informații Schengen (SIS)**. Această nouă categorie de semnalări privind existența unor informații a fost introdusă în 2022[12], în urma unei modificări a Regulamentului (UE) 2018/1862 privind utilizarea SIS în domeniul cooperării polițienești și al cooperării judiciare în materie penală[13].

În special atunci când persoana în cauză nu este cetățean al UE și nu există nicio legătură cu un caz național, anumite informații sunt comunicate de țara terță numai către Europol, care prelucrează datele și comunică rezultatele analizelor sale tuturor statelor membre. Scopul noilor dispoziții a fost de a **maximiza exploatarea informațiilor** primite de Europol din țări terțe, făcându-le mai accesibile comparativ cu situația în care ar fi fost disponibile numai prin intermediul propriului sistem al Europol. Acestea au completat alte măsuri, cum ar fi portalul european de căutare (ESP) și cadrul de interoperabilitate[14] dintre sistemele de informații ale UE pentru gestionarea securității, a frontierelor și a migrației, abordând deficiențele structurale ale acestor sisteme care împiedică activitatea autorităților naționale și, în special, a polițiștilor de frontieră.

**SIS** este considerat un **canal suplimentar esențial de diseminare**: acesta este cea mai utilizată bază de date din Europa pentru asigurarea respectării legii, pentru controlul la frontiere și pentru migrație. În 2024, au fost efectuate peste 15 miliarde de căutări în SIS, comparativ cu aproximativ 14 milioane de căutări în sistemul informațional Europol (EIS) și cu mai puțin de 3 miliarde de căutări (la nivel mondial) în cele 19 baze de date ale INTERPOL, care sunt celelalte două sisteme de informații principale pentru autoritățile competente[15].

---

10 A se vedea, de exemplu, articolul 25 alineatul (4a) din RE, care prevede posibilitatea ca Europol să transfere date către țări terțe după ce efectuează o autoevaluarea tuturor circumstanțelor legate de transferul de date cu caracter personal și concluzionează că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal, și articolul 25 alineatul (5) din RE, care extinde domeniul de aplicare al cazurilor excepționale în care Europol poate transfera ad-hoc, în cazuri justificate în mod corespunzător, (categorii de) date către țări terțe și organizații internaționale.

11 Articolul 12 alineatul 2 din RE.

12 Regulamentul (UE) 2022/1190; JO L 185, 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Regulamentul (UE) 2018/1862; JO L 312, 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Regulamentul (UE) 2019/818; JO L 135, 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 Raportul anual privind SIS al eu-LISA din 2024, disponibil online la adresa https://www.eulisa.europa.eu/sites/default/ files/documents/sis-annual-report-2024.pdf, Europol, Raportul anual de activitate consolidat (CAAR) 2024, disponibil online la adresa https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF, și https://www.interpol.int/How-we-work/Databases.

**(2) <u>Inovare</u>: articolul 18 alineatul (2) litera (e) și articolul 33a din RE privind prelucrarea datelor cu caracter personal de către Europol pentru proiecte de inovare și cercetare**

**Evoluțiile tehnologice** prezintă atât oportunități enorme, cât și provocări considerabile pentru securitatea internă a UE[16] și au avut un impact atât de profund asupra criminalității, încât au modificat chiar natura, „ADN-ul" amenințărilor pe care le reprezintă formele grave de criminalitate și criminalitatea organizată[17]. Infractorii incorporează rapid noile tehnologii în operațiunile lor, creând noi modele de afaceri și perfecționându-și tacticile. În același timp, aceste progrese oferă **autorităților de aplicare a legii oportunități fără precedent de a-și consolida capacitățile**. Prin urmare, cercetarea și inovarea joacă un rol esențial în securitatea internă prin dezvoltarea de soluții menite să contracareze amenințările emergente și să țină pasul cu formele și *modus operandi* în continuă evoluție ale rețelelor infracționale, inclusiv cele care rezultă din utilizarea abuzivă a tehnologiei. Uniunea a investit și va continua să investească în dezvoltarea de instrumente inovatoare prin intermediul cercetării și inovării în domeniul securității finanțate de UE, prin intermediul **ProtectEU**, Strategia europeană de securitate internă[18].

Înființat la finalul anului 2019, în cadrul mandatului miniștrilor JAI din statele membre ale UE, **Laboratorul de inovare al Europolului (EIL)**[19] urmărește să impulsioneze angajamentul Europol față de inovarea în materie de asigurare a respectării legii. Regulamentul (UE) 2022/991 a introdus modificări substanțiale în Regulamentul privind Europol pentru a consolida mandatul Europol în materie de inovare, atât pentru a sprijini potențialul EIL, cât și pentru a promova sinergii cu alte activități de cercetare și inovare la nivelul UE, în special în cadrul Comisiei, sub egida **Centrului de inovare al UE** pentru securitate internă[20].

Articolul 18 alineatul (2) din RE privind activitățile de prelucrare a informațiilor a fost modificat pentru a permite Europol să **prelucreze date operaționale cu caracter personal** și **în cadrul proiectelor de cercetare și inovare**. Disponibilitatea unor seturi de date de înaltă calitate pentru a permite testarea empirică a validității noilor instrumente este considerată în general o condiție prealabilă esențială pentru dezvoltarea de tehnologii. În schimb, seturile de date nefiabile sau părtinitoare utilizate pentru testare pot duce la producerea unor tehnologii mediocre[21].

Garanții adaptate în materie de protecție a datelor pentru o astfel de prelucrare au fost prevăzute la articolul 18 alineatul (3a), la articolul 30 alineatele (2) și (3) și la articolul **33a din RE**. Acest din urmă articol impunea crearea unui **spațiu de testare**, stipulând că toate datele cu caracter personal prelucrate în cadrul unui proiect trebuie să fie copiate temporar într-un spațiu separat, izolat și protejat de prelucrare a datelor în cadrul Europol, pentru a fi utilizate exclusiv pentru proiectul respectiv.

---

16 Europol, Internet Organised Crime Threat Assessment (IOCTA) (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online) 2024, disponibil online la adresa Internet Organised Crime Threat Assessment (IOCTA) 2024 | Europol.

17 Europol, EU SOCTA 2025, p. 19.

18 COM(2025) 148 final din 1 aprilie 2025, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52025DC0148, p. 9.

19 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02016L0680-20160504

20 A se vedea, în special, articolul 4 alineatul (1) literele (v) și (w) din RE.

21 SWD(2020) 543 final din 9 decembrie 2020, p. 29.

**(3) <u>Anchete penale</u>: articolul 18 alineatul (6a) și articolul 18a din RE privind condițiile de prelucrare a datelor cu caracter personal primite fără clasificarea persoanelor vizate (DSC)**

În rolul său de **centru de informații în materie penală al UE**, Europol nu numai că facilitează colectarea și schimbul de informații, ci și contribuie la **creșterea eficacității anchetelor printr-o analiză avansată a datelor** și prin detectarea legăturilor dintre infracțiuni și rețelele infracționale transfrontaliere care nu sunt vizibile la nivel național. Aceste capacități sprijină statele membre prin creșterea volumului de informații disponibile ce pot fi utilizate în anchete penale.

Odată cu utilizarea extinsă și intensivă a tehnologiei, **seturile de date mari și complexe au devenit noua normalitate în toate aspectele vieții**, inclusiv în ceea ce privește criminalitatea[22]. Anchetele privind criminalitatea organizată sau terorismul au început să se confrunte cu provocarea de a analiza volume mari de date stocate electronic, care sunt adesea de ordinul terabiților, conținând inclusiv date audio, video și generate automat, confiscate în cursul anchetelor. De exemplu, în cadrul anchetei comune de desființare a rețelei EncroChat[23], anchetatorii au avut de analizat milioane de mesaje pe care infractorii și le-au trimis unii altora pentru a planifica infracțiuni grave. În acest context, disponibilitatea instrumentelor, a expertizei și a resurselor necesare în domeniul tehnologiei informației și a comunicațiilor (TIC) pentru a analiza seturi de date mari și complexe [cunoscute în jargonul tehnic sub denumirea de „volume mari de date" sau („*big data*")[24]] este esențială pentru autoritățile de aplicare a legii și autoritățile judiciare.

Deși Regulamentul privind Europol adoptat în 2016 nu a impus, în sine, restricții privind analiza volumelor mari de date, acesta nu conținea dispoziții structurate care să stabilească condițiile cu privire la analizarea acestui tip de date. Punctul **cel mai critic** a fost **cerința DSC**. DSC se referă la necesitatea de a examina seturile de date pentru a clasifica datele cu caracter personal în funcție de diferite categorii, enumerate în mod exhaustiv în anexele II.A. și II.B. la Regulamentul privind Europol, înainte de a proceda la prelucrarea efectivă a datelor în scopuri de investigare, inclusiv înainte de verificarea încrucișată a datelor pentru a detecta legăturile sau înainte de efectuarea de analize de natură strategică sau tematică sau de analize operaționale[25]. Categoriile relevante sunt legate de diferite tipuri de implicare în anchetele penale, inclusiv (i) suspecții, potențiali viitori infractori; precum și (ii) contactele, asociații, victimele, martorii și informatorii asociați cu activități infracționale. În general, Europol nu poate nici să prelucreze, nici să stocheze datele cu caracter personal ale persoanelor care nu se încadrează în niciuna dintre aceste categorii.

Furnizorii de date, precum **statele membre** sau **organismele și agențiile UE**, efectuează deja, de regulă, DSC înainte de a transfera datele cu caracter personal către Europol[26]. În temeiul dreptului UE, toate statele membre sunt obligate să efectueze DSC pentru propriile activități

---

22 Europol, EU SOCTA 2025, *passim*.

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochatcommunications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 AEPD, Opinia 7/2015, p. 7, disponibilă la https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf. „În termeni generali, ca numitor comun al diferitelor definiții disponibile, „**volumele mari de date**" se referă la practica de a combina volume uriașe de informații din surse diferite și de a le analiza, utilizând algoritmi mai sofisticați pentru a fundamenta deciziile. Volumele mari de date se bazează nu numai pe capacitatea tot mai mare a tehnologiei de a sprijini colectarea și stocarea unor cantități mari de date, ci și pe capacitatea acesteia de a analiza, de a înțelege și de a profita de întreaga valoare a datelor (în special utilizând aplicații de analiză a datelor)".

25 A se vedea articolul 18 alineatul (2) din ER.

26 Statele membre transferă date către Europol prin intermediul aplicației sale de rețea pentru schimbul securizat de informații (SIENA), unde DSC este introdusă drept un câmp obligatoriu.

de prelucrare și pentru propriile investigații, indiferent de transferul de date către Europol, această analiză bazându-se pe norme echivalente, dar nu identice, cu cele ale Europol[27]. Cu toate acestea, pentru seturile de date mari și complexe, operațiunea de prelucrare anterioară manuală consumă resurse și necesită mult timp. Analiza datelor dintr-un singur telefon mobil poate dura, în mod semiautomatizat, până la trei zile, iar într-o singură anchetă pot fi confiscate chiar și sute de telefoane mobile. DSC pentru **volumele mari de date nu este întotdeauna posibilă**, având în vedere volumul mare al seturilor de date, modul în care sunt (ne)structurate datele, lipsa resurselor sau necesitatea **efortului manual excesiv**. În practică, singura posibilitate este de a analiza mai întâi datele în profunzime din punct de vedere operațional sau de a detecta legăturile, tot în mod semiautomatizat, prin verificarea încrucișată a datelor disponibile.

Regulamentul (UE) 2022/991 a clarificat condițiile pentru ca DSC să ofere **securitate juridică** în ceea ce privește prelucrarea seturilor de date mari și complexe. Europol și Autoritatea Europeană pentru Protecția Datelor (AEPD) au interpretat în mod diferit litera și spiritul Regulamentului privind Europol în ceea ce privește perioada aplicabilă de păstrare a datelor. Potrivit Europol, această perioadă ar trebui să fie de trei ani; potrivit AEPD, aceasta ar trebui să fie de șase luni[28]. De asemenea, au fost necesare noi dispoziții pentru a oferi **un grad suplimentar de flexibilitate**, asigurând un just echilibru între protecția datelor și aspectele legate de securitate.

Articolul 18 alineatul (5a) din RE, coroborat cu articolul 73 din RPDUE, a clarificat mai întâi principiul general al DSC în temeiul articolului 18 alineatul (2) și al anexei II. Europol este însărcinat, după caz și pe cât posibil, **să atribuie în mod clar datele cu caracter personal unei categorii specifice de persoane vizate**. În practică, Europol ar trebui să stabilească, ca regulă generală, rolul exact în activitatea infracțională (de exemplu, dacă o persoană este suspect, victimă sau doar martor) pentru fiecare persoană ale cărei date cu caracter personal vor fi prelucrate, și nu la nivel agregat pentru toate persoanele dintr-un fișier de date care urmează să fie prelucrat sau dintr-o parte a acestuia (de exemplu, prin simpla stabilire a faptului că toate persoanele menționate sunt implicate într-o activitate infracțională care intră sub incidența mandatului său pe baza unei examinări a circumstanțelor generale care au generat fișierul de date) înainte ca datele cu caracter personal să poată fi prelucrate.

Articolul 18 alineatul (6a) din RE permite în mod explicit prelucrarea datelor cu caracter personal primite fără DSC pentru **o perioadă de până la 18 luni**, care poate fi prelungită până la 36 de luni în cazuri justificate, exclusiv în **scopul completării DSC**. Articolul 18 alineatul (6a) din RE nu se referă în mod explicit la seturi de date mari și complexe, ci, la nivel general, necesită un test de „**strictă necesitate**”.

Articolul 18a din RE prevede o derogare, permițând Europol să prelucreze datele cu caracter personal primite de la **o autoritate competentă**, de la Parchetul European (**EPPO**) sau de la **Eurojust**, în cazul în care acest lucru este necesar pentru a sprijini o **anchetă penală în curs**,

---

[27] A se vedea, de exemplu, articolul 6 din Directiva (UE) 2016/680 („Directiva privind protecția datelor în materie de asigurare a respectării legii” în ceea ce privește autoritățile competente în mod indirect); JO L 119, 4.5.2016, p. 89, ELI: https://eur-lex.europa.eu/eli/dir/2016/680/oj?eliuri=eli%3Adir%3A2016%3A680%3Aoj&locale=ro; Articolul 51 din Regulamentul (UE) 2017/1939 al Consiliului („Regulamentul privind EPPO”); JO L 283, 31.10.2017, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2017/1939/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro; Articolul 27 alineatul (3) din Regulamentul (EU) 2018/1727 („Regulamentul privind Eurojust”); JO L 295, 21.11.2018, p. 138, ELI: https://eur-lex.europa.eu/eli/reg/2018/1727/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

[28] https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

fără a fi necesară efectuarea DSC, în cazul în care aceasta nu a fost încă efectuată, și în afara categoriilor de persoane vizate enumerate în Regulamentul privind Europol. Europol poate prelucra datele printr-o **analiză operațională,** sau, în cazuri excepționale și justificate corespunzător, prin **verificări încrucișate** pentru a identifica conexiunile sau alte legături relevante. Această derogare a fost concepută pentru a aborda diferențele dintre normele privind DSC aplicabile Europol și cele aplicabile autorităților competente, EPPO și Eurojust.

**(4) Cooperarea cu terți: Articolele 26, 26a și 26b din RE privind schimbul de date cu caracter personal între Europol și părți private**

Infractorii abuzează din ce în ce mai mult de serviciile (transfrontaliere) ale părților private, precum serviciile bazate pe internet, serviciile financiare și serviciile clasice de telecomunicații. În consecință, **părțile private dețin un volum însemnat de date cu caracter personal relevante pentru anchetele penale**. În special, internetul a creat un spațiu public care se este deținut de părți private, ceea ce face dificilă aplicarea normelor în spațiul online cu scopul de a asigura respectarea legii într-un mod la fel de eficient ca și în spațiul offline.[29]

În acest context, **cooperarea dintre autoritățile de aplicare a legii și părțile private** a devenit **indispensabilă.** Astfel cum se prevede în **ProtectEU**, Strategia europeană de securitate internă, consolidarea parteneriatelor cu sectorul privat va fi esențială pentru facilitarea schimbului de informații.[30] Șefii serviciilor de poliție au solicitat, de asemenea, în declarația lor comună privind viitorul Europol[31], ca Europol să servească drept „**portal esențial pentru obținerea de informații de la entități private**". Natura acestei colaborări variază de la schimbul de informații și furnizarea de date comerciale cu sursă deschisă până la implicarea în proiecte de cercetare și inovare și furnizarea de servicii care sprijină funcționarea întreprinderilor.[32] De exemplu, în 2025, Europol a dejucat cu succes operațiunea „Lumma stealer", cea mai semnificativă amenințare de „hoți de informații" („infostealer") din lume, prin cooperarea cu Microsoft, care identificase, la nivel mondial, peste 394 000 de calculatoare Windows infectate cu programul malware Lumma[33].

Regulamentul (UE) 2022/991 a introdus **posibilități suplimentare** pentru Europol de a face schimb de date cu caracter personal cu părți private. Înainte, Europol putea primi date cu caracter personal de la părți private numai prin intermediul unei unități naționale Europol (ENU) sau prin intermediul unor puncte de contact sau autorități identificate în prealabil ale țărilor terțe sau ale organizațiilor internaționale. Scopul prelucrării de către Europol era limitat la identificarea ENU relevante sau a punctului de contact sau a autorității de contact a țării terțe sau a organizației internaționale care ar fi putut să își asume responsabilitatea pentru cazul respectiv.

**Forma modificată a articolului 26 din RE a extins sarcina Europol**, permițându-i să prelucreze în mod cuprinzător informațiile (inclusiv datele cu caracter personal) provenite de la părți private. Unul dintre scopurile principale ale prelucrării a rămas identificarea unității naționale Europol (ENU) în cauză. Cu toate acestea, Europol este autorizat acum să completeze

---

29 SWD(2020) 543 final din 9 decembrie 2020, p. 16.

30 A se vedea ProtectEU: o strategie europeană de securitate internă, p. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Cooperarea cu părțile private, 31 mai 2023, EDOC #1306090v13. A se vedea, de asemenea, Milieu Consulting, Study on the Practice of direct exchange with of personal data between Europol and Private Parties (Studiu privind practica schimburilor directe de date cu caracter personal între Europol și părțile private), raport final, septembrie 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Alte exemple sunt disponibile în documentul de lucru al serviciilor Comisiei.

informațiile și cu propria sa analiză pentru a facilita prelucrarea ulterioară a unui caz la nivel național.

Pe lângă dispozițiile orizontale de la articolul 26 din RE, articolul 26a din RE a introdus norme pentru **situațiile de criză online**, iar articolul 26b a abordat **diseminarea online a materialelor care conțin abuzuri sexuale asupra copiilor**. În aceste cazuri, Europol poate acorda asistență statelor membre prin prelucrarea datelor cu caracter personal primite direct de la părți private. Europol are și posibilitatea de a transmite date cu caracter personal părților private, de la caz la caz.

Regulamentul (UE) 2022/991 a introdus posibilitatea de a utiliza infrastructura Europol pentru schimbul de informații între autoritățile competente și părți private, precum și capacitatea Europol de a solicita statelor membre să obțină, în conformitate cu legislația lor națională, date cu caracter personal de la părți private.

Aceste dispoziții au fost adoptate în concordanță cu alte inițiative, cum ar fi Regulamentul privind conținutul online cu caracter terorist (TCO)[34] și Regulamentul privind serviciile digitale (DSA)[35]. Se au în vedere măsuri suplimentare de consolidare a implicării părților private în lupta împotriva criminalității și de facilitare a accesului legal la date pentru a realiza „ambiția unei schimbări a culturii în materie de securitate” (**abordare la nivelul întregii societăți**) în cadrul **ProtectEU**, Strategiei europeană de securitate internă[36].

### (5) Supravegherea internă și externă a respectării drepturilor fundamentale de către Europol

Regulamentul (UE) 2022/991 subliniază obligația Europol de a respecta drepturile fundamentale în temeiul dispozițiilor care definesc sarcinile Europol și al garanțiilor conexe consolidate, în special prin **consolidarea supravegherii interne și externe a agenției**.

În domeniul protecției datelor, alinierea Regulamentului privind Europol la garanțiile în materie de protecție a datelor prevăzute în RPDUE a necesitat introducerea unor noi norme pentru supravegherea de către **responsabilul cu protecția datelor** (RPD) și de către **Autoritatea Europeană pentru Protecția Datelor** (AEPD). De exemplu, obligația de a furniza o evaluare a impactului asupra protecției datelor (EIPD) și consultarea prealabilă a AEPD au devenit sistematice pentru orice nou tip de prelucrare. Regulamentul (UE) 2022/991 a introdus, de asemenea, o nouă competență pentru Europol în ceea ce privește cererile de exercitare a drepturilor de acces. Înainte, autoritățile naționale competente erau responsabile cu tratarea cererilor de exercitare a drepturilor de acces în cazul în care statele membre erau furnizorii de date.

Regulamentul (UE) 2022/991 a instituit, de asemenea, **un nou post de ofițer pentru drepturile fundamentale** (FRO) în cadrul Europol, care este însărcinat, *printre altele*, să îl informeze pe directorul executiv al Europol cu privire la posibilele încălcări ale drepturilor fundamentale în cadrul activităților agenției.

În plus, **controlul democratic și responsabilitatea** au fost **consolidate** prin monitorizarea politică a activităților Europol de către **Parlamentul European și parlamentele naționale**, astfel cum se prevede la articolul 88 alineatul (2) al doilea paragraf din Tratatul privind funcționarea Uniunii Europene (TFUE). Regulamentul (UE) 2022/991 a consolidat

---

[34] Regulamentul (UE) 2021/784; JO L 172, 17.5.2021, p. 79, ELI: https://eur-lex.europa.eu/eli/reg/2021/784/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

[35] Regulamentul (UE) 2022/2065; JO L 277, 27.10.2022, p. 1, ELI: https://eur-lex.europa.eu/eli/reg/2022/2065/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

[36] A se vedea ProtectEU: o strategie europeană de securitate internă, p. 2.

monitorizarea efectuată de **Grupul mixt de control parlamentar specializat** (JPSG)[37]. De exemplu, acesta prevede consultarea obligatorie a JPSG cu privire la proiectul de programare multianuală și programul anual de lucru al Europol, posibilitatea ca JPSG să adreseze Europol recomandări specifice fără caracter obligatoriu și să le prezinte Parlamentului European și parlamentelor naționale, precum și instituirea unui forum consultativ care să asiste JPSG, la cerere, prin furnizarea de consiliere independentă cu privire la aspecte legate de drepturile fundamentale.

## 3. Constatările principale ale evaluării

### *3.1. Situația actuală a punerii în aplicare operaționale a noilor competențe și sarcini ale Europol în materie de prelucrare a datelor cu caracter personal*

Regulamentul (UE) 2022/991 **a intrat în vigoare la 28 iunie 2022**. Cu toate acestea, punerea sa în aplicare operațională a depins de diverse măsuri de guvernanță, tehnice și administrative, precum și de cerințe operaționale, precum crearea de noi structuri TIC, în anumite cazuri.

Trei ani mai târziu, **aproape toate dispozițiile** enumerate la articolul 68 alineatul (3) din Regulamentul (UE) 2022/991 **au devenit operaționale**. Dispozițiile referitoare la analiza seturilor de date mari și complexe [articolul 18 alineatul (6a) și articolul 18a din RE] și cooperarea cu părți private (articolele 26, 26a și 26b din RE) au început să se aplice de la 28 iunie 2022 sau la scurt timp după această dată. Prelucrarea datelor cu caracter personal pentru proiecte de cercetare și inovare [articolul 18 alineatul (2) litera (e) din RE] a început în 2023, după ce spațiul de testare, denumit ODIN, a fost instituit pentru a respecta cerințele specifice de protecție a datelor în temeiul articolului 33a din RE. Până la 29 iunie 2025, posibilitatea ca Europol să propună statelor membre **semnalări privind informații în SIS** în conformitate cu articolul 4 alineatul (1) litera (t) din RE nu devenise încă operațională, deoarece punerea în aplicare tehnică a noului tip de semnalare este încă în curs. Se preconizează că sistemul va deveni operațional **în 2026**.

### *3.2. Evaluarea impactului operațional al noilor competențe și sarcini ale Europol în materie de prelucrare a datelor cu caracter personal asupra obiectivelor agenției în temeiul articolului 3 din RE*

În ceea ce privește impactul operațional al noilor competențe și sarcini ale Europol în materie de prelucrare a datelor cu caracter personal, consultarea a indicat că **statele membre mențin, în general, o perspectivă favorabilă** în privința relevanței, eficacității și valorii adăugate a acestora, precum și asupra sprijinului acordat de Europol autorităților lor competente în domeniile conexe[38].

Competențele de investigare care fac obiectul acestei evaluări nu sunt utilizate în mod continuu sau sistematic pentru prelucrarea datelor în scopuri de monitorizare; unele au chiar un caracter excepțional, în timp ce altele sunt utilizate mai frecvent, în funcție de necesități, în cadrul investigațiilor. **Utilizarea operațională a noilor dispoziții** în perioada de referință **a variat semnificativ** din punct de vedere **cantitativ**, în funcție de diferitele caracteristici tehnice și condiții juridice asociate acestora.

Europol a primit un număr **deloc neglijabil** de noi contribuții fără DSC din partea statelor membre în temeiul articolului 18 alineatul (6a) din RE, și anume 653 de contribuții în 2023 și 597 de contribuții în 2024. Nu a existat o creștere pe termen scurt a contribuțiilor fără DSC, iar

---

37 Consultați https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

38 A se vedea dovezile prezentate în secțiunea 5 din documentul de lucru al serviciilor Comisiei care însoțește prezentul raport și, în special, observațiile Europol și răspunsurile statelor membre la întrebările 2, 4 și 5 din chestionarul scurt din 2 iunie 2025, din anexa III la documentul de lucru al serviciilor Comisiei.

numărul de cazuri în care s-a aplicat articolul 18 alineatul (6a) a rămas **constant** în comparație cu cazurile echivalente din perioada anterioară datei de 28 iunie 2022. De asemenea, noile dispoziții nu au avut niciun impact negativ asupra implicării statelor membre în punerea în aplicare a DSC[39]. Între 2023 și 2024, ponderea contribuțiilor fără DSC reprezenta **mai puțin de 1% din totalul contribuțiilor** acceptate de Europol din partea statelor membre (0,85% în 2023 și 0,71% în 2024). Începând cu iunie 2022, Europol a finalizat în mod constant DSC în termen de 18 luni, fără a apela la posibilitatea de prelungire la 36 luni. Europol și șase state membre au subliniat faptul că, în pofida îmbunătățirii securității juridice, **sarcina administrativă a rămas semnificativă** atât pentru Europol, cât și pentru autoritățile competente, prin prisma eforturilor necesare pentru a respecta clasificarea datelor cu caracter personal raportată la implicarea individuală în infracțiune. Această cerință este pusă în aplicare cu strictețe de către Europol[40].

Europol a raportat că schimbul de informații cu **părțile private** era încă neglijabil în 2023, având în vedere că fuseseră înregistrate doar 26 cazuri de punere în aplicare a articolului 26 din RE (pe lângă cazurile care intră sub incidența Regulamentului privind serviciile digitale)[41]. Cu toate acestea, în **2024**, statisticile au arătat o **creștere bruscă, ajungând la 284** de cazuri (o creștere de aproape 1 000%) care implicau cooperarea cu părți private în temeiul articolului 26 din RE. Acest lucru a fost valabil în special în cazul datelor provenite de la societăți private pentru investigarea **infracțiunilor financiare și economice**. De asemenea, Europol a utilizat în mod semnificativ articolul 26b din RE în lupta împotriva exploatării sexuale a copiilor (CSE), domeniu în care cooperarea cu părțile private era deja substanțială înainte. În ambele cazuri, datele includ, de asemenea, cooperarea care a fost posibilă în temeiul cadrului juridic anterior. Datele disponibile nu arată în ce măsură aceste noi cazuri se datorează noilor dispoziții sau unei utilizări sporite a posibilităților existente.

În **2025**, Europol a adoptat o **nouă strategie** pentru a consolida în continuare cooperarea cu părțile private. În plus, s-au luat măsuri de modernizare a infrastructurii TIC a Europol aflate la dispoziția autorităților competente pentru schimbul de informații cu părțile private. În **2023**, Europol a lansat *Plateforme Européenne de Retraits de Contenus illégaux sur Internet* (Platforma europeană pentru eliminarea conținutului ilegal online, **PERCI**) pentru a facilita punerea în aplicare a Regulamentului privind conținutul online cu caracter terorist și, în viitor, a articolului 18 din Regulamentul privind serviciile digitale (DSA), precum și a *Serviciului UE de semnalare a abuzurilor asupra copiilor* **(EU CARES)**. PERCI nu este încorporat în sistemul informațional Europol (SIE)[42].

**Alte dispoziții nu au fost utilizate** deloc (articolul 26a din RE), deși erau operaționale, **sau** au fost aplicate **doar în mod excepțional** [un caz în care articolul 18a din RE a fost utilizat în 2024 și un proiect realizat prin prelucrarea datelor cu caracter personal în temeiul articolului 18 alineatul (1) litera (t) din RE în 2025, trei noi proiecte fiind deja în pregătire].

Din cauza perioadei limitate de punere în aplicare operațională a dispozițiilor introduse prin Regulamentul (UE) 2022/991 și dat fiind că anchetele penale și al procedurile judiciare durează mult, statele membre nu au fost în măsură să furnizeze date cantitative cu privire la impactul acestor dispoziții în termeni operaționali. În schimb, acestea au oferit câteva exemple de

---

39 Astfel cum a subliniat un stat membru în cursul consultării, „[statele membre] pot să distingă în mod clar tipul de date cu care au de a face, ceea ce poate fi foarte important în cadrul anchetei în sine”.

40 A se vedea subsecțiunea 7.1.3. din documentul de lucru al serviciilor Comisiei care însoțește prezentul raport și răspunsurile statelor membre la întrebarea 9 din chestionarul scurt din data de 2 iunie 2025, din Anexa III a documentului de lucru.

41 Europol, Raportul din 2023 în temeiul articolului 16 alineatul (11) din RE.

42 Regulamentul (UE) 2019/818; JO L 135, 22.5.2019, p. 85, ELI: https://eur-lex.europa.eu/eli/reg/2019/818/oj?eliuri=eli%3Areg%3A2016%3A794%3Aoj&locale=ro.

investigații de succes care demonstrează **beneficiile tangibile ale noilor posibilități de investigare în situații reale** pentru dispozițiile deja utilizate, precum EncroChat, Sky ECC, rețelele infracționale din zona balcanică implicate în traficul de cocaină, sau Lumma Stealer.

Europol și opt state membre au semnalat, de asemenea, câteva **domenii în care sunt necesare îmbunătățiri** pentru a maximiza utilizarea eficientă și coerentă a noului cadru juridic și pentru a consolida rolul Europol în viitor. Există preocupări, în special din partea Europol, cu privire la faptul că, din cauza fragmentării, a complexității excesive și a dimensiunii dispozițiilor legale, practicienii sau părțile private pot fi demotivați în privința utilizării noilor instrumente disponibile. Observațiile statelor membre se referă mai degrabă la modul în care Europol pune în aplicare în mod restrictiv garanțiile privind protecția datelor sub supravegherea AEPD, ceea ce riscă să submineze eficacitatea și potențialul anumitor dispoziții.

### *3.3. Evaluarea impactului noilor competențe și sarcini ale Europol în materie de prelucrare a datelor cu caracter personal asupra drepturilor fundamentale*

Comisia **nu** a găsit **nicio** dovadă a unui **impact negativ asupra drepturilor fundamentale** care să rezulte din utilizarea operațională a noilor competențe de prelucrare a datelor cu caracter personal ca urmare a utilizării limitate, până în prezent, a noilor competențe de prelucrare a datelor cu caracter personal.

Pe lângă punerea în aplicare a cerințelor specifice în materie de protecție a datelor asociate noilor competențe din acest domeniu, Europol a luat treptat toate măsurile necesare pentru a pune în aplicare noile mecanisme orizontale de supraveghere legate de drepturile fundamentale.

În 2024, Consiliul de administrație al Europol a adoptat normele revizuite de punere în aplicare a RPD, acesta fiind unul dintre ultimele acte de punere în aplicare necesare legate de noul regim de protecție a datelor. Dovezile colectate sugerează că Europol și Consiliul său de administrație au asigurat, de asemenea, în cooperare cu responsabilul cu protecția datelor din cadrul Europol și cu AEPD, o **implementare riguroasă a noilor garanții în materie de protecție a datelor** introduse în 2022. Această abordare a prevenit în mod eficace, la prima vedere, orice impact negativ sau ingerință în drepturile persoanelor la viață privată și la protecția datelor cu caracter personal de la prima utilizare a noilor competențe de prelucrare a datelor cu caracter personal. Potrivit statelor membre, Europol dispune în prezent de un **cadru juridic solid în materie de protecție a datelor**, care asigură garanții suficiente pentru potențiala utilizare sporită a noilor sale competențe. Șapte state membre au subliniat, de asemenea, că acest cadru **facilitează fluxul de informații** prin consolidarea încrederii, deși se mai pot aduce îmbunătățiri. Un singur stat membru a exprimat o opinie negativă[43].

Pe lângă **provocările** specifice legate de DSC, Europol și patru state membre au menționat că este loc de îmbunătățire în ceea ce privește costurile și timpul asociate **evaluării impactului asupra protecției datelor** (EIPD) și **consultării prealabile** a AEPD, care sunt efectuate, în practică, în mod implicit. O altă provocare semnalată de șase state membre se referă la gestionarea de către Europol a **cererilor de exercitare a dreptului de acces de către persoanele vizate**, pentru care acum este competent chiar și atunci când un stat membru este proprietarul datelor.

**Primul ofițer pentru drepturile fundamentale** a fost numit în decembrie **2022**. În primii doi ani ai mandatului său, acesta **nu** a primit și nici nu a prezentat **nicio plângere** directorului executiv. JPSG a continuat să monitorizeze îndeaproape activitățile Europol și nu a emis nicio

[43] A se vedea răspunsurile statelor membre la întrebarea 9 din chestionarul scurt din 2 iunie 2025, în anexa III la documentul de lucru însoțitor al serviciilor Comisiei.

recomandare de la intrarea în vigoare a noilor dispoziții. Parlamentul European a înființat **Forumul consultativ al JPSG privind drepturile fundamentale** în februarie **2024**.

### *3.4. Analiza cost-beneficiu a noilor competențe și sarcini ale Europol în materie de prelucrare a datelor cu caracter personal*

Având în vedere stadiul incipient al punerii în aplicare a dispozițiilor introduse prin Regulamentul (UE) 2022/991 și experiența limitată cu acestea, este **prematur** pentru Comisie să tragă concluzii semnificative cu privire la noile dispoziții în urma unei **analize cost-beneficiu**.

Serviciile Comisiei au colectat informații de la Europol cu privire la costurile suportate până în prezent în legătură cu punerea în aplicare operațională a Regulamentului (UE) 2022/991, pentru dispozițiile examinate. Aceste costuri s-au ridicat la aproximativ **25 de milioane EUR** (aproximativ 5% din suma totală alocată Europol[44]) în perioada 2022-2025, incluzând în principal costuri unice. Până în prezent, statele membre nu au suportat noi costuri relevante legate în mod specific de Regulamentul (UE) 2022/991.

**Majoritatea costurilor** (aproape 17 milioane EUR) au constat în investiții semnificative în **dezvoltarea de noi structuri TIC**, în dispoziții de punere în aplicare privind cercetarea și inovarea (spațiul de testare ODIN) și în sisteme de informații pentru schimbul de date cu caracter personal cu părți private (PERCI și EU CARES). Costurile cu **resursele umane (RU)**, legate atât de TIC, cât și de operațiuni, au reprezentat aproximativ o treime din cheltuielile totale (aproximativ 8 milioane EUR). Pe termen lung, **principalele costuri recurente** vor fi cele în domeniul resurselor umane.

Trebuie remarcat faptul că cele 8 milioane EUR menționate mai sus nu includ costurile de resurse umane pentru Unitatea de gestionare a informațiilor (IMU) sau resursele asociate măsurilor de supraveghere (anterioare și noi) care au un caracter orizontal și pentru care nu este posibilă o defalcare la nivelul punerii în aplicare a unor dispoziții specifice. Costurile aferente acestor resurse nu sunt neglijabile. De exemplu, în 2023, s-a estimat că **60 de echivalente normă întreagă (ENI)** (aproape 5 % din personalul Europol) participau la activități în cadrul organismelor de **asigurare/supraveghere și al entităților de supraveghere/consiliere**. Europol a alocat 25 ENI eforturilor de a răspunde la supravegherea protecției datelor și la acțiunile de asigurare corespunzătoare. Este vorba despre monitorizarea recomandărilor AEPD, precum și despre activitatea generată în contextul consultărilor prealabile pentru prelucrarea operațională a datelor. Șaisprezece dintre acești 25 ENI sunt implicați în mod specific în activități legate de cerințele AEPD. Începând din iunie 2025, Europol dispune de o echipă specializată formată din opt membri cu normă întreagă în domeniul protecției datelor, inclusiv RPD.

Potrivit Europol și unui număr de cincisprezece state membre, se preconizează că **beneficiile** noilor competențe și sarcini de prelucrare a datelor cu caracter personal, în special cu privire la analizarea seturilor de date complexe și mari, și la cooperarea cu părțile private, vor fi semnificative și vor **depăși costurile asociate**. Niciun stat membru nu a avut o opinie diferită. Pe termen lung, se preconizează în mod rezonabil o serie de câștiguri în materie de eficiență, datorită efectului economiilor de scară și scăderii costurilor marginale. Unul dintre statele membre a subliniat că „este important ca Europol să furnizeze resursele TIC necesare pentru a furniza și a dezvolta în continuare instrumentele necesare pentru punerea în aplicare a noilor

[44] În aceeași perioadă, bugetul alocat Europol s-a ridicat la un total de aproximativ **860 de milioane EUR** (crescând progresiv de la 192de milioane EUR în 2022 la 241 de milioane EUR în 2025). Pentru mai multe detalii, a se consulta documentul de lucru al serviciilor Comisiei.

posibilități prevăzute de Regulamentul (UE) 2022/991", care a fost sprijinit, de asemenea, de alte două state membre și de alte părți interesate[45].

În opinia Europol și a cinci state membre, posibilele **ineficiențe** în materie de punere în aplicare trebuie, de asemenea, să fie abordate în cadrul **existent de guvernanță, administrare și protecție a datelor**, pentru a se evita subminarea impactului operațional al noilor sarcini de prelucrare a datelor cu caracter personal prin amânarea sau restricționarea utilizării acestora. Cinci state membre au pus sub semnul întrebării punerea în aplicare prea prudentă a normelor de protecție a datelor de către Europol și Consiliul său de administrație, sub îndrumarea AEPD. Acestea sugerează că flexibilitatea acordată de colegiuitori ar trebui utilizată în mod adecvat pentru a maximiza eficacitatea și eficiența sarcinilor Europol și pentru a asigura relevanța și rentabilitatea pe termen lung a acestora.

O evaluare a metodelor de lucru ale Europol și a domeniilor potențiale de simplificare nu intră în domeniul de aplicare al raportului în temeiul articolului 68 alineatul (3) din RE și va fi efectuată în cadrul evaluării în temeiul articolului 68 alineatul (1) din RE.

## 4. Concluzii și perspective

În concluzie, principalele constatări preliminare ale Comisiei sunt că statele membre își mențin **sprijinul pentru rolul pe care îl joacă Europol** în domeniile-cheie în care acesta asistă în prezent statele membre prin prisma **noilor sale sarcini de prelucrare a datelor cu caracter personal**. Cu toate acestea, pentru a **maximiza beneficiile** noilor competențe de prelucrare a datelor cu caracter personal, în opinia unor părți interesate, este necesar să se **abordeze posibilele ineficiențe**, în special în cadrul existent de guvernanță, administrare și protecție a datelor. De asemenea, ar fi util să se găsească modalități de atenuare a **complexității și a fragmentării** cadrului juridic care ar putea descuraja practicienii să utilizeze noile posibilități.

În general, Comisia nu a găsit elemente care să indice faptul că noile norme au avut un **impact negativ asupra drepturilor fundamentale**, în special datorită unor garanții solide în materie de protecție a datelor, care să faciliteze, de asemenea, fluxul de informații prin creșterea încrederii partenerilor. Pentru unele state membre, agenția a pus pe primul loc o abordare conservatoare, deși **ar trebui să se prioritizeze în mod adecvat flexibilitatea acordată de colegiuitori** în ceea ce privește clasificarea persoanelor vizate, evaluarea impactului asupra protecției datelor, consultarea prealabilă cu Autoritatea Europol pentru protecția datelor, gestionarea cererilor privind drepturile de acces.

Având în vedere perioada limitată de punere în aplicare a noilor norme privind protecția datelor cu caracter personal prevăzute în Regulamentul (UE) 2022/991, dovezile colectate nu sunt însă concludente cu privire la toate întrebările.

În Strategia europeană de securitate internă, **ProtectEU**[46], Comisia a anunțat că va propune o revizuire ambițioasă a mandatului Europol pentru a aborda provocările tot mai mari în materie de securitate. În conformitate cu Orientările sale privind o mai bună legiferare[47], Comisia a lansat pregătiri pentru evaluarea Regulamentului privind Europol și a metodelor de lucru ale Europol, deschizând calea pentru o **propunere a Comisiei în 2026 pentru ca agenția să**

---

45 A se vedea dovezile prezentate în secțiunea 5 din documentul de lucru al serviciilor Comisiei care însoțește prezentul raport și, în special, observațiile Europol și răspunsurile statelor membre la întrebările 2, 4 și 5 din chestionarul scurt din 2 iunie 2025, din anexa III la documentul de lucru al serviciilor Comisiei și Declarația comună a șefilor de poliție europeni privind viitorul Europol.

46 ProtectEU: o strategie europeană de securitate internă, p. 10.

47 A se vedeahttps://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en?prefLang=ro.

**devină mai operațională, astfel cum se prevede în orientările politice**[48]. În iulie 2025, Comisia a publicat cererea de contribuții[49] și a contractat un studiu extern pentru a sprijini evaluarea Regulamentului privind Europol și evaluarea impactului pentru noua propunere. Evaluarea Regulamentului privind Europol efectuată în scopul pregătirii prezentului raport este menită să contribuie la evaluarea respectivă.

[48] Ursula von der Leyen, Orientările politice pentru următoarea Comisie Europeană 2024-2029, e6cd4328-673c-4e7a-8683-f63ffb2cf648_en

[49] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Cooperarea-in-materie-de-aplicare-a-legii-un-nou-regulament-privind-Europol-propunere-_ro