COMISIA
EUROPEANĂ

Bruxelles, 24.6.2025
COM(2025) 349 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU, COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN ȘI COMITETUL REGIUNILOR

Foaie de parcurs privind accesul legal și efectiv la date pentru autoritățile de aplicare a legii

Introducere

Astfel cum se prevede în Strategia europeană de securitate internă („ProtectEU”)[1], **securitatea reprezintă piatra de temelie a tuturor libertăților noastre**. Democrația, statul de drept, drepturile fundamentale, bunăstarea europenilor, competitivitatea și prosperitatea – toate acestea depind de capacitatea noastră de a oferi o garanție de securitate de bază.

Uniunea Europeană și statele membre au datoria de a se asigura că cetățenii se pot bucura de un **nivel ridicat de securitate în viața lor de zi cu zi**. În acest scop, autoritățile de aplicare a legii și autoritățile judiciare trebuie să dispună de instrumentele necesare pentru a urmări activitățile ilicite, a identifica autorii, a dezmembra rețelele infracționale și a proteja victimele, asigurând, în cele din urmă, justiția penală, cu respectarea deplină a drepturilor fundamentale.

Terorismul, criminalitatea organizată, frauda online, traficul de droguri, abuzul sexual asupra minorilor, extorcarea sexuală online, programele de tip ransomware și multe alte infracțiuni au ceva în comun: lasă **urme digitale**. Astfel cum observă Europol în Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată (SOCTA) pentru 2025, aproape toate formele grave de criminalitate și criminalitatea organizată au o amprentă digitală[2]. **În prezent, în aproximativ 85 % din anchetele penale se recurge la probe electronice**[3]. Cererile de date adresate furnizorilor de servicii s-au triplat între anii 2017 și 2022, iar necesitatea acestor date este în continuă creștere[4].

Deși recent am văzut exemple remarcabile de autorități de aplicare a legii și autorități judiciare care au reușit să ia măsuri drastice împotriva rețelelor specifice de comunicații utilizate de grupurile infracționale[5], mult mai multe anchete **întârzie sau eșuează din cauza lipsei accesului în timp util la probele digitale**[6]**.** Autoritățile de aplicare a legii și autoritățile judiciare au pierdut teren în fața infractorilor în ultimul deceniu, deoarece infractorii utilizează instrumente și produse oferite de furnizori de servicii care au luat măsuri de prevenire a cooperării în legătură cu solicitări legitime[7].

Probele penale critice rămân inaccesibile deoarece[8]:

---

[1] EUR-Lex - 52025DC0148 - RO - EUR-Lex.

[2] European Union Serious and Organised Crime Threat Assessment 2025 („Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în Uniunea Europeană 2025”) EU-SOCTA-2025.pdf.

[3] Evaluarea de impact a Comisiei referitoare la propunerile de regulament și de directivă privind probele electronice (17 aprilie 2018) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:RO:PDF.

[4] Raportul SIRIUS din 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.

[5] *Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized* („Dezmembrarea rețelei EncroChat de comunicații criptate utilizată de grupurile infracționale duce la arestarea a peste 6 500 de persoane și la confiscarea unei sume de aproximativ 900 de milioane EUR”) |. Europol joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf / *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe* („Dezmembrarea unei rețele criptate transmite unde de șoc printre grupurile infracționale organizate din întreaga Europă”) |. Europol.

[6] Conform celor raportate de Grupul la nivel înalt (HLG) privind accesul la date pentru asigurarea eficace a respectării legii – Comisia Europeană.

[7] *Concluding report of the High-Level Group on access to data for effective law enforcement* („Raportul final al Grupului la nivel înalt privind accesul la date pentru asigurarea eficace a respectării legii”) (15 noiembrie 2024).

[8] *Common Challenges in Cybercrime* („Provocări comune în materie de criminalitate informatică”), Analiză din 2024 efectuată de Europol și Eurojust.

- **sunt șterse** de către furnizorii de servicii în termen de câteva zile, în concordanță cu obligațiile care le revin în ceea ce privește protecția datelor cu caracter personal și a vieții private sau cu nevoile lor comerciale;
- **nu pot fi obținute** din cauza conflictelor de legi dintre jurisdicții, deoarece fiecare țară are legi și reglementări diferite în ceea ce privește accesul la date, ceea ce face dificilă obținerea datelor stocate în străinătate;
- **nu pot fi extrase de pe dispozitivele confiscate în cadrul anchetelor penale,** deoarece efectuarea **expertizei criminalistice digitale** este dificilă, dacă nu chiar imposibilă;
- **nu pot fi citite** deoarece datele sunt criptate;
- **nu pot fi analizate în mod eficace și legal** din cauza lipsei de tehnologii adecvate sau de resurse umane suficiente pentru a filtra și a analiza în mod eficace cantități mari de date confiscate, fără a aduce atingere cadrelor juridice ale UE și ale statelor membre.

Pentru a răspunde acestor provocări, în 2023 a fost înființat un **Grup la nivel înalt privind accesul la date pentru asigurarea respectării legii** (Grupul la nivel înalt), care a prezentat un set de 42 de recomandări în mai și noiembrie 2024. **Consiliul Justiție și Afaceri Interne al UE** a aprobat recomandările Grupului la nivel înalt[9] la 13 iunie 2024 și, ulterior, în decembrie 2024, a adoptat concluzii prin care invită Comisia să elaboreze o foaie de parcurs. Foaia de parcurs urma să se bazeze pe activitatea Grupului la nivel înalt și pe recomandările acestuia în ceea ce privește punerea în aplicare a unor măsuri care să asigure accesul legal și efectiv la date pentru asigurarea respectării legii[10]. Prezenta comunicare răspunde acestei solicitări.

Pe măsură ce digitalizarea devine din ce în ce mai răspândită și le oferă infractorilor o sursă tot mai mare de noi instrumente, este esențial să existe un cadru pentru **accesul legal la date** cu scopul de a se asigura că infractorii sunt aduși în fața justiției. „Accesul legal” la care se referă prezenta foaie de parcurs reprezintă accesul, în conformitate cu legea, la informațiile digitale de care autoritățile de aplicare a legii au nevoie în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.

Pentru a fi legal, accesul la date trebuie să fie **necesar și proporțional și să respecte drepturile fundamentale**, asigurând protecția adecvată a vieții private și a datelor cu caracter personal. Accesul trebuie să se bazeze pe norme **clare, precise și accesibile, prevăzute de lege**, să fie supus unor **mecanisme independente de supraveghere** și să permită **căi de atac eficace** pentru persoanele care pot fi afectate de accesul la datele lor. Asigurarea **securității cibernetice** a sistemelor digitale împotriva accesului neautorizat este, de asemenea, importantă pentru protecția împotriva amenințărilor la adresa securității cibernetice.

I. <u>Asigurarea disponibilității probelor digitale: păstrarea datelor</u>[11]

În Spania, o anchetă penală privind dispariția unei tinere a fost soluționată în 2019 datorită datelor de localizare stocate de un furnizor de servicii de comunicații în concordanță cu o

[9] *Recommendations of the High-Level Group on access to data for effective law enforcement* („Recomandările Grupului la nivel înalt privind accesul la date pentru asigurarea eficace a respectării legii”).

[10] Concluziile Consiliului privind accesul la date pentru asigurarea eficace a respectării legii (12 decembrie 2024), https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/ro/pdf; Concluziile Consiliului privind viitoarele priorități pentru consolidarea eforturilor comune de combatere a terorismului ale Uniunii Europene și ale statelor sale membre (12 decembrie 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/ro/pdf.

[11] Păstrarea datelor se referă la furnizorii de servicii care păstrează anumite date care nu se referă la conținut și care sunt prelucrate în contextul serviciilor de comunicații pe care le furnizează pentru o anumită perioadă, cu

obligație legală la nivel național. Aceste date au permis anchetatorilor să localizeze femeia dispărută, să stabilească faptul că suspectul de răpire se afla, de asemenea, în zona respectivă și să excludă alți suspecți[12]. Datele de comunicații care nu se referă la conținut (de exemplu, informațiile privind abonații, datele de localizare și data, ora, durata, expeditorul și destinatarul, precum și dimensiunea comunicării) sunt esențiale în majoritatea anchetelor și urmăririlor penale. Aceste date pot fi decisive pentru identificarea și localizarea victimelor, a persoanelor suspectate și acuzate, făcând lumină în privința unei infracțiuni săvârșite și contribuind inclusiv la excluderea suspecților.

În concordanță cu legislația UE privind protecția vieții private și a datelor, furnizorii de servicii de comunicații electronice pot stoca date de comunicații care nu se referă la conținut și care trec prin sistemele lor numai atât timp cât acest lucru este necesar în scopuri profesionale specificate, explicite și legitime. Totuși, obligațiile legale le pot impune să păstreze (sau „să stocheze") aceste date în alte scopuri, de exemplu dacă sunt necesare pentru prevenirea, investigarea, depistarea și urmărirea penală a infracțiunilor.

Întrucât Directiva UE privind păstrarea datelor[13] a fost invalidată în 2014[14], peisajul legislativ al UE în ceea ce privește obligarea furnizorilor de servicii să stocheze date a devenit fragmentat și inegal. Cadrele de păstrare a datelor din statele membre diferă în ceea ce privește tipurile de comunicații electronice pe care furnizorii de servicii trebuie să le păstreze, categoriile de date vizate și perioadele de păstrare necesare[15]. În plus, unele state membre nu au nicio legislație privind păstrarea datelor. Autoritățile de aplicare a legii și autoritățile judiciare se confruntă cu obstacole juridice și operaționale în calea desfășurării activității lor. Furnizorii de comunicații electronice, în special furnizorii mai mici, se confruntă, de asemenea, cu costuri și obstacole suplimentare atunci când își furnizează serviciile în întreaga UE, deoarece sunt obligați să respecte cerințe legale diferite de la un stat membru la altul.

Prin urmare, Grupul la nivel înalt a recomandat instituirea **unui cadru armonizat la nivelul UE privind păstrarea datelor** în vederea asigurării disponibilității probelor digitale necesare pentru investigarea și urmărirea penală a infracțiunilor. Un regim armonizat la nivelul UE ar viza limitarea fragmentării între statele membre în ceea ce privește normele privind păstrarea și garanțiile referitoare la drepturile fundamentale, în special dreptul la viață privată și la protecția datelor, precum și dreptul la apărare, inclusiv dreptul la un proces echitabil. Un astfel de cadru juridic ar asigura astfel și securitatea juridică pentru autoritățile competente, pe de o parte, și pentru furnizorii de servicii, pe de altă parte[16].

---

scopul de a permite accesul autorităților competente în cadrul anchetelor penale în temeiul unor garanții adecvate și de a asigura justiția penală.

[12] *La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina* |. *España*.

[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.

[14] Hotărârea Curții (Marea Cameră) din 8 aprilie 2014. Digital Rights Ireland Ltd împotriva Minister for Communications, Marine and Natural Resources și alții.

[15] Pentru o prezentare generală, a se vedea *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU* („Efectul jurisprudenței Curții de Justiție a Uniunii Europene asupra regimurilor naționale de păstrare a datelor și asupra cooperării judiciare în UE") |. Eurojust |. Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală și *European Commission Study on the retention of electronic communications non-content data for law enforcement purposes* („Studiul Comisiei Europene privind păstrarea datelor care nu se referă la conținut din comunicațiile electronice în scopul asigurării respectării legii").

[16] Grupul de recomandări 6, Raportul final al Grupului la nivel înalt.

Acțiune-cheie

- **În 2025, Comisia va elabora o evaluare a impactului în vederea actualizării normelor UE privind păstrarea datelor, după caz.**

Grupul la nivel înalt a identificat necesitatea de a **consolida sinergiile dintre practicienii din domeniul aplicării legii și furnizorii de servicii**[17].

În acest scop, **Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust)** sunt invitate să își continue și să își extindă eforturile **pentru a facilita cooperarea și schimbul de informații și de bune practici dintre practicieni și furnizorii de servicii** prin intermediul **proiectului SIRIUS**[18], cu sprijinul continuu al Comisiei. Proiectul SIRIUS a devenit cea mai importantă sursă de informații **pentru sprijinirea practicienilor din domeniul aplicării legii și a autorităților judiciare din UE și din afara acesteia în ceea ce privește accesarea probelor electronice stocate de furnizorii de servicii online** cu sediul în țări terțe. Platforma SIRIUS are peste 8 000 de membri din comunitățile de aplicare a legii și judiciare, reprezentând 47 de țări din întreaga lume, și a sprijinit în mod direct aproape 70 de operațiuni polițienești.

În același scop, Europol și Eurojust ar trebui să utilizeze proiectul SIRIUS pentru a elabora, în cooperare cu **sectorul privat, un catalog de date pe care serviciile de comunicații electronice le prelucrează în mod legitim în scopuri profesionale**. Catalogul va ajuta autoritățile competente să identifice datele care pot fi disponibile pentru cererile lor de acces legal, să identifice furnizorii de servicii relevanți și să direcționeze mai bine cererile de acces legal, economisind astfel timp și costuri atât pentru autoritățile publice, cât și pentru furnizorii de servicii.

Acțiuni-cheie

- **Cu sprijinul continuu al Comisiei, Europol și Eurojust sunt invitate să se bazeze pe proiectul SIRIUS pentru a raționaliza cooperarea cu furnizorii de servicii de comunicații electronice.**

- **Europol și Eurojust sunt invitate să elaboreze, în cooperare cu sectorul privat, un catalog al datelor pe care furnizorii de comunicații electronice le prelucrează în scopuri profesionale (începând cu T4 2025).**

II. Obținerea de probe în toate sistemele și jurisdicțiile: interceptarea legală

Accesul legal la datele comunicațiilor în timp real este esențial pentru combaterea infracționalității online și offline. În 2020, o echipă comună de anchetă franco-neerlandeză a desființat EncroChat, o rețea de telefonie criptată, utilizată pe scară largă de grupurile infracționale organizate. Această anchetă comună a implicat interceptarea, în timp real, a milioane de mesaje între infractorii care intenționau să săvârșească infracțiuni grave, partajarea acestor mesaje cu alte autorități și analizarea lor. Datorită informațiilor obținute, autoritățile de aplicare a legii din întreaga Europă și din alte părți ale lumii au perturbat activitățile infracționale, printre care atacuri violente, corupție, tentative de omor și trafic de droguri pe

[17] Grupul de recomandări 5, Raportul final al Grupului la nivel înalt.
[18] Proiectul SIRIUS | Europol.

scară largă. Anumite mesaje au indicat planuri de săvârșire a unor infracțiuni violente iminente și au permis autorităților de aplicare a legii să le prevină[19]. Ordinul european de anchetă (OEA) a facilitat schimbul eficient de astfel de probe[20].

Cazul EncroChat demonstrează că accesul în timp real la datele referitoare la conținutul comunicațiilor constituie un instrument esențial pentru investigarea și urmărirea penală eficace a grupurilor infracționale organizate. Totuși, acest caz rămâne una dintre puținele povești de succes: Grupul la nivel înalt a remarcat că eficacitatea interceptării legale[21] a scăzut drastic, deoarece comunicarea a trecut de la apelurile telefonice și mesajele text clasice la serviciile de mesagerie „over the top” (OTT) furnizate prin intermediul aplicațiilor. În prezent, aproximativ 97 % din toate mesajele mobile sunt trimise prin intermediul aplicațiilor de mesagerie, în timp ce mesajele text și MMS clasice reprezintă doar aproximativ 3 % din mesaje[22]. Grupul la nivel înalt a remarcat, de asemenea, că, începând din 2020, în urma perturbării unora dintre principalele rețele de comunicații utilizate de grupurile infracționale, multe dintre acestea au decis să revină la servicii regulate de mesagerie OTT, criptate de la un capăt la altul[23].

Normele naționale care impun obligații pentru interceptarea legală sunt fragmentate în UE[24]. Grupul la nivel înalt a remarcat că, deși unele state membre impun obligații similare pentru toate tipurile de servicii de comunicații electronice, inclusiv pentru cele OTT, unele state membre exclud serviciile OTT. În plus, adesea, furnizorii de servicii nu sunt stabiliți în statul membru al autorității solicitante, ceea ce poate cauza probleme complexe de jurisdicție, conflicte de legi și provocări în materie de asigurare a respectării legii[25]. Prin urmare, conținutul unor astfel de servicii de mesagerie este practic inaccesibil.

Ordinul european de anchetă și alte instrumente de cooperare pot contribui la depășirea provocării generate de interceptarea transfrontalieră în anumite părți ale UE. Totuși, autoritățile statelor membre se confruntă în continuare cu dificultăți atunci când le utilizează: aceste instrumente nu pot sprijini interceptarea în cazul în care serviciul este furnizat fie din state membre care nu participă la instrumentul în cauză, fie dintr-o țară terță. Prin urmare, Grupul la nivel înalt a recomandat o serie de măsuri pentru a se asigura că o gamă largă de furnizori, inclusiv furnizorii OTT, răspund la cererile de interceptare legală[26].

În replică, **Comisia va propune modalități de îmbunătățire a măsurilor de consolidare a cooperării transfrontaliere în materie de interceptare** atât între autorități, cât și între autorități și furnizorii de servicii. În urma recomandărilor Grupului la nivel înalt, Comisia se

[19] *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe* („Dezmembrarea unei rețele criptate transmite unde de șoc printre grupurile infracționale organizate din întreaga Europă”) |. Europol; *Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée*.

[20] Ordinul european de anchetă | Eurojust | Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală.

[21] În contextul prezentei comunicări, tehnologiile de interceptare legală care sunt puse în aplicare de către un operator de comunicații pentru a obține acces în timp real la datele comunicațiilor în cadrul anchetelor judiciare, precum și tehnologiile care pot fi implementate în mod autonom de către autoritățile de aplicare a legii.

[22] Raportul final al Grupului la nivel înalt, p. 38.

[23] *Internet Organised Crime Threat Assessment* („Evaluarea amenințării pe care o reprezintă criminalitatea organizată online”) (IOCTA), 2024.

[24] A se vedea Cartea albă a UE privind infrastructura digitală, p. 14; Raportul Letta privind piața internă, p. 59, și Raportul Draghi privind competitivitatea UE, p. 70, 74, 76.

[25] Raportul final al Grupului la nivel înalt, p. 41.

[26] Grupul de recomandări 8, Raportul final al Grupului la nivel înalt.

va concentra în primul rând pe îmbunătățirea instrumentelor existente, în special a ordinului european de anchetă, și pe cooperarea voluntară (în cazul în care nu există conflicte de legi cu țări terțe sau acestea au fost soluționate). În cele din urmă, statele membre ar trebui să poată impune obligații legale de interceptare tuturor furnizorilor de comunicații care propun servicii la nivel național, astfel cum se prevede în legislația națională, indiferent dacă sunt servicii de telecomunicații clasice sau bazate pe internet și indiferent de locul în care se află.

În plus, unele state membre nu dispun de capacitățile de rețea necesare pentru schimbul de date în cadrul cooperării transfrontaliere. Prin urmare, **Comisia va identifica nevoile statelor membre** și va sprijini instalarea de rețele securizate cu o lățime de bandă suficientă între statele membre relevante, care să permită transferul unor cantități mari de date în timp real. Această inițiativă ar putea fi finanțată din programele UE.

Acțiuni-cheie

Comisia urmează:

- **să propună măsuri de îmbunătățire a eficienței cererilor transfrontaliere de interceptare legală prin intermediul instrumentelor existente, inclusiv evaluarea necesității de a consolida în continuare ordinul european de anchetă (până în 2027);**

- **să analizeze măsuri de creare a unor condiții de concurență echitabile pentru toate tipurile de furnizori de comunicații în ceea ce privește asigurarea respectării obligațiilor de interceptare legală;**

- **să stabilească cea mai eficientă abordare pentru a soluționa problema furnizorilor de comunicații necooperanți;**

- **să sprijine implementarea capacităților securizate de schimb de informații între statele membre, Europol și alte agenții de securitate (în perioada 2026-2028).**

Statele membre sunt încurajate să pună în aplicare măsuri transfrontaliere de interceptare legală, pe baza mecanismelor existente, cum ar fi ordinul european de anchetă și acordurile bilaterale și multilaterale.

III. Recuperarea probelor din dispozitivele confiscate în cadrul anchetelor: criminalistica digitală

Pentru a desfășura anchete penale, autoritățile de aplicare a legii și autoritățile judiciare trebuie să poată accesa, colecta, analiza și păstra probele digitale stocate pe dispozitive electronice. Aceste probe digitale pot, de exemplu, să contribuie la identificarea membrilor grupurilor infracționale organizate sau la excluderea persoanelor ca suspecți[27].

Grupul la nivel înalt a discutat o serie de provocări care împiedică accesul la aceste probe digitale. Autoritățile naționale se confruntă cu o lipsă acută de resurse și capacități pentru desfășurarea activității de criminalistică digitală. Acestea se străduiesc să facă față necesității de a dezvolta în permanență noi competențe și instrumente pentru a ține pasul cu noile tehnologii (de exemplu, noi tipuri de dispozitive și sisteme de operare, internetul obiectelor și

[27] Un caz discutat în cadrul Grupului la nivel înalt se referea la analiza unui dispozitiv care a avut un rol esențial în a dovedi că un suspect nu a fost implicat într-un omor. Raportul final al Grupului la nivel înalt, p. 12.

cloud computing). Cooperarea transfrontalieră dintre statele membre este subminată de lipsa unor capacități comparabile și de absența unor mecanisme de recunoaștere a competențelor și expertizei experților în criminalistică digitală. Soluțiile comerciale existente devin rapid depășite, sunt inaccesibile ca preț și sunt adesea dezvoltate în afara UE. De asemenea, acestea pot fi insuficient adaptate la nevoile autorităților statelor membre sau pot să nu îndeplinească standardele UE privind răspunderea în materie de criminalistică digitală sau alte cerințe legale.

Prin urmare, pentru a consolida capacitatea autorităților europene de aplicare a legii de a efectua expertize criminalistice digitale pe dispozitivele confiscate, Grupul la nivel înalt a recomandat acordarea de finanțare specifică pentru proiecte destinate atât cercetării și dezvoltării de instrumente de criminalistică digitală, cât și adoptării acestora. Grupul la nivel înalt a salutat eforturile în curs ale Comisiei de a sprijini aceste proiecte prin finanțare în cadrul anumitor instrumente ale UE (Orizont Europa, programul Europa digitală și Fondul pentru securitate internă) și al instrumentelor corespunzătoare din cadrul următorului buget pe termen lung al UE (cadrul financiar multianual).

Ca răspuns la aceste recomandări[28], **Comisia, cu sprijinul Europol, va coordona o analiză a lacunelor și a nevoilor în ceea ce privește cercetarea, dezvoltarea, implementarea, întreținerea și adoptarea de soluții tehnice comune pentru criminalistica digitală.**

Utilizarea resurselor trebuie maximizată prin crearea de sinergii între proiectele de criminalistică digitală, inclusiv prin integrarea celor finanțate prin programe ale statelor membre în mecanismele sau rețelele existente. Aceasta ar trebui să includă finanțarea parteneriatelor public-privat pentru a furniza instrumente software pe deplin testate și gata de utilizare, fără costuri de acordare a licențelor[29].

În cadrul mandatului OLAF de a efectua anchete administrative, oficiul a dobândit o experiență semnificativă în materie de procese și instrumente de criminalistică digitală și poate ajuta autoritățile statelor membre să își consolideze capacitățile prin intermediul Programului antifraudă al Uniunii.

Registrul de instrumente al Europol este o platformă online securizată, aflată exclusiv la dispoziția autorităților de aplicare a legii, pentru partajarea gratuită și necomercială a software-ului dezvoltat de Europol, de agențiile europene de aplicare a legii și de mediul academic. Autoritățile naționale de anchetă au utilizat pe scară largă instrumentele registrului pentru a sprijini activitățile desfășurate în domeniul criminalității grave și organizate, care include traficul de persoane, criminalitatea informatică și abuzul sexual online asupra minorilor. Acest registru ar trebui să rămână canalul privilegiat de distribuție pentru instrumentele digitale de anchetă dezvoltate de proiectele UE, precum și de statele membre, care vor fi încurajate să partajeze instrumentele de criminalistică digitală cu sursă deschisă dezvoltate la nivel național în cadrul mecanismelor sau rețelelor existente. **Europol își poate dezvolta și promova în continuare Registrul de instrumente** pentru a pune la dispoziția autorităților de aplicare a

[28] Grupul de recomandări 1, Raportul final al Grupului la nivel înalt.

[29] De exemplu, Asociația Europeană pentru Dezvoltarea Tehnologiei de Combatere a Criminalității Informatice (EACTDA) (www.eactda.eu) furnizează instrumente software pe deplin testate și gata de utilizare, fără costuri de acordare a licențelor, și acces la codul sursă pentru agențiile UE de aplicare a legii. Pe lângă cele opt instrumente finalizate până în prezent, EACTDA dezvoltă încă 16 instrumente digitale de anchetă, care urmează să fie furnizate până la jumătatea anului 2025.

legii din UE instrumente de anchetă de încredere, securizate, gratuite, ușor de instalat și scalabile.

Comisia va **sprijini, de asemenea, adoptarea de soluții inovatoare de către autoritățile de aplicare a legii din statele membre prin intermediul mecanismelor existente, cum ar fi EMPACT**[30]**, și prin cereri de propuneri** specifice în cadrul Fondului pentru securitate internă.

Grupul la nivel înalt a subliniat că **licențele pentru instrumentele de criminalistică digitală** sunt costisitoare și uneori inaccesibile ca preț pentru unele autorități de aplicare a legii. Instrumentele de criminalistică digitală pot furniza date în formate care nu sunt compatibile cu sistemele utilizate pentru prelucrarea ulterioară a datelor. În plus, încrederea este fundamentală pentru activitățile de criminalistică digitală, care nu ar trebui să se bazeze pe instrumente de tip „cutie neagră" (și anume instrumente care prelucrează date fără ca autoritățile de încredere să poată verifica modul în care funcționează). Partajarea instrumentelor de criminalistică digitală ar trebui să fie sprijinită de sisteme de evaluare și, după caz, de certificarea instrumentelor comerciale la nivelul UE, pentru a se asigura că acestea îndeplinesc standardele în materie de credibilitate și de criminalistică fără a impune sarcini nejustificate. Sprijinul ar trebui acordat, de asemenea, prin sisteme comune de achiziții publice, asigurând cooperarea dintre unitățile operaționale și punctele de contact din cadrul autorităților responsabile de achizițiile publice[31].

Prin urmare, **Comisia va sprijini unitățile operaționale ale statelor membre și autoritățile lor responsabile de achiziții publice să instituie achiziții comune de licențe pentru instrumente de criminalistică digitală, începând cu o etapă-pilot.**

Acțiuni-cheie

Comisia, cu sprijinul Europol, urmează:

- **să coordoneze o analiză a lacunelor și a nevoilor în ceea ce privește cercetarea, dezvoltarea, implementarea, întreținerea și adoptarea unor soluții tehnice comune pentru criminalistica digitală înainte de T2-2026;**

- **să sprijine în continuare dezvoltarea de soluții tehnice pentru criminalistica digitală prin mecanisme adecvate de finanțare și de coordonare;**

- **să sprijine statele membre și autoritățile responsabile de achizițiile publice să instituie achiziții comune de licențe pentru instrumente de criminalistică digitală (înainte de T2-2027), începând cu o etapă-pilot.**

Europol este invitată să dezvolte și să promoveze în continuare Registrul său de instrumente pentru a permite accesul autorităților de aplicare a legii la instrumente digitale necomerciale (începând cu T3-2025).

Statele membre sunt invitate să participe, să sprijine și să ghideze dezvoltarea, validarea și adoptarea instrumentelor de criminalistică digitală.

[30] EMPACT (Platforma multidisciplinară europeană împotriva amenințărilor infracționale) este o inițiativă în materie de securitate derulată de statele membre ale UE pentru a identifica, a acorda prioritate și a aborda amenințările reprezentate de criminalitatea internațională organizată și gravă.

[31] Pe baza proiectului iProcureNet (www.iprocurenet.eu/), finanțat în cadrul programului Orizont Europa pentru cercetare și inovare al UE, care a creat o metodologie pentru achizițiile publice comune în domeniul securității, precum și o rețea de autorități responsabile de achizițiile publice din statele membre.

Agenția UE pentru Formare în Materie de Aplicare a Legii (CEPOL) oferă formare anchetatorilor din domeniul criminalisticii digitale, inclusiv în ceea ce privește criminalistica mobilă și criminalistica datelor în timp real. În urma recomandării Grupului la nivel înalt[32], **Comisia ar trebui să sprijine în continuare crearea de materiale și resurse de formare** prin intermediul mecanismelor existente, implicând practicienii și mediul academic[33]. În plus, CEPOL și statele membre ar trebui să **acorde prioritate furnizării de formare în domeniul criminalisticii digitale.**

Grupul la nivel înalt a subliniat, de asemenea, că ar putea fi creat un sistem de certificare la nivelul UE pentru experții în criminalistică digitală. Un astfel de sistem ar asigura calitatea activității de criminalistică digitală, ar contribui la îmbunătățirea transparenței procedurilor judiciare și ar spori încrederea dintre autoritățile de aplicare a legii la nivel transfrontalier.

În concordanță cu recomandările Grupului la nivel înalt[34], CEPOL **ar putea sprijini practicienii și mediul academic, utilizând pe deplin rețelele și mecanismele existente[35], să creeze un sistem de certificare la nivelul UE pentru experții în criminalistică digitală**.

Acțiuni-cheie

<u>Comisia</u> urmează:

- **să sprijine în continuare crearea de materiale și resurse de formare.**

<u>CEPOL și statele membre</u> sunt încurajate:

- **să acorde prioritate furnizării de formare în domeniul criminalisticii digitale (începând cu T3-2025);**
- **să sprijine dezvoltarea și punerea în aplicare a unui sistem de certificare la nivelul UE pentru experții în criminalistică digitală (care urmează să fie elaborat între T1-2026 și T4-2028).**

Grupul la nivel înalt a formulat recomandări privind facilitarea schimbului de soluții și de instrumente de criminalistică digitală între statele membre într-un mediu de încredere[36]. Drept urmare, **<u>Europol ar trebui să își dezvolte în continuare rolul de centru de excelență al UE în materie de asigurare a respectării legii pentru expertiza operațională digitală în domeniul criminalisticii digitale</u>**. Acest demers ar putea include instituirea unui proiect similar SIRIUS[37] pentru a facilita schimbul de cunoștințe, expertiză, soluții tehnice, instrumente de criminalistică digitală și bune practici într-un mediu de încredere. Europol ar trebui, de asemenea, să își intensifice rolul de coordonare în ceea ce privește crearea de cunoștințe în domeniul criminalisticii digitale la nivelul UE, pe baza mecanismelor create în

[32] Grupul de recomandări 3, Raportul final al Grupului la nivel înalt.

[33] De exemplu, Grupul european de formare și educație în combaterea criminalității informatice – ECTEG (www.ecteg.eu) este o asociație care lucrează în strânsă cooperare cu Europol și CEPOL, cu scopul de a furniza resurse gratuite de formare autorităților de aplicare a legii în domeniul anchetelor digitale. În prezent, acesta este finanțat din Fondul pentru securitate internă al UE.

[34] Grupul de recomandări 3, Raportul final al Grupului la nivel înalt.

[35] În special ECTEG.

[36] Grupul de recomandări 1, Raportul final al Grupului la nivel înalt.

[37] Proiectul SIRIUS, condus de Europol și Eurojust, sprijină autoritățile de aplicare a legii și autoritățile judiciare din UE prin facilitarea accesului transfrontalier eficient la probele electronice stocate de furnizorii de servicii online. Proiectul oferă instrumente practice, formare și resurse pentru peste 9 000 de practicieni, încurajează cooperarea dintre furnizorii de servicii online și promovează schimbul de cunoștințe prin intermediul unor evenimente și parteneriate internaționale.

ultimii ani[38]. Europol poate iniția unele dintre aceste acțiuni în cadrul mandatului său actual. Totuși, Europol va avea nevoie de un mandat consolidat și de resurse suplimentare pentru a dezvolta pe deplin aceste acțiuni și pentru a răspunde în mod eficace nevoilor operaționale ale statelor membre.

Ca urmare a angajamentului stabilit în Orientările politice pentru Comisia Europeană 2024 2029 și astfel cum s-a anunțat în Strategia europeană de securitate internă, **Comisia va propune o revizuire ambițioasă a mandatului Europol**. Pentru a pregăti acest lucru, în strânsă cooperare cu statele membre, Comisia va analiza modalitățile de stimulare a expertizei tehnologice și a capacității Europol de a sprijini autoritățile naționale de aplicare a legii în spațiul digital. Consolidarea capacităților Europol în materie de criminalistică digitală, pe baza unui mandat consolidat și cu resurse suplimentare, va fi esențială în acest efort.

Grupul la nivel înalt a recomandat îmbunătățirea accesului la cunoștințe pentru experți prin mecanisme specifice și prin colaborarea experților cu producătorii și dezvoltatorii de instrumente de criminalistică digitală[39]. Începând din 2026, **Europol, utilizând propriile resurse, ar trebui să încurajeze cooperarea dintre autoritățile naționale relevante și experți pentru a facilita cooperarea dintre sectorul public și cel privat în domeniul criminalisticii digitale**. Europol ar trebui să sprijine statele membre să dezvolte instrumente digitale și proceduri comune, care includ stabilirea unor formate de date comune în scopul criminalisticii digitale[40].

Acțiuni-cheie

Europol este invitat:

- **să devină un centru de excelență pentru expertiza operațională în domeniul criminalisticii digitale și să își intensifice rolul în coordonarea creării de cunoștințe în acest domeniu la nivelul UE (începând din 2026);**

- **să faciliteze cooperarea dintre autoritățile de aplicare a legii și părțile private, inclusiv furnizorii de servicii, în ceea ce privește criminalistica digitală și să contribuie la stabilirea unor formate comune de date în scopul criminalisticii digitale (începând din 2026).**

IV. Asigurarea faptului că probele pot fi citite: decriptarea datelor

Criptarea și alte măsuri de securitate cibernetică joacă un rol important în protejarea sistemelor informatice împotriva spionajului și a perturbărilor și în securizarea comunicațiilor, a vieții private și a datelor cu caracter personal. Între 60 % și 80 % din aplicațiile de mesagerie sunt criptate de la un capăt la altul, inclusiv cele oferite de furnizorii principali, cum ar fi WhatsApp,

[38] Comunități specifice de pe Platforma Europol pentru experți (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); Forumul experților criminaliști (https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); Zilele Europol pentru industrie și cercetare) (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Grupul de recomandări 1, Raportul final al Grupului la nivel înalt.

[40] Aceste eforturi ar trebui sprijinite de o sursă de finanțare adecvată din partea UE (programe pentru cercetare sau dezvoltare, în funcție de nivelul de maturitate al sistemelor avute în vedere).

Messenger, Signal și iMessage, în timp ce utilizarea mesajelor text și a apelurilor telefonice clasice înregistrează o scădere drastică la nivel mondial[41].

Grupul la nivel înalt a remarcat că aceste evoluții au un impact asupra capacității autorităților de aplicare a legii și a autorităților judiciare de a colecta probe în cadrul anchetelor și urmăririlor penale, întrucât interceptarea legală a comunicațiilor devine, în mare parte, inutilizabilă. Grupul la nivel înalt a subliniat că statele membre au expertiză și capacități limitate de a decripta datele în repaus, existând diferențe semnificative în ceea ce privește ratele de succes, care variază de la 15-20 % în unele state membre până la peste 66 % în altele.

Echipamentele de decriptare sunt costisitoare și foarte specializate, iar hardware-ul consumă multe resurse. Majoritatea departamentelor de criminalistică digitală din cadrul autorităților de aplicare a legii se bazează pe soluții comerciale pentru a accesa datele de pe dispozitive. Aceste soluții sunt adaptate cu dificultate la evoluțiile tehnologice și devin rapid caduce; costul ridicat al licențelor reduce în mod semnificativ numărul de utilizatori autorizați; iar aceste soluții sunt adesea dezvoltate în afara UE și, prin urmare, este posibil să nu răspundă nevoilor autorităților UE sau să nu îndeplinească standardele în materie de criminalistică digitală. Prin urmare, acestea sunt utilizate cu succes doar într-un număr foarte mic de anchete.

În plus, utilizarea acestor instrumente are și alte dezavantaje. În cadrul anchetelor pe care le efectuează, autoritățile exploatează adesea vulnerabilitățile pentru a obține acces la cheile de decriptare de pe dispozitive, ceea ce, în unele cazuri, ar putea crea o discrepanță în raport cu obiectivul de politică de a asigura securitatea cibernetică în mod implicit. În plus, accesarea datelor criptate devine din ce în ce mai complexă. Grupul la nivel înalt a remarcat că datele stocate pe anumite tipuri de dispozitive moderne, protejate prin cipuri criptografice sau algoritmi puternici de criptare și parole complexe, nu pot fi accesate de autorități, nici măcar utilizând cele mai puternice platforme de decriptare.

Dezvoltarea și introducerea **criptografiei cuantice sigure** reprezintă o necesitate pentru a proteja datele de viitoarele atacuri informatice cuantice care ar face ca tranzacțiile financiare, comunicațiile sensibile și secretele de stat să fie vulnerabile la decriptare și exploatare. Astfel cum se prevede în Recomandarea Comisiei privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către **criptografia post-cuantică (PQC)**[42] și în Strategia europeană de securitate internă (ProtectEU), implementarea soluțiilor PQC și dezvoltarea distribuției cuantice a cheilor vor fi esențiale pentru protejarea datelor în noua eră cuantică. Totuși, după cum a subliniat Europol, acest lucru va îngreuna accesul legal la probele digitale în anii următori, iar agențiile de aplicare a legii trebuie să realizeze investiții pentru a ține pasul cu evoluțiile tehnologice rapide[43].

Grupul la nivel înalt[44] a recomandat elaborarea unei foi de parcurs tehnologice pentru a pune în aplicare accesul legal specific începând cu momentul conceperii, atunci când este cazul, asigurând în același timp o securitate și o securitate cibernetică solide și respectând pe deplin

[41] Procentul menționat se referă la criptarea de la un capăt la altul în timpul transmisiei.

[42] *Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography* („Recomandare privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către criptografia postcuantică”).

[43] *The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement* („A doua revoluție cuantică: impactul informaticii cuantice și al tehnologiilor cuantice asupra asigurării respectării legii”) |. Europol.

[44] Grupul de recomandări 10, Raportul final al Grupului la nivel înalt.

obligațiile legale privind accesul legal. În replică, **Comisia încredințează unui grup de experți sarcina de a oferi sprijin în elaborarea unei foi de parcurs tehnologice privind criptarea.** Grupul va identifica și va evalua soluțiile tehnologice care ar permite autorităților de aplicare a legii să acceseze date criptate în mod legal, protejând în același timp securitatea cibernetică și drepturile fundamentale. Grupul va cuprinde experți în domeniul asigurării respectării legii, al securității cibernetice, al criptării, al tehnologiilor comunicațiilor, al standardizării și al drepturilor fundamentale. Studiile tehnologice și validarea conceptelor vor sprijini această activitate. Scopul acestei activități este de a identifica:

- **instrumentele de care autoritățile de aplicare a legii au nevoie în prezent și vor avea nevoie în viitor** pentru a găsi, a extrage și a analiza în mod legal date criptate; aceste instrumente trebuie să faciliteze activitățile de criminalistică digitală, de decriptare, de colectare de date la distanță și de evaluare a criminalității;
- **tehnologii care asigură faptul că viitoarele tehnologii ale informației și comunicațiilor**, cum ar fi a șasea generație de rețele celulare (6G) și criptarea rezistentă la atacuri cuantice, nu afectează capacitatea autorităților de aplicare a legii de a accesa date în mod legal, asigurând în același timp respectarea drepturilor fundamentale și a securității cibernetice.

În cazul în care nu există instrumente în prezent, se preconizează că foaia de parcurs tehnologică va oferi recomandări cu privire la dezvoltarea acestora și la modalitățile de asigurare a compatibilității cu cadrul juridic al UE și de garantare a securității cibernetice. Rezultatul foii de parcurs tehnologice poate, de asemenea, să stea la baza unor acțiuni specifice de promovare a unei abordări coordonate a standardizării.

Platforma de decriptare a Europol s-a dovedit a fi esențială în sprijinirea cazurilor penale importante, inclusiv a celor rezultate din cazurile Sky ECC[45] și EncroChat. Sunt necesare capacități sporite de decriptare, determinate și de investiții suplimentare în inteligența artificială (IA) și în calculul de înaltă performanță, pentru a se asigura că autoritățile de aplicare a legii au capacitatea de a decripta algoritmi din ce în ce mai complecși.

Grupul la nivel înalt a formulat o recomandare[46] de creștere a finanțării pentru sprijinirea inovării în ceea ce privește accesul la date. În replică, **Comisia va sprijini cercetarea și dezvoltarea de noi capacități de decriptare** pentru a se asigura că Europol este bine dotată după 2030 pentru a sprijini statele membre, având în vedere noile evoluții tehnologice și cele mai avansate activități de cercetare în domeniu. Această inițiativă ar putea implica creșterea finanțării pentru sprijinirea cercetării în domeniul decriptării, precum și dezvoltarea și punerea în aplicare a instrumentelor de către statele membre. Statele membre vor fi implicate îndeaproape pentru a-și împărtăși cerințele specifice, cu scopul de a-și consolida capacitățile, competențele și resursele tehnice, pe baza tehnologiilor concepute la nivelul UE și, eventual, pentru a analiza posibilitatea realizării unor achiziții publice comune.

Acțiuni-cheie

Comisia urmează:

[45] *New major interventions to block encrypted communications of criminal networks* („Noi intervenții majore pentru blocarea comunicațiilor criptate ale rețelelor infracționale") |. Europol.

[46] Grupul de recomandări 10, Raportul final al Grupului la nivel înalt.

- **să elaboreze o foaie de parcurs tehnologică privind criptarea (în T2-2026);**

- **să sprijine cercetarea și dezvoltarea de noi capacități de decriptare pentru a dota Europol cu capacități de decriptare de nouă generație (începând din 2030).**

V. Reconcilierea tehnologiei cu accesul legal: standardizarea

Standardele sunt esențiale în comunicațiile digitale. Dezvoltate de o gamă largă de actori, în principal de către industrie, acestea asigură interoperabilitatea între sistemele și dispozitivele dezvoltate de furnizorii de tehnologie și facilitează respectarea de către tehnologii a obligațiilor legale, inclusiv în ceea ce privește accesul legal în scopul asigurării respectării legii. Institutul European de Standardizare în Telecomunicații (ETSI) a elaborat mai multe standarde în domeniul interceptării legale și al divulgării legale. Există totuși lacune, cum ar fi în cazul celei de a cincea generații de rețele celulare (5G), în care neacordarea unei atenții corespunzătoare accesului legal în momentul dezvoltării rețelei a împiedicat autoritățile de aplicare a legii și autoritățile judiciare să aibă acces la probele necesare pentru a identifica și a aduce infractorii în fața instanței[47].

Grupul la nivel înalt a recomandat adoptarea unei abordări prudente în ceea ce privește conceperea de soluții pentru accesul legal la sisteme, abordare potrivit căreia nu ar trebui să i se solicite industriei integrarea unor sisteme care ar putea slăbi criptarea într-un mod generalizat sau sistemic pentru toți utilizatorii unui serviciu. Accesul legal la date trebuie să rămână specific și limitat la comunicări specifice, de la caz la caz.

În general, soluțiile ar trebui puse în aplicare pe baza unor standarde clare care să fie elaborate cu contribuții din partea tuturor părților interesate, inclusiv a reprezentanților industriei, a experților în protecția datelor, a vieții private și a securității cibernetice, precum și a practicienilor din domeniul aplicării legii. Totuși, se recomandă prudență în ceea ce privește criptarea, astfel cum a subliniat Grupul la nivel înalt. Pe baza soluțiilor identificate în foaia de parcurs tehnologică, vor fi avute în vedere măsuri specifice de promovare a unei abordări coordonate a standardizării.

Orice standardizare ar trebui să reflecte cerințele legale aplicabile și să se bazeze pe soluții evaluate. Standardizarea trebuie să se asigure că accesul legal nu intră în conflict cu standardele de securitate cibernetică aplicabile, cum ar fi cele elaborate în temeiul Regulamentului privind reziliența cibernetică, sau cu standardele care sprijină punerea în aplicare a Directivei NIS 2 și nici nu afectează în alt mod securitatea produselor și a serviciilor.

În ceea ce privește recomandările Grupului la nivel înalt[48], **Comisia va elabora și va raționaliza o abordare a UE privind standardizarea pentru securitatea internă, cu accent pe criminalistica digitală, divulgarea legală și interceptarea legală.** Această abordare se va baza pe o analiză panoramică continuă efectuată de practicienii din domeniul aplicării legii, în special prin intermediul Grupului de lucru european privind standardizarea în materie de securitate internă, condus de Europol. Această acțiune va spori, de asemenea, resursele și domeniul de aplicare al grupului de lucru și va presupune continuarea colaborării cu alte inițiative în materie de standardizare, în special în ceea ce privește IA și criminalistica digitală.

[47] A se vedea *First report on Encryption from the EU Innovation Hub on Internal Security* („Primul raport privind criptarea publicat de Centrul european de inovare pentru securitatea internă”), 11 iunie 2024.
[48] Grupul de recomandări 10, Raportul final al Grupului la nivel înalt.

Obiectivul este de a se asigura că preocupările legate de securitate sunt integrate în politica de standardizare. În plus, această inițiativă va include dezvoltarea și organizarea de cursuri de formare privind standardizarea în domeniul securității și acordarea de sprijin financiar prin intermediul Fondului pentru securitate internă experților care participă la forumurile de standardizare relevante. Inițiativa va cuprinde, de asemenea, mecanisme de guvernanță relevante.

Acțiuni-cheie

- **Comisia, în strânsă cooperare cu Europol, va dezvolta și va raționaliza activitățile de standardizare pentru accesul legal, sprijinite de mecanisme de guvernanță adecvate (între T2-2025 și T2-2027).**

- **Statele membre sunt încurajate să aloce resurse suficiente pentru a se asigura că practicienii din domeniul securității participă la forumurile de standardizare relevante privind accesul legal.**

VI. Analizarea probelor în mod eficace și legal: inteligența artificială (IA)

Europol și Eurojust au constatat recent că un număr tot mai mare de anchete conțin volume foarte mari de date[49]. Într-un caz standard de abuz sexual asupra minorilor, anchetele necesită adesea analizarea unui volum de 1-3 terabiți de date, care pot include 1-10 milioane de imagini și mii de ore de înregistrări video[50]. În 2023, 1 553 822 de fișiere mari au fost schimbate prin intermediul schimbului de fișiere de mari dimensiuni (LFE)[51] al Europol. În cazul EncroChat, au fost interceptate peste 115 milioane de conversații între suspecții de constituire a unui grup infracțional organizat. În lunile care au urmat, prin tehnici și mijloace analitice avansate, cum ar fi învățarea automată, Europol și agențiile de aplicare a legii au fost în măsură să identifice modele, legături și puncte fierbinți, ceea ce a condus la arestarea a 6 558 de suspecți. Autoritățile neerlandeze și franceze au comunicat aceste informații omologilor lor din statele membre ale UE și din țările terțe, ceea ce a dus la zădărnicirea a peste 200 de comploturi în vederea săvârșirii unui omor numai în Regatul Unit[52].

Creșterea continuă a volumului de date prelucrate în cursul anchetelor îngreunează stocarea, gestionarea și analizarea eficace a datelor fără o expertiză semnificativă, fără resurse de calcul și fără instrumente specializate. Europol și Eurojust au confirmat că volumul de date poate fi copleșitor pentru anchetatori și poate conduce la termene de prelucrare mai lungi și la probleme legate de capacitatea de stocare. De asemenea, adesea, statele membre nu dispun de mecanismele și infrastructura necesare pentru a gestiona transferul unor volume mari de date către alte state membre și către Europol.

[49] *Common Challenges in Cybercrime* („Provocări comune în materie de criminalitate informatică"), Analiză din 2024 efectuată de Europol și Eurojust.
[50] IOCTA Europol.
[51] Raportul anual de activitate consolidat al Europol pentru 2023.
[52] *Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée*; *Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized* („Dezmembrarea rețelei EncroChat de comunicații criptate utilizată de grupurile infracționale duce la arestarea a peste 6 500 de persoane și la confiscarea unei sume de aproximativ 900 de milioane EUR") |. Europol. EncroChat.

Prin urmare, utilizarea IA este esențială pentru ca autoritățile de aplicare a legii să prevină, să depisteze și să investigheze infracțiunile și, prin urmare, să protejeze societățile noastre în era digitală. Soluțiile bazate pe IA pot îndeplini sarcini simple, cum ar fi traducerea automată sau transformarea vorbirii în text, sau sarcini mai complexe, cum ar fi filtrarea datelor, corelarea probelor din volume uriașe de date sau combaterea utilizării răuvoitoare a IA. Instrumentele bazate pe IA și destinate autorităților de aplicare a legii trebuie să fie exacte, transparente și conforme pe deplin cu cadrul juridic al UE privind IA, protecția datelor și a vieții private, pentru a asigura anchete de încredere și etice, bazate pe date. Inteligența artificială și calculul de înaltă performanță au o importanță capitală pentru obținerea accesului la date criptate și pentru sprijinirea anchetelor și a analizelor criminalistice.

În urma recomandărilor Grupului la nivel înalt de a crește finanțarea destinată cercetării și dezvoltării de instrumente pentru analiza datelor bazată pe IA și de a stabili rezultate clare[53], **Comisia va promova dezvoltarea și adoptarea de soluții de IA.** Această promovare include investiții specifice în dezvoltarea capacităților esențiale, cum ar fi soluții de identificare a pistelor de investigare din volume foarte mari de date, cu respectarea deplină a principiilor de protecție a datelor și a vieții private, sau îmbunătățiri în ceea ce privește urmărirea tranzacțiilor cu criptomonede. Ar putea fi, de asemenea, posibil să se valorifice oportunitățile de antrenare, testare și evaluare a instrumentelor bazate pe IA într-un spațiu de testare în materie de reglementare a IA, astfel cum se prevede în Regulamentul privind IA[54], cu sprijinul și îndrumarea autorităților de supraveghere competente. În plus, fabricile de IA și viitoarele gigafabrici ar putea sprijini dezvoltarea de instrumente și servicii bazate pe IA pentru asigurarea respectării legii. Comisia ar trebui să faciliteze aceste eforturi, pe baza unei analize a nevoilor realizate împreună cu părțile interesate, inclusiv cu Laboratorul de inovare al Europolului și cu Centrul de inovare pentru securitatea internă al agențiilor UE din domeniul justiției și afacerilor interne.

Statele membre pot avea acces la capacități relevante la costuri reduse sau chiar fără costuri, asigurând compatibilitatea cu cerințele Regulamentului privind IA. O abordare cuprinzătoare a IA este esențială și include crearea unor formate standardizate de date pentru schimburile de date și elaborarea de orientări privind utilizarea unor astfel de sisteme în concordanță cu Regulamentul privind IA și cu legislația aplicabilă a UE privind protecția datelor. Această acțiune ar putea fi sprijinită prin finanțare din Fondul pentru securitate internă, programul Europa digitală și Orizont Europa. Acțiunea va implica sprijinirea Europol și a comunității EMPACT pentru a asigura o corelare adecvată cu nevoile operaționale și pentru a promova adoptarea și integrarea de către practicieni.

Acțiuni-cheie

Comisia urmează:

- **să promoveze crearea și adoptarea de noi soluții de IA și să le îmbunătățească pe cele existente pentru filtrarea și analizarea probelor digitale, inclusiv prin utilizarea deplină a spațiilor de testare în materie de reglementare a IA pentru dezvoltarea, testarea și evaluarea acestora, în concordanță cu Regulamentul privind IA (în perioada 2025-2028);**

[53] Recomandarea 4, Recomandările Grupului la nivel înalt.
[54] A se vedea articolul 57 din Regulamentul privind inteligența artificială.

- **să se angajeze într-un dialog cu autoritățile de aplicare a legii și cu alte părți interesate pentru a identifica nevoile acestora, pe baza activității Laboratorului de inovare al Europolului și a Centrului de inovare al agențiilor UE din domeniul justiției și afacerilor interne;**

- **să sprijine elaborarea unor orientări clare pentru utilizarea IA în asigurarea respectării legii;**

- **să sprijine proiectele-pilot care vizează dezvoltarea și antrenarea unor soluții de IA solide din punct de vedere juridic și tehnic pentru criminalistica digitală, analiza datelor și alte instrumente de anchetă care să fie utilizate în scopul asigurării respectării legii.**