COMISIA
EUROPEANĂ

Strasbourg, 1.4.2025
COM(2025) 148 final

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

privind ProtectEU: o strategie europeană de securitate internă

1. ProtectEU: o strategie europeană de securitate internă

Securitatea reprezintă piatra de temelie a tuturor libertăților noastre. Democrația, statul de drept, drepturile fundamentale, bunăstarea europenilor, competitivitatea și prosperitatea – toate depind de capacitatea noastră de a oferi o garanție de securitate de bază. În noua eră a amenințărilor la adresa securității în care trăim în prezent, capacitatea statelor membre ale UE de a garanta securitatea cetățenilor lor depinde, mai mult ca oricând, de o **abordare europeană unificată în ceea ce privește protejarea securității noastre interne**. Într-un peisaj geopolitic în continuă evoluție, Europa trebuie să continue să își respecte promisiunea trainică de pace.

Primii pași către construirea unui aparat european de securitate au fost deja făcuți. În ultimul deceniu, am înzestrat Uniunea cu mecanisme colective de acțiune îmbunătățite în domeniul asigurării respectării legii și al cooperării judiciare, al securității frontierelor, al combaterii formelor grave de criminalitate organizată, al combaterii terorismului și a extremismului violent și al protecției infrastructurii critice fizice și digitale a UE. Punerea în aplicare corespunzătoare a legislației adoptate anterior și a politicilor elaborate rămâne esențială.

Natura amenințărilor actuale și legătura intrinsecă dintre securitatea internă și cea externă a UE ne impun să mergem mai departe.

Situația amenințărilor este gravă. Liniile de demarcație dintre **amenințările hibride** și războiul deschis sunt neclare. Rusia a desfășurat o campanie hibridă online și offline împotriva UE și a partenerilor săi, pentru a perturba și submina coeziunea societală și procesele democratice și pentru a testa solidaritatea UE cu Ucraina. State străine ostile și actori sponsorizați de stat încearcă să se infiltreze și să perturbe infrastructura noastră critică și lanțurile noastre de aprovizionare, să fure date sensibile și să se poziționeze pentru o perturbare maximă în viitor. Ei utilizează criminalitatea ca serviciu, iar infractorii ca intermediari. În plus, dependențele noastre de țările terțe în ceea ce privește lanțurile de aprovizionare ne fac mai vulnerabili la campaniile hibride desfășurate de statele ostile.

Rețelele de criminalitate organizată puternice se înmulțesc în Europa, alimentate online, extinzându-se în economia noastră și afectându-ne societatea, astfel cum s-a subliniat în Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în UE (SOCTA), prezentată recent de Europol[1]. Odată ce criminalitatea organizată se instalează într-o comunitate sau într-un sector economic, eradicarea acesteia devine o luptă anevoioasă: o treime din cele mai periculoase rețele infracționale sunt active de peste zece ani. Criptomonedele și sistemele financiare paralele le ajută să spele și să ascundă produsele provenite din săvârșirea de infracțiuni.

Nivelul de amenințare teroristă din Europa continuă să planeze. Crizele regionale din afara UE creează un efect în lanț, oferind o nouă motivație actorilor teroriști din întregul spectru ideologic de a-și recruta, mobiliza sau consolida capacitățile. Aceștia își îndreaptă eforturile de radicalizare și recrutare în special către categoriile cele mai vulnerabile ale societăților noastre și mai ales către anumiți tineri. Ele inspiră atacuri ale unor actori individuali și o creștere a extremismului antisistem, al cărui scop este de a perturba ordinea juridică democratică.

Progresele tehnologice semnificative oferă instrumente esențiale pentru îmbunătățirea aparatului nostru de securitate. Însă atacurile cibernetice și acțiunile străine de manipulare a informațiilor sunt din ce în ce mai răspândite, exploatând noi tehnologii, cum ar fi inteligența artificială. Copiii, tinerii și persoanele în vârstă sunt deosebit de expuși riscului în mediul online, iar răspândirea urii în mediul online amenință libertatea de exprimare și coeziunea socială.

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

Viețile noastre au devenit mai puțin sigure, iar acest lucru este resimțit tot mai mult de europeni, a căror **percepție asupra siguranței și securității în UE** s-a erodat, astfel încât, atunci când sunt întrebați despre viitor, 64 % tind să fie îngrijorați de securitatea UE[2]. Întreprinderile sunt, de asemenea, din ce în ce mai preocupate; informarea greșită și dezinformarea, criminalitatea și activitatea ilicită, precum și spionajul cibernetic se numără toate printre primele zece riscuri identificate în Raportul din 2025 privind riscurile globale al Forumului Economic Mondial[3].

Europenii ar trebui să **își poată trăi viața fără teamă**, fie pe străzi, acasă, în locuri publice, pe metrou sau pe internet. Protecția persoanelor, în special a celor mai vulnerabile la atacuri, care tind să afecteze în mod disproporționat copiii, femeile și minoritățile, inclusiv comunitățile evreiești și musulmane, se află în centrul activității UE în materie de securitate. Acest lucru este esențial pentru construirea unor societăți reziliente și bazate pe coeziune.

Comisia stabilește o **strategie europeană de securitate internă** pentru a contracara mai bine amenințările în anii următori. Cu un set de instrumente juridice mai performante, o cooperare mai strânsă și un schimb sporit de informații, ne vom consolida reziliența și capacitatea colectivă de a anticipa, preveni, detecta și răspunde în mod eficace la amenințările la adresa securității. O abordare unificată a securității interne poate sprijini statele membre să valorifice puterea tehnologiei pentru a consolida, nu de a slăbi securitatea, promovând în același timp un spațiu digital securizat pentru toți. În plus, această abordare sprijină un răspuns comun al statelor membre la schimbările politice și economice globale care afectează securitatea internă a Uniunii.

Prezenta strategie este ghidată de **trei principii** și integrează în centrul său respectarea statului de drept și a drepturilor fundamentale.

În primul rând, ea stabilește ambiția unei schimbări a culturii în materie de securitate. Avem nevoie de **o abordare la nivelul întregii societăți,** care să implice toți cetățenii și toate părțile interesate, inclusiv societatea civilă, cercetarea, mediul academic și entitățile private. Prin urmare, acțiunile din cadrul strategiei adoptă o abordare integrată, multipartită, ori de câte ori este posibil.

În al doilea rând, **considerentele de securitate trebuie să fie încorporate și integrate în toate actele legislative, politicile și programele UE**, inclusiv în acțiunea externă a Uniunii. Legislația, politicile și programele vor trebui să fie elaborate, revizuite și puse în aplicare din perspectiva securității, asigurându-se că sunt abordate aspectele de securitate necesare, astfel încât să se promoveze o abordare coerentă și cuprinzătoare a securității.

În cele din urmă, o Europă sigură, securizată și rezilientă necesită **investiții semnificative din partea UE, a statelor sale membre și a sectorului privat**. Prioritățile și acțiunile stabilite în prezenta strategie necesită resurse umane și financiare suficiente pentru a asigura punerea lor în aplicare. Astfel cum se prevede în Comunicarea privind calea către următorul cadru financiar multianual[4], Europa va trebui să majoreze cheltuielile publice pentru securitate și să promoveze cercetarea și investițiile în domeniul securității, consolidându-și autonomia strategică.

Prezenta strategie completează **Strategia privind o Uniune a pregătirii**[5], care stabilește o abordare integrată multirisc în ceea ce privește pregătirea pentru conflicte, dezastre naturale și antropice și crize, precum și **Cartea albă privind pregătirea pentru apărare a Europei 2030**[6], care sprijină dezvoltarea și achiziționarea de capabilități de apărare în întreaga UE pentru

[2] Sondajul Eurobarometru Flash FL550: Provocări și priorități ale UE.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p. 17.
[4] COM(2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

a descuraja adversarii străini. Comisia va propune, de asemenea, un **scut european pentru democrație** pentru a consolida reziliența democratică în UE. Împreună, aceste inițiative stabilesc o viziune pentru o UE sigură, securizată și reziliență.

O nouă guvernanță europeană în materie de securitate internă

Comisia va colabora îndeaproape cu statele membre și cu agențiile UE pentru a actualiza abordarea UE în materie de securitate internă, atât la nivel strategic, cât și la nivel operațional.

Acest lucru se va realiza în următoarele moduri:

- **identificarea consecventă a potențialelor implicații în materie de securitate și pregătire ale inițiativelor noi și revizuite ale Comisiei încă de la început și pe tot parcursul procesului de negociere;**
- **reuniuni periodice ale Grupului de proiect al Comisiei privind securitatea internă europeană, sprijinite de o colaborare intersectorială strategică în cadrul Comisiei;**
- **prezentări ale analizelor amenințărilor legate de securitatea internă pentru a sprijini activitatea Colegiului de securitate;**
- **discuții cu statele membre în cadrul Consiliului cu privire la evoluția provocărilor în materie de securitate internă pe baza analizei amenințărilor și schimb de opinii cu privire la principalele priorități de politică;**
- **raportarea cu regularitate către Parlamentul European și Consiliu pentru a urmări și a sprijini punerea în aplicare sistematică a inițiativelor-cheie în materie de securitate.**

2. Conștientizarea integrată a situației și analiza amenințărilor

Vom înzestra UE cu noi modalități de partajare și combinare a informațiilor și vom furniza o analiză periodică a amenințărilor la adresa securității interne a UE, contribuind la o evaluare cuprinzătoare a riscurilor și a amenințărilor.

Securitatea începe cu **anticiparea efectivă**. UE trebuie să se bazeze pe o conștientizare a situației și pe o analiză a amenințărilor cuprinzătoare, suficient de autonome și actualizate. Informațiile acționabile, pe care statele membre sunt încurajate să le consolideze în continuare prin intermediul Capacității unice de analiză a informațiilor (SIAC), ca punct unic de intrare pentru informațiile operative ale statelor membre, sunt vitale pentru evaluarea și combaterea amenințărilor, contribuind în cele din urmă la acțiuni de politică și legislative[7]. Trebuie să valorificăm **analiza bazată pe informații** și **evaluările amenințărilor** la nivelul UE într-un mod mai eficace și mai colaborativ.

Pe baza diferitelor evaluări ale riscurilor și amenințărilor realizate la nivelul UE și pentru sectoare specifice[8], Comisia va elabora **analize periodice ale amenințărilor la adresa securității interne a UE** pentru a identifica principalele provocări în materie de securitate, cu scopul de a fundamenta prioritățile de politică. Acestea vor contribui la elaborarea unei politici

[7] Un nivel mai mare de siguranță împreună – Consolidarea disponibilității și pregătirii în domeniul apărării civile și militare a Europei, p. 23.

[8] Evaluările sectoriale ale amenințărilor care vor contribui la fundamentarea acestei analize a amenințărilor includ Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în UE (SOCTA), Raportul UE privind situația terorismului și evoluția acestuia (TE-SAT), Raportul comun de evaluare a securității cibernetice (JCAR) și evaluările viitoare ale amenințărilor, riscurilor și metodelor de spălare a banilor și de finanțare a terorismului care urmează să fie efectuate de Comisie și de Autoritatea pentru Combaterea Spălării Banilor.

de securitate internă flexibile și reactive, care să abordeze în mod eficace amenințările în continuă evoluție, să protejeze mai bine cetățenii și întreprinderile împotriva atacurilor și să permită intervenții de politică specifice în timp util. Aceste analize ale amenințărilor la adresa securității interne a UE vor contribui, de asemenea, la **evaluarea (transsectorială, multirisc) cuprinzătoare a riscurilor și amenințărilor la adresa UE**, elaborată de Comisie și de Înaltul Reprezentant, astfel cum se prevede în Strategia privind o Uniune a pregătirii.

Încrederea și gestionarea în condiții de siguranță sunt esențiale pentru schimbul de informații, iar acest lucru necesită o infrastructură fiabilă și securizată. Instituțiile, organele și agențiile UE trebuie să își asigure capacitatea de a utiliza **canale de comunicare securizate** pentru schimbul de informații sensibile și clasificate între ele și cu statele membre. Investițiile în **sisteme securizate interoperabile** și în tehnologii fiabile vor consolida autonomia UE și capacitatea UE de a gestiona crizele și de a asigura reziliența operațională. În acest context, Comisia îndeamnă colegiuitorii să finalizeze negocierile referitoare la **propunerea de regulament privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii**, în special pentru a asigura un cadru comun pentru gestionarea informațiilor sensibile neclasificate și clasificate[9].

Pentru a-și asigura propria securitate operațională și conștientizarea situației, Comisia își va revizui cadrul de guvernanță în materie de securitate corporativă și va institui un **centru integrat de operațiuni de securitate (ISOC)** pentru a proteja persoanele, activele fizice și operațiunile din toate centrele Comisiei. De asemenea, Comisia își va mări capacitățile operaționale și analitice pentru identificarea și atenuarea amenințărilor hibride.

În conformitate cu Strategia privind o Uniune a pregătirii, aspectele legate de pregătire și securitate vor fi încorporate și integrate în legislația, politicile și programele UE. Atunci când va pregăti sau va revizui legislația, politicile sau programele ținând seama de perspectiva pregătirii și a securității, Comisia va identifica în mod consecvent impactul potențial al opțiunii de politică preferate asupra pregătirii și a securității. Acest demers va fi susținut de formarea periodică a factorilor de decizie în cadrul Comisiei.

Pentru a sprijini statele membre, Comisia va discuta cu Consiliul despre provocările în continuă evoluție în materie de securitate internă și despre principalele priorități de politică și va informa periodic Consiliul cu privire la punerea în aplicare a strategiei. În plus, Comisia va informa și va implica Parlamentul European și părțile interesate relevante în toate acțiunile relevante.

Acțiuni-cheie

Comisia:

- **va elabora și prezenta analize periodice ale amenințărilor pentru provocările în materie de securitate internă a UE**

Statele membre sunt invitate:

- **să îmbunătățească schimbul de informații cu SIAC și să asigure un schimb mai bun de informații cu agențiile și organele UE**

Parlamentul European și Consiliul sunt încurajate:

- **să finalizeze negocierile referitoare la propunerea de regulament privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii**

[9] COM(2022) 119 final.

3. Consolidarea capabilităților de securitate ale UE

Vom dezvolta noi instrumente pentru asigurarea respectării legii, cum ar fi un Europol modernizat, și mijloace mai bune de coordonare și asigurare a schimbului securizat de date și a accesului legal la date.

Pentru a contracara în mod eficace amenințările în continuă evoluție, UE trebuie să își consolideze capabilitățile de securitate și să stimuleze inovarea. Ca actori principali împotriva amenințărilor la adresa securității interne, autoritățile de aplicare a legii și autoritățile judiciare au nevoie de instrumentele și capabilitățile operaționale adecvate pentru a acționa prompt și eficace. Este important ca aceste autorități să fie capabile să comunice și să se coordoneze la nivel transfrontalier și între servicii, pentru a preveni, a depista, a investiga și a urmări penal în mod eficient.

Agențiile și organele UE pentru securitate internă

Agențiile și organele UE din domeniul justiției, al afacerilor interne și al securității cibernetice joacă un rol esențial în arhitectura de securitate a UE – un rol care continuă să evolueze pe măsură ce responsabilitățile lor se extind.

Astăzi, la 25 de ani de la înființare, **Europol** este mai important ca niciodată pentru cadrul de securitate al UE. El sprijină investigațiile transfrontaliere complexe, facilitează schimbul de informații, dezvoltă instrumente inovatoare pentru activitățile polițienești și oferă expertiză avansată pentru asigurarea respectării legii. Cu toate acestea, mai mulți factori împiedică Europol să își atingă pe deplin potențialul operațional în ceea ce privește sprijinirea activităților operaționale și de investigare pentru combaterea criminalității transfrontaliere: ei variază de la un nivel insuficient de resurse la faptul că mandatul său actual nu acoperă noile amenințări la adresa securității, cum ar fi sabotajul, amenințările hibride sau manipularea informațiilor. Acesta este motivul pentru care Comisia va propune **o revizuire ambițioasă a mandatului Europol**, pentru a-l transforma într-o agenție de poliție cu adevărat operațională, sprijinind mai bine statele membre. Scopul este de a consolida expertiza tehnologică și capacitatea Europol de a sprijini agențiile naționale de aplicare a legii, de a îmbunătăți coordonarea cu alte agenții și organisme și cu statele membre, de a consolida parteneriatele strategice cu țările partenere și cu sectorul privat și de a asigura o supraveghere consolidată a Europol.

În plus, Comisia va depune eforturi pentru **a îmbunătăți în continuare eficacitatea și complementaritatea agențiilor și organelor UE pentru securitate internă și pentru a susține cooperarea neîntreruptă** dintre acestea.

Mandatul **Eurojust** va fi evaluat și consolidat pentru o cooperare judiciară mai eficace, sporind complementaritatea și cooperarea cu Europol. Aceste acțiuni includ consolidarea eficienței Eurojust, precum și a capacității sale de a oferi sprijin proactiv și analiză autorităților judiciare ale statelor membre. În plus, având în vedere competența unică a **EPPO** de a investiga și de a urmări penal infracțiunile care aduc atingere intereselor financiare ale Uniunii, Comisia va analiza cele mai bune modalități de îmbunătățire a capacității EPPO de a proteja fondurile Uniunii. Aceasta va include consolidarea cooperării dintre EPPO și Europol.

Schimbul eficient și securizat de informații între agenții este esențial pentru cooperare. Europol și Frontex au nevoie de un schimb reciproc rapid de informații, inclusiv în scopuri operaționale, ca urmare a declarației comune din ianuarie 2024[10]. **eu-LISA** are un rol central în asigurarea stocării securizate și a disponibilității datelor pentru o mai bună coordonare și un schimb de informații mai eficient între agenții. **Agenția pentru Drepturi Fundamentale a**

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Uniunii Europene oferă expertiză privind protecția drepturilor fundamentale în elaborarea și punerea în aplicare a politicilor de securitate.

Autoritatea UE pentru Combaterea Spălării Banilor (ACSB) a fost împuternicită să coreleze informațiile, pe baza unui răspuns pozitiv/negativ, cu informațiile puse la dispoziție de Europol, EPPO, Eurojust și Oficiul European de Luptă Antifraudă pentru a efectua analize comune ale cazurilor transfrontaliere.

ENISA joacă un rol central în punerea în aplicare a legislației europene în materie de securitate cibernetică. În viitoarea **revizuire a Regulamentului privind securitatea cibernetică**, Comisia va evalua mandatul acestei agenții și va propune modernizarea acestuia pentru a-i consolida valoarea adăugată europeană.

Cooperarea dintre autoritățile vamale și alte autorități de aplicare a legii va fi intensificată odată cu propunerea de creare a **Autorității vamale a UE** și a **Platformei de date vamale a UE** în cadrul pachetului de reformă vamală a UE. Informațiile din viitoarea platformă și datele conexe furnizate de Europol, Eurojust, EPPO, OLAF, ACSB și Frontex, în cadrul competențelor lor, vor consolida analiza comună și vor contribui la activități operaționale mai coerente, în special la frontierele externe. Comisia încurajează colegiuitorii să finalizeze rapid negocierile privind reforma vamală a UE și va continua să îi sprijine în acest scop.

Consolidarea complementarității dintre EPPO, OLAF, Europol, Eurojust, ACSB și Autoritatea vamală a UE propusă se va baza, de asemenea, pe rezultatele revizuirii în curs a **arhitecturii antifraudă a UE**. Securitatea internă poate beneficia de această abordare holistică, axându-se pe o mai bună utilizare atât a mijloacelor penale, cât și a celor administrative, pe interoperabilitatea sistemelor informatice și pe îmbunătățirea cooperării.

Comunicații critice

În prezent, **sistemele de comunicații critice**[11] funcționează, în majoritatea cazurilor, în mod izolat la nivel național. Aceasta înseamnă că, adesea, membrii personalului care asigură prima intervenție nu pot comunica cu omologii lor atunci când trec frontiera în alte state membre. În unele state membre, există, de asemenea, limitări în ceea ce privește comunicațiile între diferitele tipuri de personal care asigură prima intervenție (de exemplu, poliția și ambulanțele). Standardele majorității sistemelor nu îndeplinesc cerințele actuale în ceea ce privește funcționalitatea și reziliența, limitând în mod semnificativ capacitatea de reacție a personalului care asigură prima intervenție, în special la nivel transfrontalier.

Pentru a îmbunătăți capacitatea UE de a reacționa la crize, Comisia va propune acte legislative pentru crearea unui **sistem european de comunicații critice (EUCCS)** care să conecteze sistemele de comunicații critice de nouă generație ale statelor membre în UE. Obiectivul este ca EUCCS să se bazeze pe trei piloni strategici: mobilitate operațională, reziliență puternică și autonomie strategică. Inițiativa EUCCS va stabili cerințe armonizate și va contribui la modernizarea sistemelor de comunicații critice ale statelor membre, permițându-le să funcționeze fără sincope. De asemenea, ea va extinde acoperirea sistemelor prin intermediul viitorului sistem multiorbital IRIS[212]. Proiectele finanțate de UE vor construi capabilitățile tehnice ale EUCCS, bazându-se în principal pe furnizorii europeni de tehnologie, pentru a promova autonomia strategică a UE în acest sector sensibil.

[11] Și anume rețelele utilizate de autoritățile de aplicare a legii, polițiștii de frontieră, autoritățile vamale, protecția civilă, pompierii, personalul medical de intervenție în situații de urgență și alți actori-cheie pentru securitatea și siguranța publică.
[12] Infrastructura UE pentru reziliență, interconectivitate și securitate prin satelit.

Accesul legal la date

Autoritățile de aplicare a legii și autoritățile judiciare trebuie să fie în măsură să investigheze și să ia măsuri împotriva criminalității. În prezent, aproape toate formele grave de criminalitate organizată au o amprentă digitală[13]. Aproximativ 85 % din investigațiile penale se bazează în prezent pe capacitatea autorităților de aplicare a legii de a accesa informații digitale[14].

Grupul la nivel înalt privind accesul la date pentru o asigurare eficace a respectării legii a subliniat în raportul său final[15] că autoritățile de aplicare a legii și sistemele judiciare au pierdut teren în fața infractorilor în ultimul deceniu, deoarece infractorii recurg la instrumente și produse care provin din alte jurisdicții, oferite de furnizori ce au luat măsuri care fac imposibilă cooperarea în legătură cu solicitări legitime în cazuri penale individuale. Cooperarea sistematică dintre autoritățile de aplicare a legii și părțile private, inclusiv furnizorii de servicii, este, prin urmare, esențială în eforturile viitoare de a perturba activitatea celor mai periculoase rețele infracționale și a membrilor acestora, din Uniune și din afara ei.

Pe măsură ce digitalizarea devine din ce în ce mai răspândită și oferă o sursă tot mai mare de noi instrumente pentru infractori, este esențial să existe un cadru pentru accesul la date care să răspundă nevoilor de a asigura respectarea legislației noastre și de a ne proteja valorile. În același timp, asigurarea faptului că sistemele digitale rămân securizate împotriva accesului neautorizat este, în egală măsură, vitală pentru menținerea securității cibernetice și protejarea împotriva amenințărilor emergente la adresa securității. Aceste cadre de acces trebuie, de asemenea, să respecte drepturile fundamentale, asigurând, printre altele, protecția adecvată a vieții private și a datelor cu caracter personal.

În ultimii ani, UE a luat măsuri atât pentru a combate **criminalitatea online, cât și pentru a facilita accesul la probele electronice pentru toate infracțiunile**, prin adoptarea unor norme privind probele electronice care se vor aplica pe deplin începând din august 2026[16]. Aceste măsuri vor fi completate de instrumente internaționale pentru schimbul de informații și de probe. Comisia va propune în curând semnarea și încheierea noii **Convenții a ONU împotriva criminalității informatice**.

Pentru a da curs recomandărilor Grupului la nivel înalt[17], în prima jumătate a anului 2025, Comisia va prezenta o **foaie de parcurs prin care stabilește măsurile juridice și practice** pe care propune să le ia **pentru a asigura accesul legal și efectiv la date**. Ca urmare a acestei foi de parcurs, Comisia va acorda prioritate unei evaluări a impactului **normelor de păstrare a datelor** la nivelul UE și elaborării unei **foi de parcurs tehnologice privind criptarea**, pentru a identifica și a evalua soluțiile tehnologice care ar permite autorităților de aplicare a legii să acceseze date criptate în mod legal, protejând securitatea cibernetică și drepturile fundamentale.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52019PC0070.
[15] Raportul final al Grupului la nivel înalt privind accesul la date pentru o asigurare eficace a respectării legii – 15.11.2024, 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Regulamentul (UE) 2023/1543 al Parlamentului European și al Consiliului din 12 iulie 2023 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale, JO L 191, 28.7.2023.
[17] 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.

Cooperare operațională

Comisia va colabora cu statele membre, cu agențiile și organele UE și cu țările partenere pentru a consolida cooperarea operațională, care este esențială pentru o abordare mai eficace a combaterii criminalității organizate transnaționale și a terorismului.

Ca principal cadru al UE pentru acțiuni comune împotriva formelor grave de criminalitate organizată, **Platforma multidisciplinară europeană împotriva amenințărilor infracționale (EMPACT)** a obținut rezultate operaționale substanțiale. Următorul ciclu EMPACT 2026-2029 reprezintă o oportunitate de a consolida și mai mult acest cadru. Pentru a perturba activitatea celor mai periculoase rețele infracționale și a membrilor acestora, Uniunea trebuie să își raționalizeze și să își concentreze eforturile asupra celor mai presante priorități, consolidând angajamentele statelor membre și asigurând o utilizare eficace a resurselor.

În acest scop, Comisia va colabora cu președințiile Consiliului și cu statele membre pentru a **maximiza potențialul EMPACT și pentru a aborda prioritățile-cheie pentru următorul ciclu EMPACT 2026-2029.** În aceste domenii prioritare, este nevoie de informații cu privire la cele mai periculoase rețele infracționale, de investigații comune și de grupuri operative operaționale, precum și de un răspuns judiciar puternic, inclusiv o abordare de tip „urmărirea banilor”. În plus, Uniunea trebuie să combată recrutarea și infiltrarea în scopuri infracționale și să consolideze cooperarea și formarea între agenții și la nivel internațional în materie de aplicare a legii.

Comisia va sprijini, de asemenea, alte forme de **cooperare operațională transfrontalieră în materie de aplicare a legii între statele membre și țările asociate spațiului Schengen**. Spațiul Schengen, fără controale la frontierele interne, necesită o cooperare strânsă și schimb de informații între autoritățile de aplicare a legii din statele membre pentru a asigura un nivel ridicat de securitate internă. În prezent, agenții de aplicare a legii se confruntă în continuare cu provocări atunci când supraveghează sau efectuează intervenții urgente la nivel transfrontalier[18], iar contracararea amenințărilor hibride necesită, de asemenea, o cooperare transfrontalieră sporită. Ar trebui creat un **grup la nivel înalt privind viitorul cooperării operative în materie de asigurare a respectării legii** pentru a dezvolta o viziune strategică comună.

Schimbul eficient de date între autoritățile de aplicare a legii este, de asemenea, esențial pentru o cooperare transfrontalieră eficace. Odată instituită, **arhitectura de interoperabilitate** va oferi autorităților de aplicare a legii și Europol acces efectiv la informații esențiale. În același timp, UE și statele sale membre ar trebui să acorde prioritate schimbului bilateral și multilateral de informații, prin punerea în aplicare juridică și tehnică a **Regulamentului Prüm II**[19], în cooperare cu eu-LISA și Europol. Acest lucru va permite schimburi automatizate securizate de amprente digitale, profiluri ADN, date privind înmatricularea vehiculelor, imagini faciale și evidențe ale poliției prin intermediul routerelor UE. La nivel național, statele membre trebuie să pună în aplicare **Directiva privind schimbul de informații**[20], consolidând canalele de

[18] Astfel cum s-a raportat în evaluarea de către Comisie a efectului dat de statele membre Recomandării (UE) 2022/915 a Consiliului din 9 iunie 2022 privind cooperarea operativă în materie de asigurare a respectării legii (5909/25).

[19] Regulamentul (UE) 2024/982 al Parlamentului European și al Consiliului din 13 martie 2024 privind căutarea și schimbul automatizat de date în scopul cooperării polițienești, și de modificare a Deciziilor 2008/615/JAI și 2008/616/JAI ale Consiliului și a Regulamentelor (UE) 2018/1726, (UE) 2019/817 și (UE) 2019/818 ale Parlamentului European și ale Consiliului (Regulamentul Prüm II), JO L, 2024/982, 5.4.2024.

[20] Directiva (UE) 2023/977 a Parlamentului European și a Consiliului din 10 mai 2023 privind schimbul de informații dintre autoritățile de aplicare a legii ale statelor membre și de abrogare a Deciziei-cadru 2006/960/JAI a Consiliului, JO L 134, 22.5.2023, p. 1.

schimb de informații pentru un flux transfrontalier neîntrerupt de informații, asigurând în același timp integrarea acestora în sistemele de la nivelul Uniunii, cum ar fi SIENA[21].

Cooperarea transfrontalieră eficace se bazează, de asemenea, pe promovarea unei **culturi comune a UE în materie de aplicare a legii**. Activitățile de formare în comun, centrele de excelență și programele de mobilitate sunt esențiale pentru atingerea acestui obiectiv. Comisia va analiza modul în care UE poate sprijini cel mai bine formarea autorităților statelor membre, bazându-se pe **CEPOL** ca agenție a UE pentru formare în materie de aplicare a legii.

Consolidarea securității frontierelor

Consolidarea rezilienței și a securității frontierelor externe este esențială pentru a contracara amenințările hibride, cum ar fi utilizarea migrației ca armă, pentru a preveni intrarea în UE a bunurilor și a actorilor care generează amenințări, precum și pentru a combate în mod eficace criminalitatea transfrontalieră și terorismul. **Sistemul de informații Schengen (SIS) urmează să fie îmbunătățit** în 2026 pentru a permite statelor membre să introducă alerte privind resortisanți ai țărilor terțe implicați în terorism, inclusiv luptători teroriști străini, și în alte infracțiuni grave, pe baza datelor comunicate de țările terțe către Europol.

O mai bună **interoperabilitate** a sistemelor de informații la scară largă ale UE va oferi statelor membre informații esențiale privind persoanele din țări terțe care trec sau intenționează să treacă frontierele externe, ajutând autoritățile să evalueze condițiile de autorizare a intrării pe teritoriul statelor membre[22]. Comisia va continua să colaboreze îndeaproape cu statele membre și cu eu-LISA pentru punerea în aplicare rapidă a acestor sisteme, în special a **Sistemului de intrare/ieșire (EES), a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și a Sistemului de informații privind vizele (VIS) revizuit**, pentru a asigura buna funcționare și beneficiile în materie de securitate ale acestora.

Pentru a spori în continuare securitatea frontierelor și a consolida cooperarea UE în fața amenințărilor în continuă evoluție, **Comisia va propune consolidarea Frontex**. Numărul de agenți ai Poliției de Frontieră și Gărzii de Coastă la nivel european ar trebui să se tripleze în timp, ajungând la 30 000. Agenția ar trebui să fie dotată cu tehnologii avansate pentru supraveghere și conștientizarea situației, inclusiv cu informații relevante pentru gestionarea europeană integrată a frontierelor și cu acces la servicii guvernamentale solide ale UE de observare a Pământului pentru controlul la frontiere, care urmează să fie desfășurate până în 2027. Acest lucru ar trebui să consolideze și mai mult capacitatea de detectare, prevenire și combatere a criminalității transfrontaliere la frontierele externe, precum și să consolideze sprijinul acordat statelor membre în ceea ce privește punerea în aplicare a returnărilor, în special în ceea ce privește resortisanții țărilor terțe care prezintă un risc în materie de securitate.

Fraudarea documentelor și frauda de identitate facilitează introducerea ilegală de migranți, traficul de persoane, mișcările infracționale clandestine și traficul de bunuri ilicite. **Detectorul de identități multiple (MID)**[23], odată ce va fi operațional, va îmbunătăți capacitatea autorităților naționale de a identifica persoanele care utilizează identități multiple și de a combate frauda de identitate. Comisia va explora modalități de sporire a securității

[21] Secure Information Exchange Network Application (Aplicație de rețea pentru schimbul securizat de informații).
[22] În special, Sistemul de intrare/ieșire (EES) va permite statelor membre să identifice resortisanții țărilor terțe la frontierele externe ale spațiului Schengen și să înregistreze intrările și ieșirile acestora, permițând identificarea sistematică a persoanelor care depășesc durata de ședere autorizată. Înainte de sosirea unui resortisant al unei țări terțe la frontierele externe, Sistemul european de informații și de autorizare privind călătoriile (ETIAS) și Sistemul de informații privind vizele (VIS) vor permite statelor membre să evalueze în prealabil dacă prezența unui resortisant al unei țări terțe pe teritoriul UE ar prezenta un risc în materie de securitate.
[23] MID este una dintre componentele de interoperabilitate introduse prin Regulamentul (UE) 2019/818 și prin Regulamentul (UE) 2019/817.

documentelor de călătorie și de ședere eliberate cetățenilor UE și resortisanților țărilor terțe. În plus, Comisia va evalua modul în care portofelele UE pentru identitatea digitală, care urmează să fie introduse în cadrul european al identității digitale până la sfârșitul anului 2026, pot contribui la sporirea securității documentelor de călătorie și la îmbunătățirea verificării identității. Acest lucru va completa propunerile privind credențialele digitale de călătorie și aplicația UE pentru credențiale digitale de călătorie[24].

Informațiile privind călătoriile sunt esențiale pentru ca autoritățile să identifice și să investigheze deplasările infractorilor, ale teroriștilor și ale altor persoane care reprezintă amenințări la adresa securității. Deși există un cadru al UE pentru informațiile comerciale privind călătoriile aeriene[25], prelucrarea datelor provenite de la alte moduri de transport în scopul asigurării respectării legii este fragmentată. În consecință, infractorii și teroriștii pot exploata diferite moduri de transport pentru activități ilegale nedetectate. Comisia va colabora cu statele membre și cu sectorul transporturilor pentru a **consolida cadrul referitor la informațiile privind călătoriile** prin explorarea unui sistem al Uniunii care să impună operatorilor de zboruri private să colecteze și să transfere date privind pasagerii, prin evaluarea normelor de prelucrare a datelor din registrele cu numele pasagerilor și prin evaluarea modalităților de raționalizare a prelucrării informațiilor privind călătoriile maritime. În ceea ce privește transportul rutier, Comisia va evalua o utilizare extinsă a sistemelor de **recunoaștere automată a plăcuțelor de înmatriculare (ANPR)** și va spori posibilitățile de sinergii cu SIS.

Analiza prospectivă, inovarea și abordarea bazată pe capabilități

Comisia va elabora **o abordare prospectivă cuprinzătoare privind securitatea internă la nivelul UE**, bazându-se pe cele mai bune practici identificate la nivel național. Această abordare va sprijini elaborarea politicilor și va orienta investițiile în cercetarea și inovarea relevante în domeniul securității finanțate de UE.

Cercetarea și inovarea joacă un rol esențial în securitatea internă prin crearea de soluții pentru a contracara amenințările emergente, inclusiv cele generate de utilizarea abuzivă a tehnologiei[26]. UE trebuie să continue să investească, prin intermediul cercetării și inovării în domeniul securității finanțate de UE[27], în dezvoltarea de instrumente și soluții inovatoare pentru a aborda amenințările la adresa securității, respectând în același timp normele UE și drepturile fundamentale. Comisia ar trebui să sprijine tranziția de la cercetare la implementare, pentru a asigura adoptarea eficace a acestor capabilități moderne, acordând prioritate **tehnologiilor moderne,** cum ar fi IA. Această abordare ar trebui să includă cursuri de formare pentru a îmbunătăți utilizarea sistemelor de IA și a altor capabilități tehnice de către autoritățile de aplicare a legii și autoritățile judiciare. În plus, după caz, potențialul de dublă utilizare al tehnologiilor ar trebui exploatat în ambele direcții (de la civil la apărare și de la apărare la civil)[28].

[24] https://ec.europa.eu/commission/presscorner/detail/ro/ip_24_5047.

[25] Registrul cu numele pasagerilor (PNR) și cadrul privind informațiile prealabile referitoare la pasageri (Advance Passenger Information – API) instituite prin Directiva (UE) 2016/681 („Directiva PNR") și Regulamentul (UE) 2025/12 și Regulamentul (UE) 2025/13 („Regulamentele API").

[26] A se vedea raportul Centrului Comun de Cercetare al Comisiei intitulat „Emerging risks and opportunities for EU internal security stemming from new technologies" (Riscuri și oportunități emergente pentru securitatea internă a UE care decurg din noile tehnologii) https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] „Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025" (Studiu privind consolidarea cercetării și inovării în domeniul securității finanțate de UE – 20 de ani de cercetare și inovare în domeniul securității civile finanțate de UE), https://data.europa.eu/doi/10.2837/0004501.

[28] Astfel cum se prevede în raportul Niinistö.

Centrul european de inovare pentru securitatea internă[29], o rețea de laboratoare de inovare care oferă cele mai recente actualizări în materie de inovare și soluții eficace pentru a sprijini activitatea actorilor din domeniul securității interne din UE și din statele membre, va contribui la integrarea cercetării în practică și în politici. Sporirea eficacității Europol necesită consolidarea Registrului de instrumente al Europolului (Europol Tool Repository – ETR), permițându-i să identifice, să dezvolte, să achiziționeze în comun și să aplice tehnologii avansate din punct de vedere operațional. În plus, în cadrul Centrului său Comun de Cercetare, Comisia va înființa un **Campus de cercetare și inovare în domeniul securității**, care va reuni cercetători pentru a scurta ciclul de la rezultatele cercetării la inovare, dezvoltare și punerea în aplicare cu succes, reducând în același timp costurile de dezvoltare, testare și validare.

Spațiul nostru european de cercetare este, prin însăși natura sa, colaborativ și, prin urmare, permeabil la ingerințele străine și la dezinformare. În urma adoptării recomandării Consiliului privind securitatea cercetării[30], Comisia și statele membre iau măsuri pentru a capacita actorii relevanți, printre altele prin înființarea unui centru de expertiză privind securitatea cercetării.

Acțiuni-cheie

Comisia va adopta:

- **o propunere legislativă pentru a transforma Europol într-o agenție de aplicare a legii cu adevărat operațională în 2026;**
- **o propunere legislativă pentru a consolida Eurojust în 2026;**
- **o propunere legislativă pentru a consolida rolul și sarcinile Frontex în 2026;**
- **o propunere legislativă pentru a institui un sistem european de comunicații critice în 2026.**

Comisia:

- **va prezenta, în 2025, o foaie de parcurs care va stabili calea de urmat în ceea ce privește accesul legal și efectiv la date pentru asigurarea respectării legii;**
- **va elabora, în 2025, o evaluare a impactului în vederea actualizării normelor privind păstrarea datelor la nivelul UE, după caz;**
- **va prezenta, în 2026, o foaie de parcurs tehnologică privind criptarea pentru a identifica și a evalua soluțiile tehnologice care să permită accesul legal la date al autorităților de aplicare a legii;**
- **va depune eforturi în vederea creării unui grup la nivel înalt pentru consolidarea cooperării operaționale în materie de asigurare a respectării legii;**
- **va crea, în 2026, un Campus de cercetare și inovare în domeniul securității în cadrul Centrului său Comun de Cercetare.**

Comisia, în cooperare cu statele membre și cu agențiile relevante ale UE:

- **va consolida arhitectura EMPACT;**
- **va depune eforturi în vederea implementării rapide a arhitecturii de interoperabilitate și a punerii în aplicare a Regulamentului Prüm II;**
- **va consolida cadrul referitor la informațiile privind călătoriile.**

Statele membre sunt invitate:

[29] Centrul european de inovare pentru securitatea internă | Europol.
[30] JO C/2024/3510, 30.5.2024.

- **să transpună și să pună în aplicare pe deplin Directiva privind schimbul de informații.**

4. Reziliența împotriva amenințărilor hibride și a altor acte ostile

Vom consolida reziliența împotriva amenințărilor hibride prin îmbunătățirea protecției infrastructurii critice, prin consolidarea securității cibernetice, prin securizarea nodurilor de transport și a porturilor și prin combaterea amenințărilor online.

Frecvența și gradul de sofisticare a actelor ostile care subminează securitatea UE au crescut, actorii răuvoitori extinzându-și în mod semnificativ arsenalul. Campaniile hibride care vizează UE, statele sale membre și partenerii săi s-au intensificat, incluzând acte de sabotaj care vizează infrastructura critică, incendieri, atacuri cibernetice, ingerințe electorale, acțiuni străine de manipulare a informațiilor și ingerințe străine (FIMI), inclusiv dezinformarea, precum și utilizarea migrației ca armă. Având în vedere rolul lor politic și operațional și natura informațiilor pe care le gestionează, instituțiile, organele, oficiile și agențiile Uniunii („entitățile Uniunii") nu sunt scutite.

UE trebuie să **își sporească reziliența**, să utilizeze instrumentele actuale în mod eficace și să dezvolte noi modalități de a face față acestor amenințări în continuă evoluție generate de actori statali și nestatali, atât în prezent, cât și în viitor.

Infrastructura critică

Amenințările la adresa **infrastructurii critice**, inclusiv amenințările hibride, cum ar fi sabotajul și activitățile cibernetice răuvoitoare, reprezintă o preocupare majoră, în special în ceea ce privește infrastructura care conectează statele membre – fie interconexiunile energetice, fie cablurile de comunicații transfrontaliere, precum și transporturile. De la războiul de agresiune al Rusiei împotriva Ucrainei, actele de sabotaj care vizează infrastructura critică au crescut, în special în 2024, afectând numeroase state membre. Cooperarea dintre autoritățile de aplicare a legii, serviciile de securitate și de securitate cibernetică, serviciile militare și de protecție civilă și operatorii privați este esențială pentru a anticipa, a detecta, a preveni și a răspunde în mod eficace la astfel de acte.

Reducerea vulnerabilităților și consolidarea rezilienței entităților critice sunt imperative pentru a asigura furnizarea neîntreruptă a serviciilor esențiale vitale pentru economie și societate. Transpunerea la timp și punerea corectă în aplicare de către toate statele membre a **Directivei privind reziliența entităților critice (CER)**[31] și a **Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2)**[32] sunt, prin urmare, esențiale în această privință.

Pentru a asigura progrese rapide, Comisia va sprijini statele membre în identificarea entităților critice[33] și în schimbul de bune practici privind strategiile naționale și evaluările riscurilor în ceea ce privește serviciile esențiale, în cooperare cu **Grupul privind reziliența entităților critice și cu Grupul de cooperare NIS**. În cazul în care apar perturbări ale infrastructurii critice cu impact transfrontalier semnificativ, **Planul de acțiune al UE privind infrastructura critică**

[31] Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului.

[32] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

[33] Sectoarele vizate de directivă sunt energia, transporturile, sectorul bancar, infrastructura pieței financiare, sănătatea, apa potabilă, apele uzate, infrastructura digitală, administrația publică, spațiul, producția, prelucrarea și distribuția de alimente.

va coordona răspunsurile la nivelul UE. Comisia încurajează Consiliul să adopte rapid **Planul de acțiune al UE în domeniul cibernetic,** care va consolida și mai mult coordonarea în contextul gestionării crizelor, facilitând o colaborare mai strânsă între autorități în ceea ce privește reziliența fizică și digitală. În urma testelor de rezistență efectuate cu succes în sectorul energetic în 2023, Comisia va promova **teste de rezistență voluntare** în alte sectoare-cheie pentru securitatea internă. În plus, Comisia va oferi o **imagine de ansamblu la nivelul Uniunii a riscurilor transfrontaliere și transsectoriale** pentru serviciile esențiale, pentru a sprijini evaluările riscurilor efectuate de statele membre și pentru a contribui la o evaluare cuprinzătoare a riscurilor la nivelul UE. În conformitate cu Strategia privind o Uniune a pregătirii, Comisia va colabora cu statele membre pentru a identifica și alte sectoare și servicii care nu intră sub incidența legislației actuale și pentru care ar putea exista necesitatea de a se lua măsuri.

Grupul operativ UE-NATO privind reziliența infrastructurii critice a promovat o cooperare excelentă în ceea ce privește schimbul de bune practici și sporirea rezilienței în sectoarele energiei, transporturilor, infrastructurii digitale și spațiului. Această activitate va continua în cadrul **dialogului structurat UE-NATO privind reziliența**. **Setul de instrumente al UE pentru contracararea amenințărilor hibride** oferă un sprijin solid statelor membre și partenerilor în ceea ce privește pregătirea pentru amenințările hibride și contracararea acestora. **Echipele de răspuns rapid în caz de amenințări hibride**[34] oferă, la cerere, asistență personalizată pe termen scurt statelor membre, diferitelor misiuni ale UE și partenerilor. În plus, Comisia va continua cooperarea UE în ceea ce privește combaterea sabotajului prin activități ale experților[35], inclusiv un **program de lucru comun dedicat** pentru ca experții să simplifice schimbul de informații și să cartografieze contramăsurile.

Incidentele care afectează **cablurile submarine** din Europa evidențiază necesitatea unor măsuri mai ferme și a unor răspunsuri mai clare. Astfel cum se subliniază în **Planul de acțiune al UE privind securitatea cablurilor**[36], Comisia, împreună cu Înaltul Reprezentant, va colabora cu statele membre, cu agențiile UE și cu parteneri precum NATO pentru a preveni, a detecta, a răspunde și a descuraja amenințările la adresa cablurilor submarine. Pentru a elabora un tablou situațional integrat al amenințărilor, Comisia va colabora cu statele membre pentru a dezvolta și a implementa, în mod voluntar, un mecanism integrat de supraveghere a cablurilor submarine pentru fiecare bazin maritim, începând cu un nod regional nordic/baltic.

Securitatea cibernetică

Caracterul persistent al **activităților cibernetice răuvoitoare**, care face adesea parte dintr-o gamă mai largă de amenințări multidimensionale și hibride, necesită o atenție și acțiuni continue la nivel european. În ultimii ani, Uniunea a adoptat o serie de acte cu putere de lege în domeniul securității cibernetice care consolidează reziliența cibernetică a entităților NIS2 cu activități în sectoare critice ale UE, precum și a entităților Uniunii[37], îmbunătățesc securitatea produselor digitale (Regulamentul privind reziliența cibernetică) și stabilesc un cadru pentru sprijinirea pregătirii și a răspunsului la incidente (Regulamentul privind solidaritatea cibernetică). În ianuarie 2025, Comisia a adoptat **Planul de acțiune european privind securitatea cibernetică**

[34] Busola strategică a UE pentru securitate și apărare 2022, p. 22.
[35] Consilierii UE în materie de protecție a securității, rețeaua europeană de eliminare a dispozitivelor explozive (EEODN), rețeaua ATLAS, Rețeaua UE de securitate pentru protecția spațiilor publice cu risc ridicat (EU HRSN), Grupul consultativ pentru securitate CBRN, Grupul privind reziliența entităților critice (CERG).
[36] JOIN(2025) 9 final.
[37] Regulamentul (UE, Euratom) 2023/2841 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în instituțiile, organele, oficiile și agențiile Uniunii, JO L, 2023/2841, 18.12.2023.

a spitalelor și a furnizorilor de asistență medicală[38] pentru a îmbunătăți detectarea amenințărilor, pregătirea pentru acestea și răspunsul în situații de criză. Punerea sa deplină în aplicare este esențială. În același timp, pentru a aborda noile amenințări și evoluții, trebuie să ne intensificăm acțiunile, în special în domeniul schimbului de informații, al securității lanțului de aprovizionare, al atacurilor cibernetice și de tip ransomware, precum și al suveranității tehnologice.

În plus, punerea în aplicare necesită acoperirea deficitului actual de competențe în domeniul securității cibernetice de 299 000 de persoane. Comisia va colabora cu statele membre în cadrul Uniunii competențelor[39] pentru a extinde forța de muncă din domeniul securității cibernetice, în special prin utilizarea noii Academii de competențe în materie de securitate cibernetică. Planul strategic pentru educația în domeniul STEM[40] contribuie la îmbunătățirea fluxului de talente și a răspunsului Europei la nevoile pieței forței de muncă în materie de securitate cibernetică.

În paralel cu sporirea rezilienței sale, UE va continua să utilizeze pe deplin cadrul privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare (**setul de instrumente pentru diplomația cibernetică**) pentru a preveni, a descuraja și a răspunde la amenințările cibernetice generate de actori statali și nestatali.

Securitatea lanțurilor de aprovizionare TIC

Setul de instrumente pentru securitatea cibernetică a rețelelor 5G oferă cadrul relevant pentru protejarea rețelelor 5G, dar, în prezent, este insuficient pus în aplicare de statele membre. Persistă riscuri inacceptabile în materie de securitate, în special în ceea ce privește înlocuirea furnizorilor cu grad ridicat de risc. O abordare armonizată a securității lanțului de aprovizionare TIC poate remedia fragmentarea actuală a pieței interne cauzată de abordările diferite la nivel național, poate evita dependențele critice și poate reduce riscul reprezentat de furnizorii cu grad ridicat de risc pentru lanțurile noastre de aprovizionare TIC, securizând astfel infrastructura noastră critică.

În concordanță cu această abordare, în viitoarea **revizuire a Regulamentului privind securitatea cibernetică**, Comisia va analiza în sens mai larg securitatea și reziliența lanțurilor de aprovizionare TIC și a infrastructurii TIC. În plus, Comisia va propune îmbunătățirea **cadrului european de certificare a securității cibernetice**, pentru a se asigura că viitoarele sisteme de certificare pot fi adoptate în timp util și pot răspunde nevoilor în materie de politici.

Pe baza evaluărilor sectoriale existente sau în curs[41], Comisia va elabora, împreună cu statele membre, o **planificare strategică pentru evaluări coordonate ale riscurilor în materie de securitate cibernetică**.

Serviciile cloud și de telecomunicații au devenit un element de bază în lanțurile de aprovizionare ale infrastructurilor critice, ale întreprinderilor și ale autorităților publice. Comisia va lua măsuri pentru a încuraja entitățile critice să aleagă **servicii cloud și de telecomunicații care oferă un nivel adecvat de securitate cibernetică**, ținând seama nu numai de riscurile tehnice, ci și de riscurile și dependențele strategice.

[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.
[41] Cum ar fi rețelele 5G, telecomunicațiile, energia electrică, energia din surse regenerabile și vehiculele conectate.

Atacuri cibernetice și de tip ransomware

O provocare majoră persistentă în UE și la nivel mondial este **ransomware**, un raport estimând un cost anual global de peste 250 de miliarde EUR până în 2031[42]. Atât **Directiva NIS 2**, cât și **Regulamentul privind reziliența cibernetică** vor îmbunătăți în mod semnificativ poziția de securitate a entităților, făcând mai costisitoare desfășurarea atacurilor de către rețelele ransomware. În plus, Comisia va colabora îndeaproape cu statele membre pentru a se asigura că mai multe atacuri de tip ransomware, în special amenințările persistente avansate, și plățile de răscumpărare sunt raportate autorităților de aplicare a legii, facilitând investigațiile.

Pentru a preveni și a opri atacurile cibernetice, UE trebuie să consolideze schimbul de informații dintre autoritățile de aplicare a legii, autoritățile și entitățile din domeniul securității cibernetice, precum și părțile private, sub egida Europol și a Agenției UE pentru Securitate Cibernetică (ENISA).

Europol și Eurojust ar trebui să continue să se bazeze pe realizările pe care le-au obținut în ceea ce privește eliminarea operațiunilor ransomware, sprijinind cooperarea în materie de asigurare a respectării legii. În acest scop, autoritățile de aplicare a legii ar trebui să maximizeze utilizarea mecanismelor de cooperare, inclusiv a **modelului internațional de răspuns la ransomware al Europol** și a **Inițiativei internaționale de combatere a atacurilor de tip ransomware (*Counter Ransomware Initiative* – CRI)**[43], iar ENISA și Europol ar trebui să coopereze pentru a extinde colecția de instrumente de decriptare pentru tipurile de atac de tip ransomware[44].

Suveranitatea tehnologică

Securitatea cibernetică și suveranitatea tehnologică sunt strâns legate între ele, iar dependențele tehnologice trebuie abordate cu prioritate. Uniunea trebuie **să orienteze dezvoltarea și implementarea de noi tehnologii**, Comisia depunând eforturi pentru a **consolida capabilitățile în domeniul tehnologiilor strategice**, cum ar fi IA, tehnologiile cuantice, conectivitatea avansată, tehnologia de tip cloud, edge și internetul obiectelor[45], prin intermediul unor inițiative viitoare, cum ar fi Planul de acțiune continental privind IA, Strategia privind tehnologiile cuantice și altele[46]. Comisia va continua să sprijine implementarea în timp util a celor mai recente **protocoale de internet** convenite la nivel internațional, care sunt esențiale pentru menținerea unui internet scalabil și eficient, cu un nivel sporit de securitate cibernetică. De asemenea, sunt necesare acțiuni suplimentare pentru a aborda **provocările legate de spectrul de frecvențe radio,** cum ar fi cele legate de spoofing-ul GNSS, bruiaj, riscurile și dependențele lanțului de aprovizionare, cum ar fi utilizarea tehnologiilor de detectare cuantică și explorarea dezvoltării capacității de monitorizare a frecvențelor radio.

Implementarea soluțiilor de **criptografie postcuantică** (*post-quantum cryptography* – PQC) va fi esențială pentru protejarea comunicațiilor sensibile, a datelor în repaus și pentru protejarea identităților digitale în noua eră cuantică. Pe baza Recomandării din 2024 privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către PQC[47], Comisia colaborează cu statele membre pentru a promova această tranziție. În acest sens, statele membre ar trebui să

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Disponibilă prin intermediul proiectului „No More Ransom", https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] De exemplu, EuropHPC JU https://eurohpc-ju.europa.eu/index_en, inițiativa emblematică privind tehnologiile cuantice (Quantum Flagship) pagina principală a Quantum Flagship | Quantum Flagship, rețelele 3C [COM(2024) 81 final] și Planul de acțiune al UE privind securitatea cablurilor [JOIN(2025) 9 final].
[47] Recomandare privind o foaie de parcurs coordonată pentru punerea în aplicare a tranziției către criptografia postcuantică | Conturarea viitorului digital al Europei.

identifice cazurile cu grad ridicat de risc din entitățile critice și să asigure criptarea sigură din punct de vedere cuantic pentru aceste cazuri cu risc ridicat cât mai curând posibil și nu mai târziu de sfârșitul anului 2030. De asemenea, Comisia colaborează cu statele membre și cu Agenția Spațială Europeană (ESA) pentru a dezvolta și implementa **infrastructura europeană de comunicații cuantice (EuroQCI)**[48], bazată pe distribuția cuantică a cheilor (Quantum Key Distribution – QKD), în cadrul **IRIS²**, Programul UE privind conectivitatea securizată. Ambele inițiative vor permite, în cele din urmă, entităților să transmită date și să stocheze informații în condiții de siguranță.

Tehnologiile cuantice vor juca, de asemenea, un rol esențial în aplicațiile de securitate: o **foaie de parcurs pentru detectarea cuantică în aplicațiile de securitate** va fi elaborată ca parte a **Strategiei privind tehnologiile cuantice**. În aceeași ordine de idei, Comisia depune eforturi pentru a-și proteja din punct de vedere cuantic sistemele corporative critice pentru securitate, inclusiv sistemele informatice clasificate.

Un cadru de securitate cibernetică favorabil întreprinderilor

Viitoarea revizuire a Regulamentului privind securitatea cibernetică reprezintă o oportunitate de a **simplifica legislația UE în materie de securitate cibernetică,** în conformitate cu Busola pentru competitivitate. Comisia va colabora îndeaproape cu statele membre pentru a asigura o punere în aplicare rapidă, coerentă și favorabilă întreprinderilor a cadrului orizontal de securitate cibernetică prevăzut în Directiva NIS 2, în Regulamentul privind reziliența cibernetică și în Regulamentul privind solidaritatea cibernetică, promovând simplitatea și coerența și evitând fragmentarea sau dublarea normelor în materie de securitate cibernetică în legislația UE și în legislațiile naționale.

Pentru a permite accesul securizat la serviciile online și pentru a consolida securitatea digitală în întreaga UE, **cadrul european al identității digitale** va oferi tuturor cetățenilor și rezidenților UE portofele pentru identitatea digitală de încredere înainte de sfârșitul anului 2026. Viitorul **portofel al întreprinderilor europene** va facilita interacțiuni transfrontaliere sigure între întreprinderi și administrațiile publice. Ambele sunt condiții prealabile pentru funcționarea sigură și mai eficientă a pieței unice bazate pe date, cu instrumente precum portalul digital unic, facturarea electronică, achizițiile publice electronice și pașaportul digital al produsului.

Securitatea online

Unele dintre cele mai grave amenințări hibride care pun în pericol securitatea și siguranța persoanelor din Europa și care vizează sfera democratică a UE au loc online. Printre aceste amenințări se numără activitățile ilegale și conținutul ilegal online, manipularea informațiilor care implică amplificarea artificială, informațiile înșelătoare și acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI).

Aplicarea riguroasă a **Regulamentului privind serviciile digitale (*Digital Services Act* – DSA)** este esențială pentru a asigura un mediu online sigur și accesibil, cu actori responsabili, care să fie rezilient și la amenințările hibride. DSA obligă furnizorii de platforme online foarte mari și de motoare de căutare online foarte mari să efectueze evaluări ale riscurilor și să instituie măsuri de atenuare a riscurilor sistemice care decurg din proiectarea, funcționarea sau utilizarea serviciilor lor. Astfel de riscuri pot include efecte negative asupra discursului civic și a proceselor electorale, precum și asupra securității publice, cum ar fi ingerințele de proporții ale unor actori statali străini răuvoitori, de exemplu în procesele electorale. Este importantă formarea autorităților competente ale statelor membre cu privire la utilizarea instrumentelor

[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

juridice pentru eliminarea promptă a conținutului ilegal online, în special în ceea ce privește violența cibernetică pe criterii de gen. DSA prevede un mecanism de răspuns în situații de criză, care poate fi activat în cazul în care circumstanțe extraordinare dau naștere unei amenințări grave la adresa siguranței publice sau a sănătății publice în Uniune sau în părți semnificative ale teritoriului acesteia. Pentru a completa acest mecanism, Comisia și autoritățile naționale competente desemnate drept coordonatori ai serviciilor digitale au elaborat, de asemenea, un cadru voluntar de răspuns la incidente în temeiul **DSA**. Coordonatorii serviciilor digitale au luat, de asemenea, măsuri pentru a contribui la protejarea integrității alegerilor, de exemplu prin organizarea de mese rotunde electorale și de teste de rezistență[49]. DSA, împreună cu Regulamentul privind publicitatea politică[50], oferă una dintre componentele legate de protejarea democrației și a integrității proceselor democratice, care sunt vulnerabile la atacurile unor actori ostili, inclusiv prin intermediul instrumentelor digitale și pe platformele de comunicare socială.

Punerea în aplicare a setului de instrumente **FIMI** este o altă componentă importantă care oferă un sprijin esențial la nivelul UE. Susținerea alfabetizării digitale și mediatice și a gândirii critice sunt, de asemenea, esențiale pentru aceste eforturi[51].

Contracararea utilizării migrației ca armă

Cu ajutorul și sprijinul decisiv al Belarusului, Rusia a utilizat în mod intenționat migrația ca armă și a facilitat ilegal fluxurile de migrație către frontierele externe ale UE, cu scopul de a destabiliza societățile noastre și de a submina unitatea Uniunii Europene. Acest lucru pune în pericol nu numai securitatea națională și suveranitatea statelor membre, ci și siguranța și integritatea spațiului Schengen și securitatea Uniunii în ansamblu. În concluziile sale din octombrie 2024, Consiliul European a subliniat că nu li se poate permite Rusiei și Belarusului sau vreunei alte țări să abuzeze de valorile noastre, inclusiv de dreptul la azil, și nici să ne submineze democrația.

Astfel cum se menționează în Comunicarea Comisiei din 2024 privind utilizarea migrației ca armă, pe lângă un puternic sprijin politic, Uniunea a luat măsuri financiare, operaționale și diplomatice, inclusiv cooperarea cu țările de origine și de tranzit, pentru a răspunde în mod eficace acestor amenințări[52]. Acest răspuns implică utilizarea noului cadru instituit de Consiliu pentru a sancționa persoanele și organizațiile implicate în acțiuni și politici precum utilizarea migrației ca armă de către Rusia, prin impunerea înghețării activelor și a interdicțiilor de călătorie[53]. UE va continua să utilizeze acest cadru, atunci când este necesar, și să sprijine statele membre în contracararea acestei amenințări.

Securitatea transporturilor

Porturile maritime, aeroporturile și infrastructura terestră sunt puncte de intrare și ieșire esențiale. Ele joacă un rol vital în economia și societatea UE și sunt esențiale pentru mobilitatea militară. Totuși, aceste noduri și mijloace de transport sunt, de asemenea, ținte principale ale amenințărilor externe și ale activităților infracționale. Incidentele recente, inclusiv încălcările securității transportului aerian de marfă și atacurile asupra infrastructurii feroviare, evidențiază riscurile grave. **Operatorii de transport** pot fi atât ținte, cât și instrumente pentru actorii

[49] Setul de instrumente pentru alegeri pentru coordonatorii serviciilor digitale 2025, elaborat în temeiul DSA https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.

[50] Regulamentul (UE) 2024/900 al Parlamentului European și al Consiliului din 13 martie 2024 privind transparența și vizarea unui public-țintă în publicitatea politică, JO L, 2024/900, 20.3.2024.

[51] Planul de acțiune pentru educația digitală (2021-2027) – Spațiul european al educației.

[52] COM(2024) 570 final.

[53] Regulamentul (UE) 2024/2642 al Consiliului din 8 octombrie 2024 privind măsuri restrictive având în vedere activitățile destabilizatoare ale Rusiei, ST/8744/2024/INIT, JO L, 2024/2642, 9.10.2024.

răuvoitori. Instrumentele juridice existente ale UE au consolidat securitatea aviației[54], însă, având în vedere nivelul ridicat de amenințare la adresa aviației civile, este necesar un mijloc de a prevedea incidentele și de a consulta rapid statele membre relevante. Comisia va colabora cu statele membre pentru a modifica legislația de punere în aplicare existentă în domeniul securității aviației în vederea schimbului de informații clasificate privind **evenimentele legate de securitatea aviației**. În plus, Comisia va lua în considerare **măsuri de reglementare** pentru a face față noilor amenințări, cum ar fi **incidentele legate de transportul aerian de marfă**, și pentru a consolida standardele de securitate a aviației. Acest lucru va implica, de asemenea, consolidarea **legislației privind securitatea aviației (AVSEC)** pentru a permite măsuri de răspuns imediat, menținând în același timp zona de control unic de securitate în aeroporturile din UE.

La elaborarea viitoarei **strategii portuare a UE**, pe baza **Alianței portuare a UE**, Comisia va explora modalități de a consolida în continuare legislația în materie de securitate maritimă pentru a aborda în mod eficace amenințările emergente, a securiza porturile și a spori securitatea lanțului de aprovizionare al UE. În acest scop, Comisia va asigura o punere în aplicare fermă a acesteia și va depune eforturi pentru armonizarea practicilor naționale și consolidarea verificărilor antecedentelor în porturi. Pe lângă protocoalele de securitate stabilite pentru transportul aerian de marfă, Comisia va colabora cu statele membre și cu sectorul privat pentru a extinde aceste protocoale în vederea securizării lanțurilor de transport maritim.

Autoritatea vamală a UE propusă va analiza și va evalua riscurile pe baza **informațiilor vamale** referitoare la mărfurile care intră, ies și tranzitează UE pentru a sprijini statele membre în prevenirea exploatării lanțurilor de aprovizionare internaționale de către actori răuvoitori. În conformitate cu Strategia UE în materie de securitate maritimă[55], viitorul **Pact european privind oceanele** va juca un rol esențial în consolidarea securității maritime în bazinele maritime din jurul UE și din afara acesteia, inclusiv prin încurajarea intensificării operațiunilor și exercițiilor maritime cu scopuri multiple.

Reziliența lanțurilor de aprovizionare

Europa trebuie să își reducă dependența de tehnologiile din țările terțe, ceea ce poate duce la dependență și la riscuri de securitate. Comisia urmărește să atenueze dependențele de furnizori străini unici, să reducă riscul reprezentat de furnizorii cu grad ridicat de risc pentru lanțurile noastre de aprovizionare și să asigure infrastructura critică și capacitatea industrială pe teritoriul UE, astfel cum se specifică în **Busola pentru competitivitate[56]** și în **Pactul pentru o industrie curată[57]**. Comisia va promova o **politică industrială pentru securitatea internă** prin colaborarea cu industriile UE din sectoare-cheie (de exemplu, noduri de transport, infrastructuri critice) pentru a produce soluții de securitate, cum ar fi echipamentele de detectare, tehnologiile biometrice și dronele, încorporând caracteristici de securitate din momentul conceperii. În **revizuirea normelor UE privind achizițiile publice**, Comisia va evalua dacă considerentele de securitate din Directiva din 2009 privind achizițiile publice în domeniile apărării și securității[58] sunt suficiente pentru a răspunde nevoilor de asigurare a respectării legii și de reziliență a entităților critice.

[54] Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile, JO L 97, 9.4.2008, p. 72.
[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Directiva 2009/81/CE privind coordonarea procedurilor privind atribuirea anumitor contracte de lucrări, de furnizare de bunuri și de prestare de servicii de către autoritățile sau entitățile contractante în domeniile apărării și securității, JO L 216, 20.8.2009.

Comisia va sprijini statele membre în **examinarea investițiilor străine directe (ISD)** și a achizițiilor de echipamente pentru centrele logistice, asigurându-se că tehnologia și infrastructura critică rămân sigure.

Odată intrat în vigoare, **Regulamentul privind situațiile de urgență pe piața internă și reziliența pieței interne (IMERA)** va ajuta UE să gestioneze crizele care perturbă lanțurile de aprovizionare critice și libera circulație a bunurilor, a serviciilor și a persoanelor. El va permite coordonarea rapidă în situații de criză, identificarea bunurilor și serviciilor relevante în situații de criză și va oferi un set de instrumente pentru a asigura disponibilitatea acestora. În plus, în strânsă cooperare cu statele membre, Comisia va propune instituirea **unui mecanism multiinstituțional de alertă în materie de securitate a transporturilor și a lanțului de aprovizionare** pentru a garanta schimbul securizat și în timp util de informații relevante necesare pentru a anticipa și a contracara amenințările.

În plus, odată cu punerea în aplicare a Actului privind materiile prime critice și a Regulamentului privind industria care contribuie la obiectivul zero emisii nete, utilizarea sporită a criteriilor europene privind durabilitatea, reziliența și preferința în achizițiile publice ale UE va încuraja dezvoltarea piețelor-pilot. Consolidarea legăturilor comerciale, de exemplu prin parteneriate pentru materii prime și parteneriate pentru comerț și investiții curate, va contribui la diversificarea lanțurilor de aprovizionare.

Reziliența și pregătirea pentru amenințările chimice, biologice, radiologice și nucleare

Războiul de agresiune al Rusiei împotriva Ucrainei a sporit riscul de **amenințări chimice, biologice, radiologice și nucleare (CBRN)**. Pentru a aborda potențiala achiziționare și utilizare ca armă a materialelor CBRN, Comisia va sprijini statele membre și țările partenere prin formare și exerciții specifice. Comisia va stimula, de asemenea, capacitățile de pregătire și de răspuns în domeniul CBRN, prin stabilirea priorităților în materie de amenințări, finanțarea inovării pentru contramăsuri, capacitățile rescEU și constituirea de stocuri de contramăsuri medicale, sub egida unui nou **plan de acțiune în materie de pregătire și răspuns în domeniul CBRN**. În plus, **Strategia UE privind contramăsurile medicale** va sprijini dezvoltarea de contramăsuri medicale de la cercetare la producție și distribuție pentru a proteja UE de pandemii și amenințări CBRN.

Bazându-se pe experiența pandemiei de COVID-19, UE a consolidat cadrul de securitate sanitară[59]. Comisia desemnează laboratoare de referință ale UE în domeniul sănătății publice pentru a consolida capacitățile de supraveghere și de detectare rapidă la nivelul UE și la nivel național. În 2025 va fi publicat un plan al Uniunii privind pregătirea, prevenirea și răspunsul în materie de securitate sanitară.

Acțiuni-cheie

Comisia:

- **va reexamina și revizui, în 2025, Regulamentul privind securitatea cibernetică;**
- **va elabora măsuri pentru a asigura utilizarea în condiții de securitate cibernetică a serviciilor de cloud;**
- **va propune, în 2025, o strategie portuară a UE;**
- **va revizui, în 2026, normele UE privind achizițiile publice în domeniile apărării și securității;**
- **va prezenta, în 2026, un nou plan de acțiune în materie de pregătire și răspuns în domeniul CBRN.**

[59] În special prin Regulamentul (UE) 2022/2371 privind amenințările transfrontaliere grave pentru sănătate.

Comisia, în cooperare cu statele membre:

- **va dezvolta și implementa infrastructura europeană de comunicații cuantice (EuroQCI);**
- **va asigura punerea efectivă în aplicare a Regulamentului privind serviciile digitale;**
- **va depune eforturi pentru a contracara utilizarea migrației ca armă;**
- **va institui un sistem al evenimentelor de securitate a aviației;**
- **va depune eforturi pentru a institui un mecanism multiinstituțional de alertă în materie de securitate a transporturilor și a lanțului de aprovizionare.**

Consiliul este invitat:

- **să adopte recomandarea Consiliului privind Planul de acțiune al UE în domeniul cibernetic.**

Statele membre sunt invitate:

- **să transpună și să pună în aplicare pe deplin directivele CER și NIS 2.**

5. Înăsprirea normelor pentru formele grave de criminalitate organizată

Vom contribui la eradicarea criminalității organizate propunând norme mai stricte pentru a combate rețelele de criminalitate organizată, inclusiv în ceea ce privește investigațiile, pentru a reduce vulnerabilitatea tinerilor din UE la recrutarea în scopuri infracționale și pentru a intensifica măsurile de blocare a accesului la instrumente și active infracționale.

Criminalitatea organizată exploatează un peisaj în continuă evoluție și proliferează exponențial. Ea beneficiază de tehnologii avansate, este activă în mai multe jurisdicții și are legături puternice dincolo de frontierele UE. Având în vedere aceste amenințări transnaționale complexe, coordonarea și sprijinul la nivelul UE sunt vitale.

Prevenirea criminalității

Recrutarea tinerilor în scopuri de criminalitate organizată reprezintă o preocupare tot mai mare în UE. Combaterea criminalității organizate necesită abordarea **cauzelor sale profunde** prin oferirea de educație și alternative la o viață de criminalitate printr-o abordare la nivelul întregii societăți. Comisia va sprijini integrarea considerentelor de securitate în politicile educaționale, sociale, de ocupare a forței de muncă și regionale ale UE. UE va **promova politici de prevenire a criminalității bazate pe dovezi**[60] și adaptate la contextele locale.

Pentru a-i proteja pe destinatarii serviciilor online, în special pe minori, împotriva, printre altele, a persoanelor care abuzează sexual de un copil, a traficanților de persoane și a recrutării online pentru infracțiuni sau extremism violent, măsurile prevăzute în **Regulamentul privind serviciile digitale** impun furnizorilor de platforme online accesibile minorilor să gestioneze riscurile și să acționeze împotriva conținutului ilegal, inclusiv a discursului de incitare la ură. Comisia intenționează să emită **orientări privind protecția minorilor**, pentru a ajuta furnizorii de platforme online să asigure un nivel ridicat de confidențialitate, siguranță și securitate a minorilor în mediul online. Orientările vor conține un set de recomandări pentru toate serviciile digitale care își desfășoară activitatea în Uniune, pentru a spori protecția minorilor în mediul online. În 2025, Comisia intenționează, de asemenea, să faciliteze o soluție a UE de **verificare a vârstei care să protejeze viața privată**, ceea ce va acoperi lacunele până când portofelul EUDI va fi oferit la sfârșitul anului 2026. Comisia va prezenta, de asemenea, un plan de acțiune împotriva hărțuirii cibernetice.

[60] https://www.eucpn.org/.

În plus, Comisia va continua să sprijine colaborarea voluntară a mai multor părți interesate cu platformele online și cu alți actori relevanți, inclusiv prin intermediul Forumului UE pentru internet și al codurilor de conduită specifice în temeiul Regulamentului privind serviciile digitale, cum ar fi Codul de conduită din 2025 privind discursurile ilegale de incitare la ură din mediul online. Obiectivul este de a spori gradul de conștientizare, de a răspunde în comun la amenințările actuale și emergente și de a produce și a face schimb de bune practici pentru măsurile de atenuare.

La nivel local, impactul criminalității organizate subliniază necesitatea adoptării unor soluții regionale pentru a reduce vulnerabilitatea și atractivitatea activităților ilegale. Agenda UE pentru orașe va aborda provocările în materie de securitate din orașe, pe baza inițiativei „Orașele UE împotriva radicalizării”. Comisia va sprijini statele membre în consolidarea securității urbane și regionale prin intermediul Fondului european de dezvoltare regională**.**

Existența unor fundamente educaționale și a unor competențe mai puternice stă la baza unor societăți reziliente și bazate pe coeziune. Prin intermediul **Uniunii competențelor** și al **Planului de acțiune privind integrarea și incluziunea**, Uniunea va depune eforturi pentru a ajuta oamenii să devină mai rezilienți la informarea greșită și la dezinformare, la radicalizare și la recrutarea în scopuri infracționale.

Protejarea copiilor împotriva tuturor formelor de violență, inclusiv a infracțiunilor, a violenței fizice sau mentale, atât online, cât și offline, este un obiectiv central al UE. Pentru a răspunde nevoilor specifice ale grupurilor deosebit de vulnerabile, cum ar fi copiii, care sunt tot mai expuși recrutării și radicalizării, racolării în scopuri sexuale (*grooming*) și abuzului sexual asupra copiilor, hărțuirii cibernetice, dezinformării și altor amenințări, UE va elabora un **plan de acțiune privind protecția copiilor împotriva criminalității**, care să cuprindă dimensiunile online și offline. Acest plan va stabili o abordare coerentă și coordonată, bazată pe cadrele și instrumentele disponibile, inclusiv pe viitorul Centru al UE pentru prevenirea și combaterea abuzului sexual asupra copiilor și pe alte organisme și agenții ale UE, și va propune căi de urmat în cazul în care persistă lacune.

Dezmembrarea rețelelor infracționale și perturbarea activității facilitatorilor acestora

Trebuie intensificată lupta împotriva rețelelor infracționale cu grad ridicat de risc, a liderilor și a facilitatorilor acestora. Deși succesele recente sunt notabile[61], normele depășite și definițiile inconsecvente ale rețelelor infracționale împiedică un răspuns eficace în materie de justiție penală și cooperarea transfrontalieră. Comisia va revizui legislația depășită din acest domeniu, propunând un **cadru juridic reînnoit privind criminalitatea organizată** pentru a consolida răspunsul.

Aplicarea administrativă poate completa asigurarea respectării legii pentru a obține rezultate mai rapide – astfel cum au arătat EPPO și Oficiul European de Luptă Antifraudă (OLAF) în ceea ce privește combaterea **fraudei transfrontaliere și a infracțiunilor împotriva intereselor financiare ale UE**. Autorii fraudelor în materie de subvenții se concentrează asupra unor sectoare precum energia din surse regenerabile, programele de cercetare și sectorul agricol[62]. Comisia va explora modalități de coordonare a utilizării instrumentelor penale și administrative, consolidând cooperarea cu Europol, Eurojust și EPPO. De asemenea, Comisia va continua să sprijine aplicarea pe scară mai largă a **abordării administrative** pentru a abilita

[61] Inclusiv cazurile EMPACT recente.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

autoritățile administrative locale și alte autorități administrative să perturbe infiltrarea grupărilor de criminalitate organizată[63].

UE lucrează la consolidarea cadrului său juridic pentru combaterea **corupției**[64]. Parlamentul European și Consiliul ar trebui să încheie rapid negocierile privind cadrul anticorupție actualizat propus de Comisie. Comisia va prezenta o strategie anticorupție a UE pentru a promova integritatea și pentru a consolida coordonarea între toate autoritățile și părțile interesate relevante în acest domeniu.

Armele de foc reprezintă un factor-cheie al intensificării violenței comise de grupurile infracționale organizate. Comisia va propune standarde comune de drept penal privind traficul ilicit de arme de foc. Un nou **Plan de acțiune al UE privind traficul de arme de foc** se va concentra pe protejarea pieței licite, pe reducerea activităților infracționale, pe baza unor informații mai bune și pe consolidarea cooperării internaționale, cu un accent deosebit pe Ucraina și Balcanii de Vest.

Produsele pirotehnice comercializate ilegal, utilizate în infracțiuni, necesită măsuri de îmbunătățire a prevenirii și a trasabilității. În prezent, Comisia evaluează Directiva privind produsele pirotehnice și va lua în considerare, de asemenea, **sancțiuni penale pentru traficul de produse pirotehnice**.

Urmărirea banilor

Urmărirea banilor este esențială pentru combaterea criminalității organizate și a terorismului, dar rămâne foarte dificilă. Legătura dintre criminalitatea organizată și fluxurile de bani necesită eforturi intense și combinate pentru a opri accesul rețelelor infracționale la sursele de finanțare și pentru a proteja mai bine cetățenii, întreprinderile și bugetele publice.

UE și-a consolidat eforturile prin noile norme de combatere a spălării banilor, inclusiv prin înființarea **Autorității UE pentru Combaterea Spălării Banilor (ACSB)**[65]. Colaborarea dintre ACSB, OLAF, EPPO, Eurojust și Europol este esențială pentru desfășurarea unor investigații financiare eficace. Comisia va sprijini instituirea de **parteneriate**, atât cele care facilitează cooperarea dintre agenții, cât și cele care implică sectorul privat.

Pentru a elimina motivațiile financiare din spatele criminalității organizate, este esențial să se pună sechestru pe bunuri și să se confiște câștigurile obținute din săvârșirea de infracțiuni. Normele mai stricte adoptate recent privind **recuperarea și confiscarea activelor**[66] ar trebui transpuse fără întârziere de statele membre și utilizate la întregul lor potențial. Combaterea sistemelor financiare paralele care eludează cadrul UE de combatere a spălării banilor, inclusiv a sistemelor bazate pe criptoactive, necesită, de asemenea, acțiuni inovatoare, schimbul de bune practici între statele membre și un sprijin sporit din partea Europol și Eurojust. Comisia va analiza fezabilitatea unui nou sistem la nivelul UE de urmărire a profiturilor provenite din criminalitatea organizată și a finanțării terorismului și, de asemenea, va încuraja fluxurile de informații extinse și în timp util de la **unitățile de informații financiare** către autoritățile de aplicare a legii. Comisia va explora modalități de a elimina lacunele, va sprijini statele membre

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Propunere de directivă a Parlamentului European și a Consiliului privind combaterea corupției, de înlocuire a Deciziei-cadru 2003/568/JAI a Consiliului și a Convenției privind lupta împotriva corupției care implică funcționari ai Comunităților Europene sau funcționari ai statelor membre ale Uniunii Europene și de modificare a Directivei (UE) 2017/1371 a Parlamentului European și a Consiliului, COM(2023) 234 final, Bruxelles, 3.5.2023.

[65] https://www.amla.europa.eu/index_en.

[66] Directiva (UE) 2024/1260 a Parlamentului European și a Consiliului din 24 aprilie 2024 privind recuperarea și confiscarea activelor, JO L, 2024/1260, 2.5.2024.

în consolidarea capacităților și va continua să depună eforturi pentru consolidarea cooperării cu țările terțe utilizate în mod abuziv de infractori pentru operațiuni bancare subterane.

Combaterea infracțiunilor grave

Pe lângă dezmembrarea rețelelor infracționale, combaterea infracțiunilor grave necesită eforturi specifice. Pentru a ne consolida capacitatea de a combate **frauda online** – care cauzează prejudicii financiare foarte importante[67] – Comisia va sprijini măsurile de prevenire și acțiunile mai eficace de asigurare a respectării legii și va colabora cu statele membre și cu părțile interesate pentru a sprijini și a proteja victimele, inclusiv prin acordarea de asistență pentru recuperarea fondurilor acestora. Aceste eforturi vor fi formalizate într-un **plan de acțiune privind frauda online**.

Pe baza Strategiei UE de combatere a **abuzului sexual asupra copiilor**[68] pentru perioada 2020-2025, Comisia va sprijini colegiuitorii în finalizarea celor două propuneri legislative[69] de prevenire și combatere a abuzului sexual online asupra copiilor și de eficientizare a acțiunilor de asigurare a respectării legii împotriva abuzului sexual asupra copiilor și a exploatării sexuale a copiilor. Având în vedere că normele provizorii sunt în vigoare până în aprilie 2026, este esențial să se stabilească un cadru juridic permanent, iar Comisia încurajează colegiuitorii să înceapă negocierile privind proiectul de regulament de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor. Colegiuitorii sunt, de asemenea, invitați să înregistreze progrese în direcția negocierilor referitoare la Directiva privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a materialelor care conțin abuzuri sexuale asupra copiilor, care va stabili norme minime privind definirea infracțiunilor și a sancțiunilor în domeniul exploatării sexuale a copiilor.

Jumătate dintre cele mai periculoase rețele infracționale din UE sunt implicate în **traficul violent de droguri**. Deși UE și-a consolidat recent lupta împotriva acestei infracțiuni[70], în special prin extinderea mandatului **Agenției UE privind Drogurile**, sunt necesare acțiuni suplimentare. Comisia va lucra în strânsă cooperare cu statele membre pentru a propune o nouă **strategie a UE în materie de droguri**. De asemenea, Comisia va revizui **cadrul juridic privind precursorii de droguri** și va propune un **plan de acțiune al UE de combatere a traficului de droguri** pentru a perturba rutele și modelele de afaceri**. Parteneriatul public-privat al Alianței portuare a UE** privind consolidarea protecției portuare va fi extins pentru a include porturile mai mici și cele interioare și pentru a asigura respectarea normelor de securitate maritimă. Recunoscând impactul local grav al traficului de droguri, Comisia va continua să sprijine o politică în materie de droguri echilibrată, bazată pe dovezi și multidisciplinară, pregătită pentru afluxuri bruște de droguri, în special de opioide sintetice.

Pentru a combate exploatarea persoanelor, UE a adoptat norme noi[71] și va introduce o **strategie reînnoită a UE privind combaterea traficului de persoane** (2026-2030), care acoperă toate etapele, de la prevenire la urmărirea penală, cu accent pe sprijinirea victimelor atât la nivelul UE, cât și la nivel internațional.

În lupta împotriva **introducerii ilegale de migranți**, Comisia va coordona eforturile împreună cu partenerii-cheie prin intermediul noii Alianțe mondiale de combatere a introducerii ilegale de migranți, în cooperare cu Europol, Eurojust și Frontex, inclusiv în ceea ce privește

[67] Raportul global privind combaterea escrocheriei din 2024.
[68] COM(2020) 607 final.
[69] COM(2022) 209 final și COM(2024) 60 final.
[70] COM(2023) 641 final.
[71] Directiva (UE) 2024/1712 din 13 iunie 2024 de modificare a Directivei 2011/36/UE privind prevenirea și combaterea traficului de persoane și protejarea victimelor acestuia, JO L, 2024/1712, 24.6.2024.

dimensiunea online. Propunerile Comisiei privind combaterea introducerii ilegale de migranți[72] ar trebui adoptate și puse în aplicare fără întârziere. În plus, în urma adoptării **setului de instrumente privind operatorii de transport**[73], Comisia a intensificat comunicarea cu autoritățile și operatorii străini și va continua să colaboreze cu industria aviației și cu organizațiile aviației civile[74] pentru a spori gradul de conștientizare cu privire la introducerea ilegală de migranți pe calea aerului[75].

Infracțiunile împotriva mediului amenință mediul, sănătatea publică și economiile pe termen lung. Comisia va sprijini statele membre în punerea în aplicare a Directivei privind infracțiunile împotriva mediului[76] și va consolida rețelele operaționale și acțiunile în acest domeniu[77]. Asigurarea riguroasă a respectării normelor este esențială. În plus, Convenția Consiliului Europei privind protecția mediului prin intermediul dreptului penal[78], recent adoptată, va contribui la asigurarea unor eforturi puternice și comparabile de combatere a infracțiunilor împotriva mediului, atât în Europa, cât și în afara acesteia.

Răspunsul în materie de justiție penală

Criminalitatea și terorismul pot avea un impact asupra tuturor, astfel încât este esențial să se sprijine și să se protejeze drepturile **victimelor** pentru a reduce prejudiciile și a spori securitatea generală și încrederea în autorități. Pe baza Directivei privind drepturile victimelor, Comisia va introduce o nouă **strategie a UE privind drepturile victimelor**.

Sistemele de justiție penală ale UE au nevoie de instrumente eficace pentru a răspunde amenințărilor emergente. Pentru a realiza acest lucru, Comisia a lansat un **Forum la nivel înalt privind viitorul justiției penale a UE**. Acest forum reunește statele membre, Parlamentul European, agențiile și organele UE și alte părți interesate relevante. Obiectivul său este de a discuta modalități prin care să ne asigurăm că sistemele noastre de justiție penală rămân eficace, echitabile și reziliente în contextul provocărilor în continuă evoluție, consolidând în același timp cooperarea judiciară și sporind încrederea reciprocă, inclusiv prin digitalizare[79].

Acțiuni-cheie

Comisia:

- **va prezenta, în 2026, o propunere legislativă pentru norme modernizate privind criminalitatea organizată;**
- **va prezenta, în 2025, o propunere legislativă de revizuire a cadrului juridic privind precursorii de droguri;**

[72] COM(2023) 755 final și COM(2023) 754 final.
[73] Set de instrumente care abordează utilizarea mijloacelor comerciale de transport pentru a facilita migrația ilegală către UE.
[74] Inclusiv Organizația Aviației Civile Internaționale (OACI).
[75] Comisia va sprijini, de asemenea, finalizarea Regulamentului privind măsurile împotriva operatorilor de transport care facilitează sau se implică în traficul de persoane sau introducerea ilegală de migranți, COM(2021) 753 final.
[76] Directiva (UE) 2024/1203 a Parlamentului European și a Consiliului din 11 aprilie 2024 privind protecția mediului prin intermediul dreptului penal, JO L, 2024/1203, 30.4.2024.
[77] Rețeaua UE pentru punerea în aplicare și respectarea legislației din domeniul mediului (IMPEL), Rețeaua europeană a procurorilor pentru mediu (ENPE), EnviCrimeNet și Forumul UE al judecătorilor pentru mediu (EUFJE).
[78] Comitetul de experți pentru protecția mediului prin intermediul dreptului penal (PC-ENV) – Comitetul european pentru probleme penale.
[79] În special prin instituirea Comunicării în domeniul e-justiției prin intermediul schimbului online de date (*e-Justice Communication via Online Data Exchange* – eCODEX) și a Sistemului european de informații cu privire la cazierele judiciare ale resortisanților țărilor terțe (ECRIS-TCN).

- **va prezenta, în 2025, o propunere legislativă referitoare la standardele comune de drept penal privind traficul ilicit de arme de foc;**
- **va evalua necesitatea de a revizui directivele privind produsele pirotehnice și explozivii de uz civil;**
- **va evalua necesitatea de a consolida în continuare ordinul european de anchetă și mandatul european de arestare;**
- **va prezenta, în 2026, o nouă strategie a UE privind combaterea traficului de persoane;**
- **va prezenta, în 2026, o nouă strategie a UE privind drepturile victimelor;**
- **va prezenta, până în 2027, un plan de acțiune al UE privind protecția copiilor împotriva criminalității;**
- **va prezenta, în 2025, un plan de acțiune al UE de combatere a traficului de droguri;**
- **va prezenta, în 2026, un plan de acțiune al UE privind traficul de arme de foc;**
- **va extinde succesiv, începând cu 2025, Alianța portuară a UE;**
- **va adopta, în 2026, orientările DSA privind protecția minorilor;**
- **va prezenta, în 2026, un plan de acțiune al UE împotriva hărțuirii cibernetice.**

Statele membre sunt invitate:

- **să transpună integral noile norme privind recuperarea și confiscarea activelor până la sfârșitul anului 2026 și să le utilizeze la întregul lor potențial;**
- **să pună în aplicare abordarea administrativă în lupta împotriva infiltrării grupărilor de criminalitate organizată;**
- **să creeze parteneriate public-privat împotriva spălării banilor;**
- **să transpună și să pună în aplicare pe deplin Directiva privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice.**

Parlamentul European și Consiliul sunt invitate:

- **să înregistreze progrese în direcția negocierilor referitoare la Regulamentul de stabilire a normelor de prevenire și combatere a abuzului sexual asupra copiilor și a Directivei privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a materialelor care conțin abuzuri sexuale asupra copiilor;**
- **să încheie negocierile referitoare la Directiva privind combaterea corupției.**

6. Combaterea terorismului și a extremismului violent

Vom introduce o agendă cuprinzătoare de combatere a terorismului pentru a preveni radicalizarea, a securiza spațiile online și publice, a reprima canalele de finanțare și a răspunde atacurilor atunci când acestea apar.

Amenințarea teroristă în UE se menține la un nivel ridicat. Aceasta este strâns legată de efectele de propagare ale evenimentelor geopolitice, ale noilor tehnologii și ale noilor mijloace de finanțare a terorismului. Trebuie să ne asigurăm că UE este bine pregătită pentru a anticipa amenințările, pentru a preveni radicalizarea (atât offline, cât și online), pentru a proteja cetățenii și spațiile publice împotriva atacurilor și pentru a răspunde în mod eficace la atacuri atunci când acestea apar. O **nouă agendă a UE privind prevenirea și combaterea terorismului și a extremismului violent** va fi prezentată în 2025 pentru a stabili acțiunile viitoare ale UE. În conformitate cu noua agendă, UE și Balcanii de Vest vor semna în 2025 noul **Plan comun de acțiune** privind prevenirea și combaterea terorismului și a extremismului violent.

Prevenirea radicalizării și protecția persoanelor în mediul online

La fel ca în cazul luptei împotriva criminalității organizate, combaterea terorismului și a extremismului violent începe cu **abordarea cauzelor profunde ale acestora**. C**entrul de cunoștințe al UE privind prevenirea radicalizării** își va intensifica sprijinul acordat practicienilor și factorilor de decizie printr-un nou **set cuprinzător de instrumente de prevenire** pentru a permite identificarea timpurie și intervențiile axate pe persoanele vulnerabile, în special pe minori. Adesea, radicalizarea are loc în închisori și, pentru a sprijini statele membre în abordarea acestei probleme, Comisia va emite noi recomandări.

Extremiștii teroriști și violenți utilizează platforme online pentru a răspândi conținuturi cu caracter terorist și dăunător, pentru a colecta fonduri și pentru a recruta. Utilizatorii vulnerabili, în special minorii, sunt radicalizați online într-un ritm alarmant. **Regulamentul privind conținutul online cu caracter terorist** a avut un rol esențial în combaterea răspândirii conținutului online cu caracter terorist, permițând eliminarea rapidă a celor mai odioase și periculoase materiale[80]. În prezent, Comisia evaluează funcționarea sa și va analiza cele mai bune modalități de consolidare a acestui cadru.

Protocolul UE pentru situații de criză pentru un răspuns comun și rapid al autorităților de aplicare a legii și al industriei tehnologice în cazul unui atac terorist va fi modificat pentru a asigura scalabilitatea și flexibilitatea pentru a răspunde dimensiunii online tot mai mari a atacurilor teroriste. Forumul UE pentru internet va continua să fie principala cale de cooperare voluntară cu industria tehnologică pentru a combate conținutul online cu caracter terorist și dăunător. În plus, Comisia se implică în inițiative internaționale, cum ar fi Fundația Christchurch Call și Forumul mondial al internetului pentru combaterea terorismului (GIFCT).

Combaterea finanțării terorismului

Teroriștii își finanțează activitățile prin campanii de finanțare participativă, criptoactive, neobănci sau platforme de plată online. Autoritățile de aplicare a legii trebuie să detecteze și să investigheze aceste fluxuri financiare. Astfel de acțiuni necesită mijloace, instrumente și expertiză. **Rețeaua investigatorilor financiari în combaterea terorismului** joacă un rol esențial. Comisia va analiza posibilitatea creării unui **nou sistem la nivelul UE de urmărire a finanțării terorismului** care să acopere tranzacțiile intra-UE și SEPA, transferurile de criptoactive, plățile online și electronice, completând Acordul UE-SUA privind Programul de urmărire a finanțărilor în scopuri teroriste (TFTP).

Bugetul UE trebuie să fie **protejat împotriva utilizărilor abuzive pentru a promova opiniile radicale/extremiste** în statele membre. **Regulamentul financiar** revizuit include în prezent condamnarea pentru „incitare la discriminare, ură sau violență” drept motiv de excludere de la finanțarea UE. Comisia va continua să exploreze cea mai bună modalitate de a utiliza pe deplin setul de instrumente, inclusiv atunci când selectează potențialii beneficiari. Protecția bugetului UE se bazează, de asemenea, pe o cooperare strânsă și pe schimbul de informații cu autoritățile naționale, agențiile și organele UE.

Protecția împotriva atacurilor

Pe lângă investițiile în prevenirea radicalizării, o componentă importantă a protecției cetățenilor este limitarea mijloacelor pentru ca teroriștii și infractorii să comită atacuri. Sunt necesare acțiuni atât în ceea ce privește instrumentele utilizate de teroriști, cât și pentru a proteja țintele expuse riscului de atac.

[80] Până la 31 decembrie 2024, au fost emise 1 426 de ordine de eliminare pentru a retrage conținut cu caracter terorist sau pentru a bloca accesul la acesta, marea majoritate vizând conținutul cu caracter terorist jihadist, dar și conținutul cu caracter terorist de dreapta.

Pe lângă acțiunile privind armele de foc, Comisia va **revizui, de asemenea, normele** privind **precursorii de explozivi** pentru a include substanțele chimice cu grad ridicat de risc. **Spațiile publice** rămân cele mai frecvente ținte ale atacurilor teroriste, în special pentru actorii individuali. Pentru a proteja cetățenii de prejudicii, **programul UE de consiliere în materie de protecție a securității** va fi consolidat pentru a efectua evaluări ale vulnerabilității spațiilor publice, a infrastructurii critice și a evenimentelor cu risc ridicat, la cererea statelor membre și finanțate din bugetul UE în cadrul Fondului pentru securitate internă. UE va încerca să extindă finanțarea disponibilă pentru protecția spațiului public. Comisia oferă sprijin autorităților statelor membre și operatorilor privați prin orientări și instrumente specifice, cum ar fi Centrul de cunoștințe privind protecția spațiilor publice[81], iar 70 de milioane EUR au fost deja puse la dispoziție pentru a sprijini protecția spațiului public începând din 2020.

De asemenea, Comisia va analiza posibilitatea introducerii unor cerințe pentru ca organizațiile să aibă în vedere sau să utilizeze măsuri de securitate în locurile accesibile publicului, prin colaborarea cu autoritățile locale și cu partenerii privați.

Având în vedere vulnerabilitățile evidente, **Strategia UE privind combaterea antisemitismului și susținerea vieții evreiești (2021-2030)** va continua să orienteze acțiunile Comisiei privind protejarea comunității evreiești. Comisia se va asigura, de asemenea, că există instrumente adecvate pentru a sprijini statele membre în combaterea **urii față de musulmani**.

Utilizarea **dronelor** pentru spionaj și atacuri reprezintă o provocare tot mai mare în materie de securitate. Comisia va elabora o **metodologie de testare armonizată pentru sistemele anti-drone**, va înființa un **centru de excelență anti-drone** și va evalua necesitatea armonizării legislațiilor și a procedurilor statelor membre[82].

Luptătorii teroriști străini

Pentru a identifica luptătorii teroriști străini care se întorc sau intră la frontierele externe ale UE, sunt necesare date privind persoanele care reprezintă o amenințare teroristă. În acest scop, Comisia, împreună cu Europol, își va consolida **cooperarea cu principalele țări terțe pentru a obține date biografice și biometrice privind persoanele care ar putea reprezenta o amenințare teroristă**, inclusiv luptătorii teroriști străini, care pot fi apoi introduse în Sistemul de informații Schengen în deplină conformitate cu cadrele juridice naționale și ale UE aplicabile. Prin urmare, este esențial ca statele membre să utilizeze toate instrumentele existente. Acest lucru include introducerea tuturor informațiilor relevante în **SIS**, îmbunătățirea controalelor biometrice și efectuarea de controale sistematice obligatorii asupra tuturor persoanelor la frontierele externe ale UE[83]. În plus, **indicatorii comuni de risc** elaborați de Frontex vor continua să sprijine autoritățile de control la frontieră ale statelor membre pentru a identifica și a evalua riscul de călătorii suspecte ale potențialilor luptători teroriști străini.

În plus, pentru a se asigura că statele membre mențin accesul la **probele de pe câmpul de luptă** colectate de echipa de anchetă a ONU pentru a promova tragerea la răspundere pentru infracțiunile comise de Da'esh/ISIL (UNITAD) în vederea urmăririi penale a luptătorilor teroriști străini, Comisia, împreună cu Eurojust, va evalua posibilitatea de a stoca aceste probe în baza de date a Eurojust care cuprinde probe privind cele mai grave infracțiuni internaționale. În plus, noul **registru judiciar european de combatere a terorismului** va continua să sprijine

[81] Centrul de cunoștințe privind protecția spațiilor publice.
[82] Ca urmare a setului de acțiuni-cheie din Comunicarea din 2023 privind contracararea amenințărilor potențiale reprezentate de drone, COM(2023) 659 final.
[83] În deplină conformitate cu Codul frontierelor Schengen și cu Regulamentul privind screeningul.

sistemele judiciare ale statelor membre în identificarea rapidă a legăturilor transfrontaliere în cazurile de terorism.

Acțiuni-cheie

Comisia:

- **va adopta, în 2025, o nouă agendă a UE privind prevenirea și combaterea terorismului și a extremismului violent;**
- **va semna, în 2025, cu Balcanii de Vest, un nou Plan comun de acțiune privind prevenirea și combaterea terorismului și a extremismului violent;**
- **va dezvolta un nou set cuprinzător de instrumente de prevenire împreună cu Centrul de cunoștințe al UE;**
- **va evalua, în 2026, aplicarea Regulamentului privind conținutul online cu caracter terorist;**
- **va modifica, în 2025, Protocolul UE pentru situații de criză;**
- **va prezenta, în 2026, o propunere legislativă de revizuire a Regulamentului privind comercializarea și utilizarea precursorilor de explozivi;**
- **va analiza fezabilitatea unui nou sistem la nivelul UE de urmărire a finanțării terorismului.**

Statele membre sunt invitate:

- **să îmbunătățească controalele biometrice și să efectueze controale sistematice obligatorii la frontierele externe ale UE;**
- **să utilizeze pe deplin registrul judiciar european de combatere a terorismului.**

7. UE ca actor global puternic în domeniul securității

Pentru a spori securitatea UE, vom stimula cooperarea operațională prin parteneriate cu regiuni-cheie, cum ar fi partenerii noștri vizați de politica de extindere și de vecinătate, America Latină și regiunea mediteraneeană. Interesele de securitate ale UE vor fi luate în considerare în cadrul cooperării internaționale, inclusiv prin mobilizarea mijloacelor și instrumentelor UE.

Ultimii ani au demonstrat legăturile intrinseci dintre securitatea externă și cea internă a UE. Războiul de agresiune al Rusiei împotriva Ucrainei, conflictul din Gaza, situația din Siria și conflictele emergente din întreaga lume au avut efecte de propagare grave asupra securității interne a UE. Pentru a contracara impactul instabilității globale asupra securității sale interne, **UE trebuie să își apere în mod activ interesele de securitate** prin abordarea amenințărilor externe, perturbarea rutelor de trafic și protejarea coridoarelor de interes strategic, cum ar fi rutele comerciale. În același timp, UE va continua să fie un aliat puternic al țărilor partenere, conlucrând pentru a spori securitatea mondială și pentru a consolida reziliența reciprocă la amenințări.

În ultimii ani, UE a luat măsuri semnificative pentru a-și consolida cooperarea în materie de securitate. Aceasta a încheiat acorduri operaționale de cooperare judiciară și în materie de asigurare a respectării legii, precum și alte tipuri de acorduri cu țările partenere. UE urmărește în mod activ încheierea de acorduri internaționale suplimentare, în conformitate cu directivele de negociere ale Consiliului, și inițiative de consolidare a capacităților, facilitate de agențiile și organele UE. IVCDCI – Europa globală este, de asemenea, un instrument esențial pentru consolidarea securității cu țările partenere.

Ordinea multilaterală bazată pe norme este o piatră de temelie pentru consolidarea securității mondiale. Dialogurile privind securitatea, inclusiv cele tematice, sunt vitale pentru consolidarea acestor eforturi. Punerea în aplicare a **Busolei strategice pentru securitate și apărare**, împreună cu cadrele de cooperare bilaterale și multilaterale, cum ar fi acordurile de stabilizare și de asociere și acordurile de asociere, precum și colaborările cu organizații precum ONU și NATO, sunt esențiale pentru dezvoltarea unor soluții de securitate eficace. UE va continua să își joace rolul în cadrul forurilor multilaterale[84] și își va consolida cooperarea cu organizațiile și cadrele internaționale și regionale relevante, inclusiv NATO, Organizația Națiunilor Unite, Consiliul Europei, Interpol, G7, OSCE și societatea civilă.

Cooperarea regională

Ca prioritate, continuarea sprijinului fără rezerve acordat de UE **Ucrainei** și consolidarea securității și a rezilienței țărilor implicate în **procesul de aderare la UE** reprezintă un imperativ politic și geostrategic. Sprijinirea securității UE ar trebui să meargă mână în mână cu **integrarea accelerată a țărilor candidate** în **arhitectura de securitate a UE**, în paralel cu consolidarea cooperării lor regionale. Comisia va utiliza politica de extindere a UE pentru a sprijini capacitățile țărilor candidate și potențial candidate la UE de a răspunde amenințărilor, pentru a spori cooperarea operațională și schimbul de informații și pentru a asigura alinierea la principiile, legislația și instrumentele UE. Instrumentul de asistență pentru preaderare (IPA III), precum și Mecanismele pentru Ucraina, Moldova și Balcanii de Vest sunt esențiale pentru consolidarea securității atât în țările candidate, cât și în țările potențial candidate.

De asemenea, UE va continua să integreze **partenerii din vecinătate** în arhitectura de securitate a UE. Prin intermediul **Noului Pact pentru Mediterana** și al viitoarei **abordări strategice privind Marea Neagră**, Uniunea va urmări să continue consolidarea cooperării regionale și a parteneriatelor strategice cuprinzătoare bilaterale cu o dimensiune de securitate, după caz, cu dialoguri periodice la nivel înalt privind securitatea. Cooperarea operațională cu Africa de Nord, **Orientul Mijlociu și Golful** va fi consolidată, în special în ceea ce privește combaterea terorismului, combaterea spălării banilor, a traficului de arme de foc și a producției și traficului de droguri, în special Captagon**.**

Pentru a aborda intensificarea activităților teroriste și infracționale și potențialele lor efecte de propagare în **Africa Subsahariană, în special în Sahel, Cornul Africii și Africa de Vest,** UE va consolida sprijinul acordat Uniunii Africane, comunităților economice regionale (CER) și țărilor din regiune. În conformitate cu Strategia UE în materie de securitate maritimă[85], UE va consolida cooperarea în **Golful Guineei, Marea Roșie și Oceanul Indian** pentru a combate traficul și pirateria, prin sprijinirea cooperării intraafricane și regionale și cu sprijinul prezențelor maritime coordonate ale UE și al Centrului de Analiză și Operațiuni Maritime – Stupefiante (MAOC-N).

Împreună cu **America Latină și zona Caraibilor**, UE va consolida cooperarea operațională în vederea dezmembrării și urmăririi penale a rețelelor infracționale cu grad ridicat de risc și a perturbării activităților ilicite și a rutelor de trafic, consolidând cadrele de cooperare, cum ar fi UE-CLASI (Comitetul latinoamerican pentru securitate internă) și Mecanismul de coordonare și cooperare UE-CELAC în materie de droguri. Printre priorități se vor număra reziliența și parteneriatele centrelor logistice, precum și abordările de tip „urmărirea banilor”. UE va sprijini în continuare dezvoltarea Comunității forțelor de poliție din America (AMERIPOL) pentru a deveni echivalentul regional al Europol și pentru a consolida cooperarea judiciară dintre statele

[84] Forumul mondial pentru combaterea terorismului, coaliția internațională pentru contracararea Da'esh, Forumul mondial al internetului pentru combaterea terorismului (GIFCT), Fundația Christchurch Call, Coaliția internațională pentru abordarea amenințărilor reprezentate de drogurile sintetice.
[85] JOIN(2023) 8 final.

membre și regiune. De asemenea, UE va colabora cu **Asia de Sud și Asia Centrală** cu privire la provocările comune în materie de securitate legate de terorism, traficul de bunuri ilicite, inclusiv de droguri, traficul de persoane și introducerea ilegală de migranți.

În plus, UE va sprijini cadrele de cooperare regională din țările terțe pentru a le ajuta în continuare să oprească traficul ilicit la sursă, în conformitate cu principiul responsabilității comune pentru întregul lanț de aprovizionare infracțional. În plus, UE își va aduce contribuția la consolidarea securității centrelor logistice din străinătate, prin coordonarea **inspecțiilor comune în porturile țărilor terțe**.

Cooperare operațională

Global Gateway va sprijini proiecte de infrastructură durabile și de înaltă calitate în sectoarele digital, climatic și energetic, al transporturilor, al sănătății, al educației și al cercetării. Comisia va include considerente de securitate, după caz, în viitoarele investiții din cadrul strategiei „Global Gateway". Aceasta va include inițiative esențiale pentru autonomia strategică a UE și a țărilor sale partenere, cum ar fi proiectele de infrastructură care includ evaluări de securitate și măsuri de atenuare a riscurilor.

Comisia va urmări încheierea de noi **acorduri între UE și țările terțe privind cooperarea cu Europol și Eurojust**, în special cu țările din America Latină.

În plus, participarea proactivă a țărilor din afara UE la **EMPACT** este unul dintre cele mai eficace mijloace de consolidare a cooperării operaționale. UE va încuraja în continuare implicarea în acest cadru a țărilor terțe, în special a Balcanilor de Vest, a vecinătății estice, a Africii Subsahariene, a Africii de Nord, a Orientului Mijlociu, a Americii Latine și a zonei Caraibilor. Un alt instrument de intensificare a cooperării cu țările terțe în ceea ce privește combaterea criminalității este reprezentat de grupurile operative operaționale între statele membre și coordonate de Europol, la care pot participa țări terțe. Comisia urmărește, de asemenea, să finalizeze negocierile pentru acordul internațional **UE-Interpol**[86], asigurând o abordare mai unificată a amenințărilor la adresa securității mondiale și a combaterii infracțiunilor transnaționale.

Uniunea trebuie să fie prezentă pe teren în cadrul unei abordări de tip „Echipa Europa". Personalul specializat al Uniunii și al statelor membre joacă un rol esențial în asigurarea faptului că acțiunea externă a Uniunii este bine informată, coordonată și receptivă. Pentru a aduce această abordare la un nivel superior, Comisia, sprijinită de Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate, va consolida **rețelele de legătură** și va facilita detașarea **ofițerilor de legătură regionali Europol și Eurojust,** în conformitate cu nevoile operaționale ale statelor membre.

UE va urmări o cooperare operațională mai strânsă în domeniul asigurării respectării legii și al cooperării judiciare, va încuraja schimbul de informații în timp real și operațiunile comune prin intermediul **echipelor comune de anchetă** din țările terțe, cu sprijinul Europol și Eurojust. De asemenea, Comisia va sprijini statele membre în crearea unor **centre comune de fuziune** care să reunească experți și autorități locale de aplicare a legii din țări terțe strategice.

Instrumentele politicii externe și de securitate comună (PESC)

Misiunile din cadrul politicii de securitate și apărare comune (PSAC) vor fi, de asemenea, utilizate la întregul lor potențial pentru a identifica și a aborda mai bine amenințările externe la adresa securității interne a UE, în conformitate cu mandatele lor stabilite de Consiliu. Pentru a consolida capacitățile țărilor terțe, Înaltul Reprezentant al Uniunii pentru afaceri externe și

[86] Decizia (UE) 2021/1312 a Consiliului din 19 iulie 2021 și Decizia (UE) 2021/1313 a Consiliului din 19 iulie 2021.

politica de securitate și Comisia vor sprijini acțiunile PSAC cu instrumente de finanțare specifice și vor explora toate căile de finanțare adecvate.

Măsurile restrictive ale UE reprezintă un instrument PESC bine stabilit, utilizat și pentru combaterea terorismului. Pe baza sugestiilor din partea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate, a statelor membre sau a Comisiei, Consiliul ar putea evalua modul în care măsurile restrictive autonome existente ale UE (lista UE a teroriștilor) ar putea deveni mai eficace, mai operaționale și mai flexibile. În plus, aceste instituții ar putea lua în considerare explorarea unor măsuri restrictive suplimentare care să vizeze rețelele infracționale, în conformitate cu obiectivele PESC.

Politica în domeniul vizelor și schimbul de informații

Politica UE în domeniul vizelor este un instrument-cheie pentru cooperarea cu țările terțe și securizarea frontierelor noastre prin controlul intrării în UE și stabilirea condițiilor pentru aceasta. Comisia va integra pe deplin **considerentele de securitate în politica UE în domeniul vizelor** prin intermediul unei viitoare strategii a UE privind politica în domeniul vizelor. Comisia va colabora cu colegiuitorii pentru a adopta propunerea de revizuire și raționalizare a mecanismului de suspendare a exceptării de la obligativitatea vizelor, în special pentru cazurile specifice de utilizare abuzivă a regimului de călătorii fără viză[87]. Țările terțe vor fi încurajate să facă schimb de informații cu privire la persoanele care pot reprezenta amenințări la adresa securității, care vor fi introduse în sistemele de informații și în bazele de date ale UE.

Pentru a realiza o coordonare a politicilor și eforturi în amonte, care să permită o cooperare mai eficientă, mai rapidă și mai armonioasă, Comisia va depune eforturi în vederea stabilirii unor **mecanisme privind fluxul de date** și va explora modalități de **îmbunătățire a schimbului de informații** în scopul asigurării respectării legii și al gestionării frontierelor cu țări terțe de încredere, în conformitate cu drepturile fundamentale și cu normele de protecție a datelor.

Acțiuni-cheie

Comisia:

- **va încheia acorduri internaționale între UE și țările terțe prioritare privind cooperarea cu Europol și Eurojust;**
- **va încuraja participarea țărilor partenere la EMPACT pentru combaterea criminalității organizate și a terorismului;**
- **va sprijini agențiile și organele UE în stabilirea și consolidarea acordurilor de lucru cu țările partenere;**
- **va reflecta în continuare considerentele de securitate în politica UE în domeniul vizelor prin intermediul viitoarei strategii privind vizele;**
- **va consolida schimbul de informații cu țările terțe de încredere în scopul asigurării respectării legii și al gestionării frontierelor.**

Comisia, în cooperare cu Înaltul Reprezentant al Uniunii pentru afaceri externe:

- **va utiliza pe deplin misiunile civile din cadrul politicii de securitate și apărare comune (PSAC);**
- **va coordona, până în 2027, inspecțiile comune în porturile țărilor terțe.**

Comisia, în cooperare cu Înaltul Reprezentant al Uniunii pentru afaceri externe și cu statele membre:

[87] COM(2023) 642.

- **va consolida rețelele de legătură și cooperarea în cadrul unei abordări de tip „Echipa Europa”;**
- **va înființa, începând cu 2025, echipe operaționale comune și centre de fuziune în țări terțe.**

Parlamentul European și Consiliul sunt invitate:

- **să încheie negocierile privind revizuirea mecanismului de suspendare a exceptării de la obligativitatea vizelor.**

8. Concluzii

Într-o lume a incertitudinii, trebuie îmbunătățită capacitatea Uniunii de a anticipa, de a preveni și de a răspunde amenințărilor la adresa securității.

Nu este suficient să reacționăm la crize doar atunci când acestea apar. Trebuie să ne îmbunătățim gradul de conștientizare cu o imagine completă a amenințărilor pe măsură ce acestea evoluează. Și să ne asigurăm că instrumentele și capacitățile noastre sunt la înălțimea misiunii.

Setul cuprinzător de măsuri detaliate în prezenta strategie va contribui la crearea unei Uniuni mai puternice la nivel mondial: o Uniune capabilă să anticipeze, să planifice și să se ocupe de propriile nevoi de securitate, care poate să răspundă în mod eficace la amenințările la adresa securității sale interne și să tragă la răspundere făptuitorii și care își protejează societățile și democrațiile deschise, libere și prospere.

Acest lucru necesită o schimbare de mentalitate în ceea ce privește securitatea internă. Vom depune eforturi pentru a contribui la promovarea unei noi culturi a securității în UE, în care considerentele de securitate să fie luate în considerare în toate actele legislative, politicile și programele noastre – de la inițiere până la punerea în aplicare. Și în care colaborarea între domeniile de politică ne permite să creăm noi perspective.

Aceasta nu este sarcina unei singure instituții, a unui singur guvern sau a unui singur actor. Este efortul comun al Europei.