DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE
DIRECȚIA PENTRU UNIUNEA EUROPEANĂ

FIȘĂ DE INFORMARE

ProtectEU: Agenda privind prevenirea și combaterea terorismului

COM(2026)101

Autor:
Eniko Georgescu

Data:
18 mai 2026

Publicațiile direcției pot fi accesate prin următorul link: www. cdep. ro

DATE DESPRE COMUNICARE **JAI 8**

1. Data adoptării de către Comisia Europeană: : 26.02.2026. **Responsabil:** Magnus Brunner, Comisar pentru Afaceri Interne și Migrațiune (Direcția Generală Migrație și Afaceri Interne, DG HOME

2. Denumire document: *Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor - ProtectEU: Agenda privind prevenirea și combaterea terorismului*

3. Date de identificare: COM(2026)101

4. Tipul documentului: nelegislativ, care stabilește orientări politice, evaluări și priorități pentru acțiunea ulterioară a instituțiilor UE și a statelor membre.

5. Stadiul actual:

Parlamentul European:

- etapă pregătitoare - comisia sesizată pentru raport: Comisia pentru libertăți civile, justiție și afaceri interne - LIBE; comisii responsabile pentru opinii: Comisia pentru afaceri externe - AFET; Comisia pentru securitate și apărare - SEDE (conform OEIL).

Consiliu UE:

- Reuniunea Consiliului Justiție și Afaceri Interne în 04-05.06.2026. Grupul de lucru pentru probleme de terorism.

Rezumat

Documentul se înscrie în procesul de consolidare a arhitecturii de securitate internă a Uniunii Europene, în contextul unei transformări profunde a mediului de risc, caracterizat de convergența dintre terorism, criminalitate organizată și amenințări hibride, precum și de utilizarea accelerată a tehnologiilor emergente de către actori ostili.

Această agenda, anunțată în ProtectEU, reflectă tranziția de la un model reactiv la unul anticipativ, în care prevenirea și detectarea timpurie devin elemente centrale ale politicii europene de securitate.

Propunerea evidențiază faptul că amenințările actuale nu mai pot fi abordate izolat, întrucât rețelele infracționale și teroriste operează transnațional, utilizează infrastructuri digitale și exploatează lacunele existente între diferitele domenii de politică publică.

Totodată, agenda integrează dimensiunea riscurilor CBRN (chimice, biologice, radiologice și nucleare), considerate evenimente cu probabilitate redusă, dar cu impact major.

Inițiativa acordă o importanță deosebită protejării spațiilor publice, considerate în continuare principalele ținte ale atacurilor teroriste. Se promovează conceptul de „*security by design*” (securitate prin design) într-un context extins, nu doar digital, ci și fizic care presupune integrarea măsurilor de securitate încă din faza de planificare urbană și de proiectare a infrastructurilor.

În ceea ce privește cooperarea instituțională, documentul reafirmă rolul central al agențiilor UE, în special Europol și Eurojust, în facilitarea schimbului de informații și coordonarea investigațiilor transfrontaliere. În același timp, Consiliul Uniunii Europene, prin mecanisme precum EMPACT, stabilește prioritățile operaționale în materie de combatere a criminalității și terorismului, asigurând coerența acțiunii la nivelul statelor membre.

Documentul integrează și dimensiunea externă a combaterii terorismului, subliniind importanța cooperării cu statele partenere din Balcanii de Vest, Orientul Mijlociu și Africa de Nord, precum și rolul Uniunii Europene în cadrul mecanismelor multilaterale internaționale, inclusiv ONU și Grupul de Acțiune Financiară Internațională (GAFI/FATF).

Cuvinte-cheie: lupta împotriva criminalității; securitate europeană; terorism; ajutor pentru victime; dezinformare; securitatea sistemelor informatice; mijloace de comunicare sociale; radicalizare; securitatea infrastructurii critice; spațiu de libertate, securitate și justiție

CUPRINS

I. CONTEXT

Evoluțiile recente ale mediului internațional de securitate au determinat o transformare semnificativă a modului în care Uniunea Europeană abordează prevenirea și combaterea terorismului. Amenințările actuale sunt caracterizate printr-un grad ridicat de complexitate, volatilitate și interconectare, fiind influențate atât de degradarea contextului geopolitic internațional, cât și de impactul accelerat al digitalizării și al tehnologiilor emergente asupra securității interne europene.

Instituțiile Uniunii Europene evidențiază în mod constant faptul că terorismul nu mai poate fi analizat exclusiv prin prisma atacurilor convenționale, ci trebuie abordat într-un cadru mai larg, care include criminalitatea organizată transfrontalieră, radicalizarea online, amenințările hibride, atacurile cibernetice, dezinformarea și finanțarea ilicită.

Pe fondul acestor evoluții, politica europeană de combatere a terorismului a cunoscut o tranziție graduală de la o abordare predominant reactivă către un model integrat și anticipativ de gestionare a riscurilor.

Un punct de referință în această evoluție l-a reprezentat Agenda UE[1] privind combaterea terorismului din 2020, care a consolidat arhitectura europeană de securitate în jurul unor direcții esențiale precum anticiparea amenințărilor, prevenirea radicalizării, protejarea cetățenilor și consolidarea capacității de răspuns la atacuri.

În acest sens, ProtectEU[2] marchează o schimbare de paradigmă prin promovarea unei securități europene integrate, bazate pe interoperabilitate, schimb avansat de informații, anticipare strategică și cooperare consolidată între statele membre, instituțiile Uniunii Europene și partenerii externi.

În paralel, documentele comune ale Comisiei Europene și ale Înaltului Reprezentant, inclusiv Menținerea păcii - Foaia de parcurs privind pregătirea pentru apărare 2030[3] și Scutul european pentru democrație, consolidarea democrațiilor puternice și reziliente[4] dezvoltă dimensiunea externă a securității europene și subliniază necesitatea consolidării cooperării cu statele partenere în domeniul combaterii terorismului, al prevenirii radicalizării și al combaterii amenințărilor hibride. Aceste documente promovează o abordare integrată - securitate - apărare - diplomație - și evidențiază importanța parteneriatelor externe pentru reducerea vulnerabilităților transfrontaliere.

[1] COM(2020) 795 final
[2] COM(2025) 148 final
[3] JOIN (2025) 27 final
[4] JOIN(2025) 791

O atenție deosebită este acordată regiunilor considerate relevante pentru securitatea europeană, în special Balcanilor de Vest, Orientului Mijlociu și Africii de Nord, în contextul persistenței riscurilor asociate circulației combatanților teroriști străini, traficului ilicit de arme, radicalizării și instabilității regionale. În acest cadru se înscriu Planul comun de acțiune UE – Balcanii de Vest privind prevenirea și combaterea terorismului pentru perioada 2025–2030, dialogurile UE privind combaterea terorismului cu state terțe, precum și consolidarea cooperării operaționale și a schimbului de informații cu partenerii externi ai Uniunii.

Totodată, evoluțiile tehnologice au generat preocupări crescute la nivel european privind utilizarea inteligenței artificiale, imprimării 3D, sistemelor autonome și biotehnologiilor în scopuri ostile. Evaluările Comisiei Europene, ale Europol și ale Centrului Comun de Cercetare al Comisiei Europene (JRC) evidențiază faptul că noile tehnologii pot amplifica vulnerabilitățile existente și pot facilita accesul la mijloace utilizate în activități teroriste sau extremiste.

În același timp, radicalizarea online și utilizarea platformelor digitale pentru propagandă extremistă reprezintă una dintre principalele preocupări ale instituțiilor europene. Măsurile de la nivelul UE evidențiază intensificarea fenomenului de auto-radicalizare, inclusiv în rândul minorilor, precum și utilizarea platformelor criptate și a rețelelor sociale pentru diseminarea conținutului extremist și mobilizarea susținătorilor.

Contextul strategic actual este influențat și de deteriorarea mediului de securitate din vecinătatea Uniunii Europene, inclusiv din Orientul Mijlociu și Siria, aspect evidențiat și în concluziile Consiliului Uniunii Europene privind Siria, care subliniază riscurile persistente generate de rețelele jihadiste și de potențiala reactivare a unor structuri extremiste în regiune.

În paralel, Uniunea Europeană promovează consolidarea cooperării multilaterale în domeniul combaterii terorismului, inclusiv în cadrul Organizației Națiunilor Unite, GAFI/FATF, NATO, Interpol și al altor formate internaționale relevante. Totodată, integrarea securității în abordarea europeană de tip „360 de grade" promovată prin Global Gateway reflectă orientarea Uniunii către o corelare mai strânsă între instrumentele de securitate, dezvoltare, infrastructură, diplomație și cooperare externă.

II. PREZENTAREA COMUNICĂRII

Comunicarea prezintă un nou cadru strategic pentru întărirea securității Uniunii Europene în fața amenințărilor teroriste și extremiste, cu accent pe prevenirea radicalizării, în special în mediul online, și adaptarea la noile riscuri generate de tehnologiile digitale.

Agenda propune consolidarea cooperării dintre statele membre, Europol și platformele digitale, utilizarea mai eficientă a datelor și a inteligenței artificiale în investigații, combaterea finanțării terorismului și îmbunătățirea capacității de reacție la crize.

Documentul este structurat pe piloni strategici interdependenți, fiecare fiind însoțit de ***acțiuni-cheie, măsuri legislative, inițiative operaționale și mecanisme instituționale atribuite*** Comisiei Europene, Înaltului Reprezentant, Consiliului UE, Europol, Eurojust, Frontex, CEPOL, ENISA, EASA și statelor membre.

1. Anticiparea amenințărilor și consolidarea capacităților de intelligence

Primul pilon al documentului vizează consolidarea capacităților Uniunii Europene de anticipare strategică și analiză a amenințărilor. Comunicarea subliniază că securitatea europeană trebuie să se bazeze pe capacități eficiente de previziune, avertizare timpurie și

schimb de informații, într-un context în care amenințările teroriste sunt din ce în ce mai fluide și mai greu de identificat.

Documentul evidențiază rolul central al Europol în furnizarea de *intelligence* operațional și elaborarea evaluărilor strategice privind tendințele teroriste și conexiunile dintre criminalitatea organizată și extremismul violent, inclusiv prin rapoartele EU-SOCTA 2025 și TE-SAT 2025. Inițiativa menționează explicit creșterea utilizării platformelor digitale, a canalelor criptate și a sistemelor financiare alternative, inclusiv „Hawala digitală”[5], pentru finanțarea și coordonarea activităților teroriste.

Un rol esențial în arhitectura actuală de securitate a Uniunii Europene este atribuit SIAC[6] **(Capacitatea Unică de Analiză a Informațiilor)** care reprezintă punctul unic de introducere a contribuțiilor statelor membre în materie de informații, furnizând, în timp util, evaluări ale amenințărilor. Consolidarea acestui mecanism reprezintă o prioritate strategică pentru Înaltul Reprezentant și Comisia Europeană, fiind orientată către trei direcții esențiale: ***suplimentarea resurselor operaționale, securizarea infrastructurii de comunicații și implementarea paradigmei „need to share”***. Acest demers urmărește fluidizarea schimbului de date la nivel comunitar, menținând totodată integritatea protocoalelor stricte privind informațiile clasificate.

Printre acțiunile-cheie anunțate de Comisie în cadrul acestui pilon se regăsesc:

- dezvoltarea unei proceduri comune privind evaluarea alertelor SIS;
- extinderea cadrului european API/PNR[7] către alte moduri de transport; consolidarea interoperabilității bazelor de date europene;
- îmbunătățirea schimbului operațional de informații între statele membre și agențiile UE.

2. Prevenirea radicalizării și sprijinirea victimelor terorismului

Un al doilea pilon strategic al documentului îl reprezintă prevenirea radicalizării și combaterea extremismului violent, subliniindu-se faptul că radicalizarea online s-a accelerat

---

[5] **Hawala** reprezintă un sistem de transfer alternativ sau paralel care funcționează în afara sistemelor financiare tradiționale. În general, o tranzacție hawala compensează valoarea banilor dintr-o țară în alta fără a presupune mișcarea corespunzătoare de numerar sau acoperirea peste granițe. Un alt mod de a privi tranzacția este ca pe un transfer de datorii. Originile hawala sunt foarte vechi, sistemul fiind dezvoltat cu sute de ani înaintea apariției transferurilor bancare. Hawala a apărut din necesitatea de a realiza transferuri legitime între persoane din diverse regiuni sau chiar state, în lipsa altor opțiuni disponibile în acele vremuri, însă grupările de criminalitate organizată au profitat de oportunitățile oferite de această metodă pentru a disimula originea și beneficiarul banilor vehiculați.

[6] **SIAC** are rolul de a furniza analize strategice de informații pentru Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate, precum și pentru serviciile SEAE. Acesta funcționează ca un mecanism integrat de analiză la nivelul Uniunii Europene și reunește două componente complementare: EU INTCEN (Centrul de Situații și Analiză a Informațiilor al UE), responsabil în principal de analiza informațiilor civile provenite din surse deschise și din contribuțiile serviciilor de informații ale statelor membre, și Direcția de Informații a Statului Major al UE, care furnizează evaluări și analize de natură militară. Prin cooperarea dintre aceste structuri, SIAC contribuie la evaluarea amenințărilor, sprijinirea procesului decizional european și consolidarea securității Uniunii.

[7] Extinderea cadrului API (Advance Passenger Information) și PNR (Passenger Name Record) la nivelul UE vizează, conform priorităților 2026, consolidarea securității prin includerea transportului feroviar, maritim și rutier (autocare), nu doar a celui aerian. Acțiunile-cheie includ standardizarea colectării datelor, interoperabilitatea sistemelor naționale și intensificarea schimbului de informații

semnificativ, inclusiv în rândul minorilor, iar platformele digitale sunt utilizate pentru propagandă extremistă, recrutare, finanțare și coordonare operațională.

Documentul subliniază rolul Centrului de cunoștințe privind prevenirea radicalizării în coordonarea schimbului de bune practici, dezvoltarea politicilor preventive și sprijinirea statelor membre în elaborarea strategiilor naționale de prevenire a extremismului violent.

În paralel, Comisia Europeană colaborează intens cu platformele digitale și GIFCT (*Global Internet Forum to Counter Terrorism*) pentru a elimina rapid conținutul extremist și terorist online, în acord cu prevederile Regulamentului UE 2021/784 (în vigoare din iunie 2022) și Directivei privind Serviciile Media Audiovizuale. GIFCT funcționează ca un partener cheie pentru partajarea tehnică a amprentelor digitale ale materialelor cu conținut terorist, facilitând identificarea și eliminarea rapidă a acestora de pe platformele online. Acest tip de cooperare se realizează în principal prin intermediul EU Internet Forum (EUIF), o inițiativă lansată în 2015 de Comisia Europeană, menită să sprijine dialogul voluntar între autorități publice și platformele digitale în vederea prevenirii și combaterii conținutului terorist online.

Comunicarea tratează distinct:

- combaterea radicalizării în penitenciare;
- monitorizarea persoanelor care părăsesc sistemul penitenciar;
- gestionarea întoarcerii luptătorilor teroriști străini și a membrilor familiilor acestora;
- dezvoltarea programelor de reintegrare și deradicalizare.

Documentul evidențiază că penitenciarele continuă să reprezinte medii cu risc ridicat pentru propagarea ideologiilor extremiste, motiv pentru care Comisia Europeană promovează dezvoltarea unor standarde comune privind evaluarea riscurilor, monitorizarea și reintegrarea persoanelor radicalizate.

De asemenea, statele membre sunt încurajate:

- să integreze prevenirea radicalizării în educație și sport, pe baza recomandărilor, a instrumentelor și a bunelor practici elaborate la nivelul UE;
- să consolideze campaniile de comunicare strategică și de sensibilizare, pe baza sprijinului oferit de Centrul de cunoștințe al UE;

În paralel, Agenda acordă o importanță majoră sprijinului victimelor terorismului, considerate element central al rezilienței democratice europene. Comisia susține consolidarea mecanismelor europene de sprijin psihologic, juridic și social pentru victime și dezvoltarea cooperării dintre statele membre în situații de criză.

3. Protejarea persoanelor în mediul online și combaterea extremismului digital

Agenda UE tratează mediul digital drept una dintre principalele dimensiuni strategice ale combaterii terorismului contemporan. Textul evidențiază faptul că platformele digitale sunt utilizate pentru: ***propagandă extremistă; recrutare; coordonare operațională; finanțare; instruire online; diseminarea manualelor privind fabricarea explozivilor și utilizarea armelor.***

În acest context, Comisia Europeană promovează utilizarea deplină a cadrului european privind combaterea conținutului terorist online, în special: Regulamentul (UE) 2021/784 privind prevenirea diseminării conținutului online cu caracter terorist; Regulamentul privind serviciile digitale (DSA) ce impune responsabilități sporite platformelor mari pentru moderarea

conținutului ilegal și gestionarea riscurilor sistemice[8]; Directiva serviciilor mass-media audiovizuale(DSMAV); mecanismele dezvoltate în cadrul EU Internet Forum.

Propunerea evidențiază rolul strategic al cooperării cu platformele digitale și GIFCT(*Global Internet Forum to Counter Terrorism*), care este esențială pentru:

- ✓ **Detectarea automată:** Utilizarea tehnologiilor (precum "*hashing*") pentru a identifica și șterge conținutul extremist înainte ca acesta să devină viral.
- ✓ **Eliminarea rapidă:** Prevenirea reîncărcării materialelor deja identificate ca fiind periculoase inclusiv în ceea ce privește detectarea automată și eliminarea rapidă a conținutului extremist.

În plus, Comisia va aborda aspectele de securitate ale jocurilor online în cadrul strategiei sale globale privind jocurile video, care urmează să fie publicată în 2026. În paralel, Comisia va monitoriza îndeplinirea de către furnizorii de servicii online a angajamentelor asumate în temeiul Codului de conduită privind combaterea discursului ilegal de incitare la ură din mediul online+.

Se acordă atenție și gestionării situațiilor de criză online, subliniind necesitatea unor mecanisme coordonate de răspuns rapid în cazul atacurilor teroriste și al campaniilor de propagandă extremistă cu impact transfrontalier.

4. Protejarea persoanelor în mediul fizic și împiedicarea călătoriilor în scopuri teroriste

Noua arhitectură strategică de securitate a Uniunii, dezvoltă o abordare extinsă privind protejarea cetățenilor și gestionarea mobilității asociate amenințărilor teroriste. Comisia evidențiază rolul noilor sisteme europene de informații la scară largă, inclusiv: SIS - cea mai utilizată bază de date pentru securitate și gestionarea frontierelor. Permite schimbul în timp real de alerte privind persoane (dispărute, căutate) sau bunuri între autoritățile polițienești; EES - Operațional la nivelul tuturor punctelor de trecere a frontierei externe din 10 aprilie 2026, înregistrează digital datele biometrice (amprente și imagine facială) și alfanumerice ale cetățenilor non-UE (șederi scurte), înlocuind ștampilarea pașapoartelor.

Acesta detectează automat persoanele care depășesc termenul legal de ședere; ETIAS - preconizat să devină operațional în ultimul trimestru al anului 2026, va impune cetățenilor din țări terțe (scutiți de viză) să obțină o autorizație de călătorie înainte de a ajunge la frontierele UE, evaluând riscurile de securitate, migrație sau sănătate.; Eurodac - Sistemul european de amprentare pentru gestionarea cererilor de azil. O nouă versiune este planificată să intre în funcțiune în iunie 2026, adăugând date biometrice suplimentare pentru o identificare mai rapidă.; API/PNR - colectează datele pasagerilor de la companiile aeriene înainte de sosirea în UE, permițând analiza riscurilor și identificarea amenințărilor de securitate.; sistemele de screening la frontierele externe - reglementarea privind screening-ul, aliniată cu noile sisteme IT, introduce verificări rapide de securitate, sănătate și vulnerabilitate pentru persoanele care trec frontiera în mod neautorizat. Din perspectivă strategică, aceste instrumente urmăresc:

- ➢ identificarea timpurie a persoanelor cu risc;
- ➢ împiedicarea deplasărilor în scopuri teroriste;
- ➢ detectarea luptătorilor teroriști străini;
- ➢ consolidarea controlului la frontierele externe ale Uniunii.

Comunicarea promovează extinderea cadrului API/PNR către transportul maritim, terestru și zborurile private, în scopul reducerii lacunelor operaționale exploatate de rețelele teroriste.

[8] Regulamentul privind serviciile digitale (DSA) este primul regulament în domeniul digital din lume care face ca întreprinderile digitale din întreaga UE să fie răspunzătoare pentru conținutul postat pe platformele lor

5. Restricționarea accesului la mijloacele utilizate pentru comiterea atacurilor

Acest pilon reflectă orientarea Uniunii Europene către reducerea vulnerabilităților materiale utilizate în atacurile teroriste. Raportul evidențiază:

- proliferarea armelor ilegale;
- utilizarea armelor fabricate prin imprimare 3D;
- accesibilitatea precursorilor de explozivi;
- riscurile asociate comercializării online a substanțelor sensibile.

Comisia Europeană anunță: armonizarea incriminării infracțiunilor privind armele de foc; combaterea modelelor digitale utilizate pentru imprimarea 3D a armelor; revizuirea Regulamentului privind precursorii de explozivi[9]; reevaluarea Directivei privind articolele pirotehnice[10]. Europol și Eurojust sunt prezentate drept actori centrali în coordonarea investigațiilor transfrontaliere și combaterea traficului ilicit de arme și explozivi.

6. Gestionarea amenințărilor CBRN și a tehnologiilor emergente

Noua abordare a UE privind securitatea internă consideră riscurile CBRN drept amenințări cu probabilitate redusă, dar cu impact strategic extrem de ridicat asupra securității europene. Propunerea anunță elaborarea unui nou Plan de Acțiune CBRN al UE pentru 2026, orientat spre: ***pregătire și răspuns; avertizare timpurie; formare și exerciții comune; cooperare între autoritățile de aplicare a legii, protecție civilă și sănătate publică.***

7. Combaterea amenințărilor generate de drone și protejarea spațiilor publice

Cadrul normativ și operațional propus de Comisie, tratează sistemele UAS[11] și dronele comerciale ca o vulnerabilitate emergentă majoră pentru securitatea europeană. Comunicarea evidențiază că accesibilitatea ridicată a acestor sisteme și utilizarea lor în conflictele recente demonstrează capacitatea actorilor ostili de a utiliza tehnologii comerciale pentru activități de supraveghere, sabotaj sau atac asupra infrastructurilor critice și spațiilor publice.

Pornind de la Comunicare a Comisiei privind contracararea amenințărilor reprezentate de drone[12] și Strategia europeană privind dronele 2.0,[13] Comisia promovează: ***dezvoltarea capacităților europene antidrone; consolidarea cooperării între poliție, frontieră și autoritățile aviatice; dezvoltarea unor platforme comune privind incidentele UAS; formare specializată pentru autoritățile competente.***

Totodată, cadrul conceptual agreat la nivelul instituțiilor europene dezvoltă conceptul de „*security by design*”[14], care reflectă schimbarea de paradigmă privind protecția infrastructurilor și a spațiilor publice. Astfel, securitatea nu mai este tratată ca o componentă suplimentară introdusă ulterior, ci ca un element integrat încă din faza de proiectare a infrastructurilor urbane și critice.

---

[9] Revizuirea Regulamentului (UE) 2019/1148 vizează consolidarea controalelor asupra precursorilor de explozivi și îmbunătățirea raportării tranzacțiilor online pentru a contracara utilizarea acestora în atacuri teroriste.

[10] Reevaluarea Directivei 2013/29/UE privind articolele pirotehnice, aflată în desfășurare, vizează consolidarea siguranței publice și îmbunătățirea funcționării pieței unice, cu un accent deosebit pe limitarea accesului la articole pirotehnice de mare putere și reducerea riscurilor asociate, conform datelor recente de pe EUR-Lex. [1, 2]

[11] Sistemele UAS (Unmanned Aircraft Systems) reprezintă ansamblul format dintr-o aeronavă fără pilot la bord (dronă/UAV) și echipamentul necesar pentru comanda și controlul acesteia de la distanță. Acestea includ stația de control, legătura de date și personalul operativ, fiind utilizate tot mai des pentru filmări, supraveghere, inspecții tehnice sau aplicații militare.

[12] COM (2023) 659

[13] COM(2022)652

[14] Comisia Europeană Security by Design: Protection of public spaces from terrorist attacks (Securitate de la stadiul conceperii: protejarea spațiilor publice împotriva atacurilor teroriste) (2023)

8. Consolidarea răspunsului operațional și a cooperării judiciare

Prin acest pilon se evidențiază necesitatea consolidării răspunsului coordonat al autorităților de aplicare a legii și al structurilor judiciare europene. Documentul promovează: ***intensificarea cooperării dintre Europol, Eurojust și statele membre; utilizarea extinsă a analizelor operaționale comune; dezvoltarea investigațiilor transfrontaliere; îmbunătățirea schimbului de probe digitale și informații judiciare.***

În acest context este trasată consolidarea capacității Uniunii Europene de a răspunde rapid și coordonat la atacuri și crize transfrontaliere.

9. Combaterea finanțării terorismului și a extremismului violent

Actualul cadru conceptual de securitate al Comisie, tratează finanțarea terorismului drept componentă esențială a nexus-ului dintre terorism și criminalitatea organizată.

Acțiunile-cheie ale Comisiei Europene promovează: consolidarea cooperării cu GAFI/FATF[15]; monitorizarea fluxurilor financiare alternative și digitale; combaterea utilizării criptomonedelor și canalelor informale; dezvoltarea mecanismelor europene de identificare a tranzacțiilor suspecte.

Strategia urmărește integrarea standardelor internaționale privind combaterea finanțării terorismului în cadrul european de securitate și cooperare judiciară.

10. Cooperarea internațională și dimensiunea externă a combaterii terorismului

Dimensiunea externă reprezintă unul dintre cele mai dezvoltate capitole ale Comunicării și este strâns corelată cu Comunicare Comună către Parlamentul European - menținerea păcii - foaia de parcurs privind pregătirea pentru apărare 2030[16] și Comunicare Comună către Parlamentul European, Scutul european pentru democrație: consolidarea democrațiilor puternice și reziliente[17].

Documentul evidențiază că amenințările teroriste au caracter transnațional și necesită o abordare integrată bazată pe: ***cooperare bilaterală; cooperare regională; parteneriate operaționale; consolidarea rezilienței statelor partenere***.

În cadrul Agendei ProtectEU, UE prioritizează acțiunile de securitate și prevenire a terorismului în zonele de proximitate critică: Balcanii de Vest - Integrare în securitatea UE și combaterea radicalizării, Orientul Mijlociu și Africa de Nord – Strategia europeană de gestionare a azilului și migrației; Regiunea Sahel**:** Stabilitate și combaterea criminalității organizate; Siria - Sprijin pentru tranziție și monitorizarea securității, evidențiază preocupările privind: rețelele jihadiste; combatanții teroriști străini; riscurile de reactivare a structurilor extremiste.

Documentul susține:

- integrarea treptată a partenerilor externi în arhitectura europeană de securitate;
- participarea acestora la activitățile Europol, Eurojust și CEPOL;
- dezvoltarea capacităților privind frontierele și combaterea radicalizării.

În acest context, inițiativa programatică a executivului European integrează securitatea

---

[15] Grupul de Acțiune Financiară Internațională, este organismul interguvernamental global care stabilește standarde pentru combaterea spălării banilor, finanțării terorismului și a proliferării armelor de distrugere în masă. Înființat în 1989, GAFI elaborează politici și evaluează conformitatea țărilor

[16] JOIN/2025/27 final

[17] JOIN(2025) 791 final

în abordarea „360 de grade” promovată prin Global Gateway, care corelează securitatea, diplomația, dezvoltarea și cooperarea economică. Astfel, propunerea evidențiază cooperarea cu: ONU; GAFI/FATF; GCTF; NATO; Interpol; Consiliul Europei; GIFCT.

11. Consolidarea rolului Uniunii Europene pe scena multilaterală

Consolidarea rolului Uniunii Europene pe scena multilaterală, dezvoltă explicit o dimensiune internațională și cooperativă a combaterii terorismului, consolidând poziția UE ca actor global de securitate. Această abordare se manifestă prin:

- **Multilateralism și Cooperare Internațională:** UE își intensifică colaborarea cu parteneri cheie (ex: Marea Britanie) și foruri multilaterale pentru a gestiona amenințările teroriste în continuă evoluție. Aceasta include utilizarea Ghidului privind Abordarea Comună în Lupta Împotriva Terorismului și a Strategiei Globale ONU, UE participând activ la pregătirea celei de-a noua revizuiri a acesteia în 2026.
- **Abordare Proactivă:** Strategia ProtectEU pune accent pe prevenirea radicalizării (în special a minorilor), securitatea cibernetică, combaterea finanțării terorismului și protejarea infrastructurilor critice, folosind un instrumentar de prevenție actualizat.
- **Actor Global de Securitate:** Prin revizuirea mandatelor agențiilor precum Europol și Eurojust și dezvoltarea capacității de apărare (Busola Strategică), UE reacționează la schimbările geopolitice, urmărind să fie un furnizor de securitate nu doar intern, ci și extern.
- **Tehnologie și Prevenție:** Agenda pune un accent puternic pe combaterea conținutului terorist online și utilizarea abuzivă a noilor tehnologii (IA, drone, arme 3D), colaborând cu sectorul privat.
- Prin urmare, combaterea terorismului nu mai este doar o competență internă a statelor membre, ci o componentă centrală a politicii externe și de securitate a UE, consolidată prin acțiuni comune, parteneriate strategice și mecanisme de sancționare (ex: Council Regulation (EU) 2026/456).

Comisia Europeană, Înaltul Reprezentant și coordonatorul UE pentru combaterea terorismului urmăresc***: consolidarea poziției UE în forurile multilaterale; valorificarea copreședinției UE în cadrul GCTF[18]; participarea activă la revizuirea Strategiei globale ONU de combatere a terorismului din 2026 , până la votul din iulie 2026, documentul juridic oficial activ care conține strategia completă este rezoluția precedentă adoptată de Adunarea Generală - acesta reprezintă textul consolidat pe cei 4 piloni, pe care statele membre îl folosesc ca bază de negociere pentru amendamentele din acest an***; ***aprofundarea cooperării cu GIFCT și Christchurch Call.***

Noua agendă a Uniunii Europene reflectă transformarea UE într-un actor de securitate multidimensional, orientat către gestionarea integrată a riscurilor și dezvoltarea unei capacități europene consolidate de prevenire, protecție și răspuns strategic în domeniul combaterii terorismului

III. POZIȚII ALE INSTITUȚIILOR EUROPENE

Consiliul Uniunii Europene

Consiliul Uniunii Europene susține consolidarea unei arhitecturi europene de securitate bazate pe interoperabilitate, schimb rapid de informații și consolidarea capacităților operaționale ale statelor membre.

[18] **GCTF (Forumul Global Combaterea Terorismului)**: Platformă internațională esențială pe care UE o co-prezidează și unde exportă standardele sale juridice stricte privind sancțiunile și listele teroriste.

În concluziile Consiliului JAI din 16 martie 2026, miniștrii subliniază necesitatea consolidării capacității UE de a contracara amenințările hibride, reafirmând angajamentul de a utiliza toate instrumentele disponibile pentru prevenirea, descurajarea și răspunsul la campaniile hibride care vizează Uniunea, statele membre și partenerii săi, indiferent de originea sau intensitatea acestora. Documentul condamnă activitățile hibride ale actorilor statali și nestatali, inclusiv sabotajul împotriva infrastructurii critice, atacurile cibernetice, manipularea și ingerința informațională străină, ingerințele în procesele electorale și instrumentalizarea migrației. În mod special, Consiliul denunță campaniile persistente și coordonate ale Rusiei și ale actorilor asociați, subliniind că UE va continua să răspundă ferm printr-o abordare strategică și coordonată pentru protejarea securității și stabilității europene.

Comitetul European al Regiunilor (CoR)

Comitetul European al Regiunilor susține consolidarea rolului autorităților locale și regionale în arhitectura europeană de securitate și prevenire a radicalizării. Se consideră că autoritățile locale reprezintă primul nivel de detecție timpurie a vulnerabilităților asociate radicalizării și polarizării sociale și promovează: dezvoltarea mecanismelor locale de prevenire a extremismului; protecția spațiilor publice; integrarea securității în politicile urbane și proiectele de infrastructură; dezvoltarea rezilienței comunitare; cooperarea dintre autoritățile locale, structurile de securitate și societatea civilă.

Pentru ca reziliența societală să fie eficientă, politicile europene trebuie aplicate direct în comunități. Această legătură este atestată oficial prin documentele emise de Comitetul Regiunilor:

❖ Avizul Comitetului Regiunilor (CIVEX-VIII/006) din 10 decembrie 2025, intitulat *„Perspective locale și regionale în punerea în aplicare a Strategiei europene de securitate internă ProtectEU”*. Avizul propune cere oficial integrarea conceptului de *„security by design”* (securitate prin proiectare) în dezvoltarea urbană, protejând spațiile publice prin soluții arhitecturale care nu alterează caracterul deschis al orașelor. În esență, ideile principale sunt:

- Integrarea oficială a autorităților locale și regionale în guvernanța și implementarea strategiei de securitate a UE (*ProtectEU*), într-un model de cooperare pe mai multe niveluri.
- Implicarea acestor autorități în domenii-cheie de securitate (poliție locală, prevenirea radicalizării, securitate cibernetică, protecția infrastructurii critice), în colaborare cu instituțiile UE și agenții precum Frontex, Europol și EMSA.
- Participarea lor formală la deciziile și finanțarea politicilor UE de securitate, inclusiv la elaborarea bugetului 2028–2035 și la crearea unei agende europene de securitate locală.

❖ Proiectul de Aviz din 24 martie 2026 (*Union Support for Internal Security **2028-2034***) susține necesitatea unei guvernanțe pe mai multe niveluri în cadrul sprijinului UE pentru securitatea internă 2028-2034. Avizul avertizează împotriva centralizării excesive și subliniază rolul strategic al autorităților locale în implementarea fondurilor, prin care autoritățile locale solicită în mod oficial descentralizarea Fondului pentru Securitate Internă (FSI) și alocarea de linii financiare europene directe către bugetele regionale și municipale pentru implementarea măsurilor de protecție cu acribie.

Europol și agențiile europene specializate

Europol ocupă un rol central în implementarea noii agende europene privind combaterea terorismului. Evaluările strategice EU-SOCTA 2025 și TE-SAT 2025, evidențiază o mutație severă a mediului de securitate: creșterea exponențială a complexității rețelelor infracționale și cristalizarea unui *nexus* structural între criminalitatea organizată, celulele teroriste și ecosistemul digital. Spațiul cibernetic nu mai reprezintă doar un simplu canal de

propagare a ideologiilor extremiste, ci a devenit infrastructura logistică de bază pentru finanțarea terorismului (prin active criptografice și platforme financiare descentralizate) și pentru recrutarea asimetrică. Pentru a contracara aceste amenințări transfrontaliere,
Europol promovează:

- capacități analitice avansate: Implementarea unor instrumente de *Big Data Analytics* capabile să proceseze și să coreleze volume masive de date nestructurate primite din statele membre.
- parteneriate public-private extinse**:** Cooperarea aprofundată cu marile platforme tehnologice și rețelele de gaming prin intermediul Forumului de Internet al UE, facilitând aplicarea procedurilor rapide de eliminare a propagandei în termen de maximum o oră, conform Regulamentului (UE) 2021/784.
- răspuns la amenințări emergente**:** Intensificarea investigațiilor sub umbrela platformei EMPACT privind liniile de aprovizionare cu arme de foc și materiale chimice, biologice, radiologice sau nucleare (CBRN), concomitent cu dezvoltarea unor standarde comune de securitate cibernetică și tehnologică pentru neutralizarea utilizării ofensive a sistemelor aeriene fără pilot (drone) în proximitatea infrastructurilor critice.

Eurojust și CEPOL

Această rețea de securitate internă este dublată de o coordonare judiciară riguroasă guvernată de Eurojust. Agenția susține consolidarea cooperării judiciare multilaterale prin maximizarea utilității Registrului Judiciar Antiterorist (CTR). Acest instrument permite centralizarea dosarelor penale deschise în statele membre, eliminând riscul de suprapunere a anchetelor și oferind magistraților mecanisme rapide de coordonare a urmăririi penale, a percheziților simultane și a executării eficiente a Mandatelor Europene de Arestare în cazurile de terorism transfrontalier.

Pe palierul pregătirii de personal, Agenția Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL) asigură sustenabilitatea capitalului uman din instituțiile de siguranță publică. Prin alinierea programelor sale didactice la noile rigori ale pieței unice digitale și la standardele de etică impuse de Actul privind Inteligența Artificială (AI Act), CEPOL livrează cursuri avansate de specializare destinate polițiștilor, axate pe:

- Identificarea timpurie a tehnicilor de radicalizare digitală a minorilor pe platformele de socializare și aplicațiile de gaming.
- Dezvoltarea de mecanisme de rezistență instituțională în fața campaniilor de dezinformare de tip hibrid.
- Utilizarea legală și auditabilă a algoritmilor de inteligență artificială în scopuri criminalistice și de control la frontierele externe.

În ansamblu, pozițiile și acțiunile convergente ale instituțiilor și agențiilor Uniunii Europene consacră o abordare multidimensională a securității, guvernată de principiile interoperabilității bazelor de date (sincronizarea operativă a sistemelor SIS, VIS, EES și ETIAS prin suportul tehnic al eu-LISA) și al integrării depline a dimensiunilor interne și externe ale apărării europene. Noua agendă antiteroristă nu mai reprezintă doar o grilă de standarde tehnice, ci este asumată la nivel instituțional drept instrumentul politic central pentru adaptarea pe termen lung a Uniunii Europene la transformările accelerate ale mediului strategic contemporan.

IV. INFORMAȚII ȘI EVOLUȚII REFERITOARE LA ROMÂNIA

Dimensiunea juridico-instituțională și convergența cu acquis-ul european

Din perspectivă normativă, România dispune de un cadru de reglementare consolidat și compatibil în mare măsură cu orientările europene actuale în materie de combatere a

terorismului și securitate internă.

Acest cadru este completat de legislația privind securitatea națională, prin ***Proiectul Legii securității naționale a României*** (destinat să înlocuiască integral Legea nr. 51/1991[19]; ***Regimul armelor și munițiilor***, prin Legea nr. 295/2004,republicată[20] corelată cu regimul european de control al fluxurilor de armament***;*** ***Combaterea spălării banilor și finanțării terorismului***, documentul oficial fundamental care reglementează măsurile de prevenire este Legea nr. 129/2019[21]*, precum și pentru modificarea și completarea unor acte normative;* ***Protecția infrastructurilor critice***, care are la bază Ordonanța de Urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor, acest act normativ de bază a fost aprobat prin Legea nr. 18/2011[22] și a suferit actualizări structurale succesive (inclusiv prin Legea nr. 344/2023[23]) pentru a extinde răspunderea operatorilor publici și privați pe linia securității naționale; S***ecuritatea cibernetică și gestionarea situațiilor de urgență***, fundamentat prin Legea nr. 58/2023[24], Legea nr. 124/2025[25] (care aprobă implementarea Directivei NIS 2 prin OUG nr. 155/2024)**[26]**

În acest context, România a implementat și transpus principalele instrumente legislative europene relevante pentru noua arhitectură europeană de securitate, inclusiv: Regulamentul UE[27] privind combaterea diseminării conținutului terorist online (TCO Regulation[28]); Directiva NIS și noile cerințe NIS2 privind securitatea cibernetică; legislația europeană privind precursorii de explozivi; normele europene privind schimbul de date API/PNR; cadrul european privind combaterea spălării banilor și finanțării terorismului[29]; standardele Schengen privind interoperabilitatea bazelor de date, managementul frontierelor externe și Inteligența Artificială (AI Act).

În plan instituțional, România promovează implementarea unei arhitecturi integrate de securitate compatibile cu modelul european[30] „multi-agency counter-terrorism”,este formalizat prin Legea 535/2004 privind prevenirea și combaterea terorismului, cu modificările și completările ulterioare care stabilește Sistemul Național de Prevenire și Combatere a Terorismului (SNPCT) sub coordonarea tehnică a SRI;

Această arhitectură instituțională reflectă o orientare clară către integrarea dimensiunilor interne și externe ale combaterii terorismului, în concordanță cu evoluțiile dezvoltate la nivelul Uniunii Europene prin ProtectEU[31], Strategia Uniunii[32] Securității, Strategia UE privind

[19] publicat în Monitorul Oficial, Partea I, nr.163 din 7 august 1991
[20] publicat în Monitorul Oficial nr. 425 din 10 iunie 2014
[21] publicat în Monitorul Oficial , Partea I , nr.589 din 18 iulie 2019
[22] publicat în Monitorul Oficial nr. 185 din 15 martie 2011
[23] publicat în Monitorul Oficial nr. 1019 din 13 noiembrie 2023
[24] publicat în Monitorul Oficial nr. 214 din 15 martie 2023
[25] publicat în Monitorul Oficial, Partea I, nr. 638 din 7 iulie 2025
[26] OUG nr. 155/2024 reprezintă actul normativ prin care România a transpus în legislația națională Directiva Europeană NIS 2 (Network and Information Security 2), vizând consolidarea securității cibernetice la nivelul entităților din sectoarele critice și importante.
[27] Regulamentul (UE) 2021/784 al Parlamentului European și al Consiliului din 29 aprilie 2021 privind prevenirea diseminării conținutului online cu caracter terorist (Text cu relevanță pentru SEE)
[28] **TCO Regulation** sau TCOR) este un set de norme europene obligatorii, aplicabile începând cu 7 iunie 2022. Acesta obligă furnizorii de servicii de găzduire (hosting) să elimine conținutul terorist în termen de o oră de la primirea unui ordin din partea autorităților.
[29] Regulamentul (UE) 2024/1624 al Parlamentului European și al Consiliului din 31 mai 2024 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului.
[30] Modelul european **„multi-agency counter-terrorism”** reprezintă o abordare integrată, de tip *whole-of-society*, care elimină barierele tradiționale dintre agențiile de securitate, instituțiile civile și sectorul privat pentru a combate terorismul pe întregul său ciclu de manifestare
[31] COM(2026) 101 final
[32] COM(2020) 605 final

combaterea terorismului[33] și documentele comune ale Comisiei Europene și Înaltului Reprezentant privind securitatea europeană integrate.[34] [35]

Prevenirea radicalizării și consolidarea rezilienței societale

Poziția României reflectă o convergență semnificativă cu orientarea europeană care tratează radicalizarea drept un fenomen multidimensional aflat la intersecția dintre securitate, educație, polarizare socială și vulnerabilități informaționale.

Această abordare integrată este transpusă oficial la nivel național prin **Strategia Națională pentru Prevenirea și Combaterea Antisemitismului, Xenofobiei, Radicalizării și a Discursului Instigator la Ură 2024-2027**, adoptată prin Hotărârea de Guvern nr. 540[36]. Documentul codifică juridic radicalizarea ca fenomen complex și instituie un mecanism de cooperare interinstituțională ce implică direct actori civili precum Ministerul Educației, Ministerul Culturii și universitățile alături de structurile tradiționale de securitate. Intersecția dintre polarizarea socială, vulnerabilitățile comunităților și riscurile de securitate este gestionată operațional prin Campania Guvernului României pentru Raportarea Incidentelor, un document-cadru administrat de Departamentul pentru Relații Interetnice.

Strategia Națională de Apărare a Țării pentru perioada 2025-2030 (SNAT) promovează o abordare integrată de tip *„whole-of-society”,* prin implicarea instituțiilor publice, a administrației locale, a sistemului educațional, a societății civile și a sectorului privat în consolidarea rezilienței democratice și în combaterea amenințărilor hibride, extremismului violent și campaniilor de influență ostilă.

Strategia Națională de Securitate Cibernetică este integrată în actuala Strategie Națională de Apărare a Țării prin dezvoltarea capacităților naționale de prevenire, detectare și răspuns la incidente cibernetice, fiind armonizată cu normele europene, inclusiv cu Directiva NIS2, transpusă prin Legea nr. 124/2025 privind cadrul pentru securitatea cibernetică.

[33] COM(2020) 795 final
[34] JOIN(2023) 20 final
[35] JOIN(2025) 130 final
[36] publicat în Monitorul Oficial, Partea I, Nr. 503 bis/30.V.2024