Consiliul
Uniunii Europene

Bruxelles, 18 octombrie 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	18 octombrie 2023
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2023) 665 final
Subiect:	COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU Al șaselea raport privind progresele înregistrate în punerea în aplicare a Strategiei UE privind uniunea securității

În anexă, se pune la dispoziția delegațiilor documentul COM(2023) 665 final.

Anexă: COM(2023) 665 final

COMISIA
EUROPEANĂ

Bruxelles, 18.10.2023
COM(2023) 665 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

Al șaselea raport privind progresele înregistrate în punerea în aplicare a Strategiei UE privind uniunea securității

I. Introducere

În urmă cu trei ani, Comisia a adoptat Strategia privind uniunea securității pentru perioada 2020-2025[1], care definește principalele priorități ale Uniunii în domeniul securității. De atunci, am înregistrat progrese semnificative în cadrul tuturor celor patru piloni ai strategiei, elaborând o legislație de referință în toate domeniile, de la protecția entităților critice la consolidarea rezilienței cibernetice. Între timp însă, situația amenințărilor la adresa securității din Europa și din vecinătatea noastră continuă să evolueze. Atacurile teroriste care au avut loc în ultimele zile într-una dintre școlile noastre din Franța și pe străzile din Bruxelles reiterează în mod acut necesitatea urgentă de a continua adaptarea și consolidarea arhitecturii noastre de securitate. Pericolul reprezentat de atacurile cibernetice continuă să crească, alimentat, de asemenea, de faptul că răuvoitori iau parte la conflictele actuale. Amenințările hibride, inclusiv dezinformarea, continuă să se înmulțească. Europol a identificat războiul de agresiune al Rusiei împotriva Ucrainei drept cauza unei creșteri semnificative a atacurilor cibernetice împotriva țintelor UE, atacurile majore fiind motivate politic și coordonate de grupuri de hackeri pro-ruși[2]. Acest lucru s-a resimțit în blocarea accesului la internet și în întreruperea unor servicii esențiale, cum ar fi rețelele energetice[3].

Strategia privind uniunea securității a fost concepută pentru a pregăti UE să facă față mai bine situației amenințărilor în continuă schimbare. Pe măsură ce ne-am confruntat cu crizele provocate de pandemie și de război, evenimentele au demonstrat importanța abordării adoptate în cadrul strategiei – hotărârea noastră de a crea o unitate în întregul ecosistem de securitate al UE și de a elimina barierele dintre dimensiunea cibernetică și dimensiunea fizică a securității, inclusiv combaterea criminalității organizate și a terorismului, precum și combaterea radicalizării.

Cu toate acestea, vigilența ne solicită să analizăm în permanență ce lipsește din eforturile noastre de a ne menține cetățenii în siguranță. Strategia a stabilit domeniile prioritare în care Uniunea poate aduce valoare adăugată pentru a sprijini statele membre în promovarea securității pentru toate persoanele care trăiesc în Europa. De la adoptarea sa, au fost abordate toate acțiunile stabilite și au fost incluse altele noi pentru a răspunde provocărilor actuale în materie de securitate.

În total, Comisia a prezentat 36 de inițiative legislative în cadrul Strategiei privind uniunea securității. Pentru mai mult de jumătate dintre aceste propuneri, negocierile interinstituționale s-au încheiat deja cu o nouă legislație solidă, astfel cum se descrie în tabelul din anexă. Cu toate acestea, mai multe inițiative-cheie propuse de Comisie sunt încă în curs de negociere de către Parlamentul European și Consiliu. Având în vedere că actuala legislatură parlamentară se va încheia odată cu alegerile europene din iunie 2024, sunt necesare eforturi rapide pentru a da curs acestor dosare restante, astfel încât cetățenii să poată beneficia pe deplin de uniunea securității. Prin urmare, acest al șaselea raport intermediar privind uniunea securității se axează pe evidențierea acelor dosare legislative și nelegislative esențiale privind uniunea securității

---

1 COM(2020) 605.

2 Atacurile *Distributed Denial of Service* (DDoS): a se vedea *Europol Spotlight Report „Cyber-attacks: the apex of crime-as-a-service"* (Raportul de sinteză al Europol „Atacurile cibernetice: apogeul infracționalității ca serviciu"), 13 septembrie 2023.

3 În timpul conflictului din Ucraina au fost utilizate în mod intensiv programe malware de tip *wiper* pentru a distruge date și sisteme, afectând, de exemplu, accesul la internet pentru mii de abonați din UE, precum și pentru o mare companie energetică germană care a pierdut accesul la monitorizarea de la distanță a peste 5 800 de turbine eoliene. Rolul ciberneticii în războiul Rusiei împotriva Ucrainei: impactul și consecințele sale asupra viitorului conflictului armat, studiu al Parlamentului European, septembrie 2023 – PE 702.594.

adoptate de Comisie, pentru care trebuie depuse mai multe eforturi în vederea finalizării și a punerii în aplicare efective.

În ceea ce privește actele legislative ale UE deja convenite, beneficiile acestora vor fi resimțite numai atunci când vor fi puse în practică. Activitatea trebuie să se concentreze asupra transpunerii, punerii în aplicare și aplicării corecte și integrale a acestora de către statele membre. În 2023, Comisia a continuat să se asigure că Strategia UE privind uniunea securității își îndeplinește obiectivele prin utilizarea competențelor sale instituționale pentru a iniția proceduri de constatare a neîndeplinirii obligațiilor ori de câte ori statele membre nu au transpus sau au transpus incorect legislația UE.

De asemenea, prezentul raport sintetizează situațiile în care acțiunile statelor membre și/sau ale agențiilor UE sunt esențiale pentru îndeplinirea obiectivelor. Agențiile UE joacă un rol esențial în sprijinirea punerii în aplicare a inițiativelor privind uniunea securității, iar responsabilitățile lor s-au dezvoltat în ultimii ani. Raportul prezintă unele dintre principalele sarcini noi care le-au fost alocate pentru a oferi un sprijin sporit statelor membre în punerea în aplicare a inițiativelor-cheie din cadrul uniunii securității.

În plus, situația geopolitică a subliniat importanța securității externe pentru securitatea noastră internă. Un cadru intern mai solid al UE în domeniul securității este legat în mod intrinsec de parteneriate și de o cooperare mai strânse cu țările terțe. UE trebuie să continue să urmărească în mod activ modul în care implicarea la nivel mondial poate contribui la asigurarea siguranței cetățenilor la domiciliu.

II. Un mediu de securitate adaptat exigențelor viitorului

Securitatea cibernetică și reziliența infrastructurii critice

În cadrul uniunii securității, Uniunea este hotărâtă să se asigure că toți cetățenii și toate întreprinderile europene beneficiază de protecție, atât online, cât și offline, și să promoveze un spațiu cibernetic deschis, sigur și stabil. Amploarea, frecvența și impactul în creștere ale incidentelor de securitate cibernetică reprezintă o amenințare majoră pentru funcționarea rețelelor și a sistemelor informatice și pentru piața internă. Războiul de agresiune al Rusiei împotriva Ucrainei a exacerbat și mai mult această amenințare, iar tensiunile geopolitice actuale sunt agravate de intervențiile unei multitudini de entități aliniate cu autoritățile guvernamentale, de infractori și hacktiviști. Sabotarea din toamna recentă a gazoductelor Nord Stream a evidențiat dependența unor sectoare esențiale, cum ar fi energia, infrastructura digitală, transporturile și spațiul, de reziliența infrastructurii critice. Incidentul recent care a implicat un gazoduct submarin și un cablu de date în Estonia și Finlanda ilustrează necesitatea unui nivel ridicat de pregătire pentru a face față acestui tip de situații. Deși cauza daunelor rămâne neclară, iar investigațiile sunt în curs, schimbul de informații la diferite niveluri între statele membre și Comisie a fost încurajator. Perturbările nu au avut niciun efect imediat în ceea ce privește conectivitatea la internet și nici în ceea ce privește securitatea aprovizionării cu gaze la nivel european sau local. Acesta este un semn al progreselor înregistrate și al eforturilor consolidate de pregătire din ultimele luni.

Prin urmare, un cadru juridic clar și solid este esențial pentru a asigura protecția și reziliența acestor infrastructuri critice. În acest context, un progres major a fost realizat prin adoptarea în paralel a Directivei revizuite privind măsuri pentru un nivel comun ridicat de securitate

cibernetică în Uniune (NIS2)[4] și a Directivei privind reziliența entităților critice (REC)[5], ambele intrând în vigoare la 16 ianuarie 2023. În prezent, statele membre sunt îndemnate să transpună rapid și complet aceste acte legislative fundamentale, cel târziu până la 17 octombrie 2024, pentru a institui un cadru solid la nivelul Uniunii pentru a proteja infrastructura critică a Uniunii împotriva amenințărilor fizice și cibernetice.

În iulie 2023, Comisia a stabilit, într-un regulament delegat al Comisiei, servicii esențiale în cele 11 sectoare care intră sub incidența Directivei REC[6]. Următorul pas este ca statele membre să efectueze evaluări ale riscurilor cu privire la aceste servicii. În urma recomandării Consiliului[7] din 8 decembrie 2022, s-au intensificat lucrările privind testele de rezistență pentru infrastructura critică, începând cu sectorul energetic, și privind consolidarea cooperării cu NATO și cu principalele țări partenere. Aceste lucrări au condus la elaborarea unui raport al Grupului operativ UE-NATO privind reziliența infrastructurii critice în iunie 2023, care cartografiază provocările actuale în materie de securitate pentru infrastructura critică în patru sectoare-cheie (energie, transporturi, infrastructura digitală și spațiu) și formulează recomandări pentru a spori reziliența. Recomandările, inclusiv cele privind intensificarea coordonării, a schimbului de informații și a exercițiilor, sunt puse în aplicare de personalul UE și al NATO în contextul dialogului structurat privind reziliența.

În paralel, la 6 septembrie 2023, Comisia a adoptat o propunere[8] de recomandare a Consiliului referitoare la un Plan de acțiune privind un răspuns coordonat la nivelul Uniunii la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă. La 4 octombrie 2023, a fost organizat un exercițiu sub forma unei discuții bazate pe scenarii cu privire la planul de acțiune, pentru a testa modul în care acesta s-ar aplica în practică și pentru a contribui la negocierile actuale cu privire la propunere în cadrul Consiliului.

În urma apelurilor din partea Consiliului[9], Comisia, Înaltul Reprezentant și Grupul de cooperare NIS au efectuat evaluări ale riscurilor și au elaborat scenarii de risc din perspectiva securității cibernetice. Această activitate se axează inițial pe sectorul telecomunicațiilor și pe cel al energiei electrice. Implicarea tuturor agențiilor și rețelelor relevante, civile și militare, creează pentru prima dată o evaluare cuprinzătoare și incluzivă la nivelul Uniunii. Aceasta va completa în continuare evaluările coordonate ale riscurilor de securitate la nivelul lanțurilor de aprovizionare critice care au loc în temeiul NIS2, precum și evaluările riscurilor și testele de rezistență a infrastructurii critice din sectorul energiei, al comunicațiilor pentru infrastructura digitală, al transporturilor și al spațiului. În interesul coordonării și al coerenței, aceste activități ar trebui să se bazeze unele pe altele pentru a contribui la stabilirea unei abordări standard și ar trebui să ghideze dezvoltarea exercițiilor viitoare. Succesul acestor acțiuni va depinde acum de implicarea activă a statelor membre.

Funcționarea economiilor și a societăților depinde tot mai mult de serviciile și datele spațiale, în special în domeniul securității și al apărării. Spațiul este un domeniu strategic din ce în ce mai contestat, iar importanța sa pentru securitate a crescut în special în urma invadării Ucrainei

---

4 Directiva (UE) 2022/2555 din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune și Directiva (UE) 2018/1972 (Directiva NIS 2).

5 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.

6 C(2023) 4878.

7 Recomandare a Consiliului din 8 decembrie 2022 privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice.

8 COM(2023) 526.

9 Concluziile Consiliului din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene și Apelul de la Nevers din 9 martie 2022 de consolidare a capacităților UE în materie de securitate cibernetică.

de către Rusia. Strategia spațială a UE pentru securitate și apărare a fost adoptată în martie 2023 pentru a ne consolida poziția strategică și autonomia în spațiu. Ca acțiune-cheie care decurge din această strategie, Comisia Europeană va propune în 2024 un act legislativ al UE privind spațiul care să reglementeze siguranța, durabilitatea și reziliența/securitatea activităților spațiale în UE.

Analizând dimensiunea externă, o infrastructură securizată stă la baza rezilienței economiei și a lanțurilor de aprovizionare mondiale[10] și, din acest motiv, Strategia „Global Gateway" a UE încorporează o puternică dimensiune de securitate. De asemenea, având în vedere interconexiunile dintre infrastructura UE și cea a țărilor partenere, este esențială continuarea cooperării internaționale pentru a consolida reziliența cibernetică la nivel mondial și pentru a sprijini un spațiu cibernetic liber, deschis, sigur și securizat.

Actul european privind reziliența cibernetică

Asigurarea faptului că consumatorii și întreprinderile se pot baza pe produse digitale sigure este de o importanță majoră pentru securitatea cibernetică europeană. Comisia a încercat să abordeze această necesitate în propunerea sa de act european privind reziliența cibernetică[11], adoptată la 15 septembrie 2022. Aceasta ar introduce cerințe orizontale obligatorii în materie de securitate cibernetică pentru produsele cu elemente digitale pentru o perioadă de cinci ani sau pentru întregul lor ciclu de viață (oricare dintre aceste perioade este mai scurtă). Astfel s-ar crea condițiile pentru proiectarea și dezvoltarea de produse cu elemente digitale care să fie sigure, prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu cât mai puține vulnerabilități cu putință. Aceasta ar reprezenta o etapă esențială în ridicarea standardelor de securitate cibernetică ale Europei în toate domeniile și este probabil să devină un punct de referință internațional, oferind avantaje clare pentru industria securității cibernetice a Uniunii pe piețele mondiale. Parlamentul European și Consiliul și-au adoptat pozițiile în iulie 2023, iar negocierile ar trebui să avanseze rapid.

Certificarea securității cibernetice joacă, de asemenea, un rol esențial în creșterea încrederii în produsele și serviciile TIC, permițând consumatorilor, întreprinderilor și autorităților să facă alegeri în cunoștință de cauză, cu un nivel adecvat de securitate cibernetică. Se înregistrează progrese în ceea ce privește certificarea securității cibernetice, sistemul UE de certificare a securității cibernetice bazat pe criterii comune fiind evaluat în cadrul procedurii de comitologie. Propunerea de sistem al UE de certificare a securității în cloud (*EU Cloud Security Certification Scheme* – EUCS) este în curs de pregătire de către Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și este discutată în cadrul Grupului european pentru certificarea securității cibernetice. Activitatea intensă desfășurată cu experți din mai multe sectoare, consumatori și furnizori ar trebui să conducă la o abordare juridică și tehnică solidă, care să ofere garanțiile de securitate necesare în conformitate cu dreptul Uniunii, cu angajamentele internaționale și cu obligațiile OMC. În plus, ENISA pregătește propunerea de sistem EU5G și portofelul UE pentru identitatea digitală (EUIDW). Eforturile concertate ale tuturor statelor membre sunt esențiale pentru a consolida securitatea generală a produselor TIC, a serviciilor TIC și a proceselor TIC.

Regulamente privind securitatea informațiilor și securitatea cibernetică pentru instituțiile, organele și agențiile UE (IOAUE)

Propuse împreună în martie 2022, propunerile de regulamente care să reglementeze securitatea cibernetică și securitatea informațiilor pentru instituțiile proprii ale Uniunii au evoluat în ritmuri

[10] JOIN(2021) 30.
[11] COM(2022) 454.

diferite. În luna iunie a anului trecut, s-a ajuns la un acord politic cu privire la regulamentul privind securitatea cibernetică, care permite consolidarea posturii în materie de securitate cibernetică a tuturor instituțiilor, organelor, oficiilor și agențiilor UE și care reflectă importanța pe care UE o acordă punerii rapide în aplicare a acestei propuneri. În această situație, este deosebit de îngrijorător faptul că propunerea paralelă privind securitatea informațiilor, esențială pentru finalizarea unui cadru legislativ solid pentru IOAUE, a înregistrat progrese neașteptat de lente. Ambele propuneri ar trebui să fie adoptate înainte de alegerile parlamentare europene pentru a face administrația europeană credibilă și rezilientă în contextul geopolitic actual. Un set minim de norme și standarde de securitate a informațiilor pentru toate IOAUE ar crea certitudine pentru toate părțile implicate și ar asigura o protecție coerentă împotriva amenințărilor în continuă evoluție la adresa informațiilor lor, atât cele clasificate, cât și cele neclasificate ale UE. Luate în considerare împreună, aceste norme noi ar oferi o bază stabilă pentru schimbul securizat de informații între IOAUE și cu statele membre, cu practici și măsuri standardizate de protejare a fluxurilor de informații. Ca atare, ele răspund numeroaselor solicitări ale Consiliului de a spori reziliența IOAUE și de a proteja mai bine procesul decizional al Uniunii împotriva ingerințelor răuvoitoare.

Regulamentul privind solidaritatea cibernetică

Pornind de la cadrul strategic, politic și legislativ solid deja în vigoare, propunerea de regulament al UE privind solidaritatea cibernetică[12], adoptată de Comisie la data de 18 aprilie 2023, va îmbunătăți și mai mult detectarea amenințărilor cibernetice, reziliența și gradul de pregătire la toate nivelurile a ecosistemului de securitate cibernetică al Uniunii. Aceste obiective ar urma să fie puse în aplicare prin intermediul a trei acțiuni principale:

(1) implementarea unui ***scut cibernetic european*** pentru a construi și a consolida capabilitățile comune de detectare și de conștientizare a situației. Acesta este format din toate centrele naționale de operațiuni de securitate (denumite în continuare „SOC naționale”) și din centrele transfrontaliere de operațiuni de securitate (denumite în continuare „SOC transfrontaliere”);
(2) crearea unui ***mecanism pentru situații de urgență cibernetică*** pentru a sprijini statele membre să se pregătească pentru incidentele de securitate cibernetică semnificative și de mare amploare, să răspundă la acestea și să se redreseze imediat în urma lor. Sprijinul pentru răspunsul la incidente ar include rezerva UE pentru securitate cibernetică, care ar fi pusă, de asemenea, la dispoziția instituțiilor, organelor, oficiilor și agențiilor Uniunii Europene (IOAUE) și țărilor terțe asociate la programul „Europa digitală”, cu condiția ca acordul lor de asociere la programul „Europa digitală” să prevadă acest lucru;
(3) instituirea unui ***mecanism european de evaluare a incidentelor de securitate cibernetică*** pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. Raportul de examinare post-incident ar urma să fie coordonat și întocmit de ENISA.

Au început discuțiile în cadrul Consiliului și al Parlamentului European. Încheierea negocierilor înainte de sfârșitul actualului mandat al Parlamentului European ar da un impuls major eforturilor de protejare a cetățenilor și a întreprinderilor din întreaga Uniune.

Academia UE de competențe în materie de securitate cibernetică

[12] COM(2023) 209.

În timp ce amenințările cibernetice sunt în creștere, UE are nevoie urgent de profesioniști cu aptitudini și competențe adecvate pentru a preveni, detecta, descuraja și apăra UE împotriva atacurilor cibernetice. Nevoile sale de forță de muncă în domeniul securității cibernetice sunt estimate în prezent la 883 000 de profesioniști, în timp ce posturile vacante neocupate au variat între 260 000 și 500 000 în 2022. Toate segmentele societății ar trebui să fie încurajate să contribuie la acoperirea acestui deficit, dar, în special în 2022, femeile au reprezentat doar 20 % dintre absolvenții din domeniul securității cibernetice și 19 % dintre specialiștii în tehnologia informației și comunicațiilor. În cadrul Anului european al competențelor 2023, Comisia a adoptat, la 18 aprilie 2023[13], o inițiativă salutată de statele membre[14] de a înființa o Academie de competențe în materie de securitate cibernetică pentru a elimina deficitul de talente în materie de securitate cibernetică. Academia de competențe în materie de securitate cibernetică ar reuni inițiativele existente privind competențele în materie de securitate cibernetică și ar îmbunătăți coordonarea. Comisia încurajează statele membre, autoritățile regionale și locale, precum și entitățile publice europene, să adopte strategii sau inițiative specifice privind competențele în materie de securitate cibernetică sau să integreze competențele în materie de securitate cibernetică în strategiile sau inițiativele relevante cu un domeniu de aplicare mai larg (de exemplu, securitatea cibernetică, competențele digitale, ocuparea forței de muncă etc.). Implicarea părților interesate din sectorul privat va fi, de asemenea, esențială pentru a reduce deficitul de competențe în materie de securitate cibernetică și deficitul de forță de muncă asociat în Europa.

Drone

O altă amenințare tot mai mare la adresa spațiilor publice și a infrastructurilor critice este utilizarea răuvoitoare a dronelor. Incidentele care implică drone au devenit mai frecvente în interiorul și în afara Uniunii, iar soluțiile de contracarare a dronelor reprezintă un instrument-cheie pentru autoritățile de aplicare a legii și pentru alte autorități publice din Uniune, precum și pentru operatorii privați de infrastructură critică. În același timp, utilizarea legitimă a dronelor aduce o contribuție importantă la dubla tranziție verde și digitală[15]. După cum s-a anunțat în Strategia 2.0 privind dronele, adoptată în noiembrie 2022, Comisia adoptă astăzi o comunicare privind modalitățile de contracarare a potențialelor amenințări reprezentate de drone, susținută de două manuale cu orientări practice privind aspectele tehnice esențiale[16]. Inițiativa urmărește să ofere un cadru de politică cuprinzător și armonizat, cu o înțelegere comună a normelor în vigoare pentru a combate posibilele amenințări reprezentate de drone și pentru a se adapta, după caz, la evoluțiile rapide ale tehnologiei. Statele membre și operatorii privați relevanți sunt invitați să colaboreze îndeaproape cu Comisia pentru a asigura punerea în aplicare integrală a acestei inițiative.

Securitatea maritimă și aeronautică

Activitățile ilicite, cum ar fi pirateria, jaful armat pe mare, introducerea ilegală de migranți și traficul de persoane, arme și narcotice, precum și terorismul, rămân provocări pentru securitatea maritimă și sunt agravate de amenințările aflate în continuă evoluție, de atacurile hibride și cibernetice. La 10 martie 2023, Comisia și Înaltul Reprezentant au adoptat o comunicare comună de actualizare a Strategiei UE în materie de securitate maritimă[17], care ar trebui acum să fie pusă în aplicare în conformitate cu planul de acțiune actualizat.

[13] COM(2023) 207.
[14] Concluziile Consiliului din 22 mai 2023 privind politica UE în domeniul apărării cibernetice.
[15] COM(2022) 652.
[16] COM(2023) 659.
[17] JOIN(2023) 8.

În domeniul securității aeronautice, la 2 februarie 2023, Comisia a adoptat un document de lucru al serviciilor Comisiei intitulat „Working towards an enhanced and more resilient aviation security policy” (Către o politică de securitate aeronautică consolidată și mai rezilientă)[18], care conține un program ambițios de (1) modernizare a arhitecturii de reglementare pentru securitatea aeronautică, (2) de promovare a dezvoltării și a adoptării unor soluții mai inovatoare; și (3) de actualizare a nivelului de referință în materie de securitate aeronautică, astfel încât aeroporturile din Uniune să poată beneficia pe deplin de tehnologii noi și de vârf pentru a aborda amenințările cu cel mai înalt nivel de prioritate. Un număr de 14 acțiuni emblematice trebuie puse în aplicare în termen de doi ani.

Comisia invită Parlamentul European și Consiliul să finalizeze negocierile în regim de urgență, în orice caz înainte de încheierea mandatului actualului Parlament European, cu privire la următoarele dosare:

- propunerea de act european privind reziliența cibernetică;
- propunerea de regulament privind solidaritatea cibernetică;
- propunerea de regulament privind securitatea informațiilor pentru IOAUE.

Comisia invită statele membre:

- să urmărească transpunerea cu prioritate a Directivei privind reziliența entităților critice, precum și testarea rezistenței la stres a infrastructurii critice din sectorul energetic;
- să adopte Recomandarea Consiliului referitoare la un Plan de acțiune privind un răspuns coordonat la perturbări ale infrastructurii critice cu o relevanță transfrontalieră semnificativă;
- să transpună pe deplin și de urgență Directiva NIS2 pentru a stimula securitatea cibernetică a entităților esențiale și importante;
- să se implice activ în efectuarea de evaluări ale riscurilor în materie de securitate cibernetică și în elaborarea de scenarii de risc pentru infrastructura critică și lanțurile de aprovizionare;
- să urmărească Academia de competențe în materie de securitate cibernetică, cu un angajament puternic la nivel european și cu strategii sau inițiative naționale dedicate privind competențele în materie de securitate cibernetică, implicând principalele părți interesate, inclusiv autoritățile regionale și locale;
- să colaboreze cu operatorii privați relevanți și cu Comisia pentru a asigura punerea în aplicare a tuturor acțiunilor enumerate în Comunicarea privind combaterea amenințărilor potențiale cauzate de drone;
- să pună în aplicare Planul de acțiune privind Strategia UE în materie de securitate maritimă și să prezinte rapoarte periodice cu privire la realizări;
- să pună în aplicare cele 14 acțiuni emblematice identificate pentru consolidarea securității aeronautice.

III. Combaterea amenințărilor aflate în continuă evoluție

[18] SWD(2023) 37.

Noile tensiuni geopolitice au oferit dovezi clare cu privire la modul în care provocarea în materie de securitate cu care se confruntă UE nu numai că crește, ci este din ce în ce mai volatilă și accentuată de natura hibridă a multor amenințări. De asemenea, securitatea trebuie să răspundă schimbărilor din societate și tehnologie. Pandemia de COVID-19 a sporit oportunitățile pentru infractorii cibernetici și a determinat, în special, o creștere a amenințării reprezentate de materialele online care conțin abuzuri sexuale asupra copiilor. Infractorii și răuvoitorii sunt întotdeauna pregătiți să exploateze evoluțiile tehnologice. În fața unor astfel de amenințări adesea complexe și multidimensionale, este necesară o acțiune puternică și coerentă a UE.

Regulamentul privind combaterea abuzului sexual online asupra copiilor

Evaluarea amenințării pe care o reprezintă criminalitatea organizată online efectuată de Europol a arătat că, în 2022, exploatarea sexuală a copiilor și abuzul sexual asupra copiilor au crescut și mai mult în ceea ce privește frecvența și gravitatea, infractorii continuând să profite de posibilitățile tehnice pentru a-și masca acțiunile și identitățile[19]. Sistemul actual, bazat pe detectarea și raportarea voluntară de către întreprinderi, s-a dovedit insuficient pentru a proteja copiii. Un regulament provizoriu permite detectarea și raportarea voluntară de către întreprinderi, cu condiția ca aceste acțiuni să fie legale în temeiul Regulamentului general privind protecția datelor (RGPD). Acest regulament va expira în august 2024. În mai 2022, Comisia a propus un regulament[20] pentru a combate utilizarea necorespunzătoare a serviciilor online în scopul abuzului sexual asupra copiilor. Cadrul propus pune un accent puternic pe prevenire. Întreprinderile ar fi obligate să evalueze riscul de abuz sexual asupra copiilor prin intermediul sistemelor lor și să ia măsuri preventive. Ca măsură de ultimă instanță, numai în cazul unui risc semnificativ, instanțele naționale sau autoritățile administrative independente ar putea emite ordine de detectare specifice pentru furnizorii de servicii. Un nou centru independent al UE privind abuzul sexual asupra copiilor ar facilita eforturile furnizorilor de servicii, acționând ca un centru de expertiză, furnizând informații fiabile cu privire la materialele identificate, primind și analizând rapoartele online ale furnizorilor privind abuzul sexual asupra copiilor pentru a identifica rapoartele eronate, precum și oferind sprijin victimelor. Este esențial ca noile norme să fie adoptate și puse în aplicare cât mai curând posibil pentru a proteja copiii împotriva altor abuzuri, pentru a preveni reapariția online a materialelor și pentru a-i aduce pe infractori în fața justiției. Negocierile sunt în desfășurare în cadrul Consiliului și al Parlamentului, cu scopul de a ajunge la un acord cu privire la acest dosar înainte de încheierea mandatului Parlamentului.

Directiva privind combaterea violenței împotriva femeilor și a violenței domestice

Violența cibernetică împotriva femeilor, inclusiv în contextul violenței domestice, a apărut ca o nouă formă a actelor de violență, răspândindu-se dincolo de granițele statelor membre individuale, prin intermediul internetului și al instrumentelor informatice. În martie 2022, Comisia a propus o directivă privind combaterea violenței împotriva femeilor și a violenței domestice, inclusiv norme specifice privind violența cibernetică și măsuri de eliminare a lacunelor în materie de protecție, acces la justiție și prevenire. Adoptarea și punerea în aplicare timpurie ar oferi statelor membre instrumente suplimentare pentru a combate această formă de criminalitate. Colegiuitorii s-au angajat în negocieri interinstituționale în iulie 2023 și își propun să finalizeze negocierile înainte de încheierea mandatului actual al Parlamentului European.

[19] Europol (2023), „Internet Organised Crime Threat Assessment" (IOCTA) (Evaluarea amenințării pe care o reprezintă criminalitatea organizată online), 2023.

[20] COM(2022) 209.

Securitatea cibernetică a rețelelor 5G

Securitatea rețelelor 5G este o prioritate majoră pentru Comisie și o componentă esențială a strategiei sale privind uniunea securității. Rețelele 5G reprezintă o infrastructură centrală, care asigură baza unei game largi de servicii esențiale pentru funcționarea pieței interne și pentru funcții societale și economice vitale. La 15 iunie 2023, autoritățile statelor membre ale UE reprezentate în Grupul de cooperare NIS, cu sprijinul Comisiei și al ENISA, au publicat un al doilea raport intermediar privind punerea în aplicare a setului de instrumente al UE privind securitatea cibernetică a rețelelor 5G. Potrivit raportului, 24 de state membre au adoptat sau pregătesc măsuri legislative prin care conferă autorităților naționale competența de a efectua o evaluare a furnizorilor și de a emite restricții, iar 10 state membre au impus astfel de restricții. Cu toate acestea, sunt necesare măsuri suplimentare pentru a evita vulnerabilitățile pentru Uniune în ansamblu, cu un impact negativ potențial grav asupra securității utilizatorilor individuali și a întreprinderilor din întreaga Uniune, precum și asupra infrastructurii critice a Uniunii. Toate statele membre trebuie să pună în aplicare setul de instrumente fără întârziere. În aceeași zi, Comisia a adoptat o comunicare privind punerea în aplicare a setului de instrumente de către statele membre și privind comunicațiile instituționale ale Comisiei și activitățile de finanțare ale Uniunii. Aceasta a subliniat profunda îngrijorare cu privire la riscurile pentru securitatea UE pe care le prezintă furnizorii de echipamente de comunicații pentru rețele mobile Huawei și ZTE. În acest context, Comisia ia măsuri pentru a evita expunerea comunicațiilor sale instituționale către rețelele mobile care utilizează Huawei și ZTE ca furnizori. Achizițiile vor exclude noile servicii de conectivitate care se bazează pe echipamente de la acești furnizori, iar Comisia va colabora cu statele membre și cu operatorii de telecomunicații pentru a se asigura că furnizorii respectivi sunt eliminați treptat din serviciile de conectivitate existente ale sediilor Comisiei. Comisia analizează, de asemenea, modul în care această decizie poate să se reflecte în programele și instrumentele de finanțare relevante ale Uniunii, în deplină conformitate cu dreptul Uniunii.

Accesul la date pentru o asigurare eficace a respectării legii

În era digitală de astăzi, aproape fiecare infracțiune are o componentă digitală. Tehnologiile și instrumentele sunt utilizate, de asemenea, în scopuri infracționale, inclusiv cele care sunt necesare pentru a garanta că societatea noastră are nevoie de securitate cibernetică, de protecție a datelor și de confidențialitate. Acest lucru face tot mai dificilă menținerea unei asigurări eficace a respectării legii în întreaga UE pentru a proteja securitatea publică și pentru a preveni, detecta, investiga și urmări penal infracțiunile. Deși s-au depus eforturi semnificative la nivelul Uniunii și la nivel național, inclusiv prin legislație, precum și prin inițiative de consolidare a capacităților și de inovare, persistă provocări juridice și tehnice. Comisia, care asociază președinția Consiliului, a înființat un grup la nivel înalt privind accesul la date pentru o asigurare eficace a respectării legii pentru a oferi o platformă de colaborare pentru o gamă largă de părți interesate și experți în vederea explorării provocărilor cu care se confruntă practicienii din domeniul asigurării respectării dreptului penal (de exemplu, criptarea, păstrarea datelor, 5G și standardizarea). Comisia se așteaptă ca grupul la nivel înalt să formuleze recomandări echilibrate, solide și realizabile până în iunie 2024, care să reflecte complexitatea acestor aspecte, inclusiv din perspectiva securității cibernetice și a protecției datelor. Prin urmare, statele membre și experții participanți sunt încurajați să se implice activ în acest proces și să depună eforturi în vederea găsirii unor soluții eficace, legale și general acceptate.

Amenințările hibride

Într-un context geopolitic în care amenințările hibride devin tot mai complexe și mai sofisticate, Busola strategică a UE pentru securitate și apărare[21] (Busola strategică) a furnizat o evaluare comună a amenințărilor și provocărilor cu care se confruntă Uniunea, precum și un plan de acțiune strategic. Intensificarea activității cibernetice răuvoitoare din partea statelor și a entităților nestatale, inclusiv în contextul războiului împotriva Ucrainei, a pus în evidență și mai mult spațiul cibernetic ca domeniu de politică externă și de securitate. Riscurile potențiale ale acțiunilor răuvoitoare și ale dezinformării impun o vigilență deosebită în perioadele electorale, inclusiv în perioada premergătoare alegerilor europene din 2024.

Având în vedere riscurile ridicate de efecte de propagare, UE a continuat să dezvolte activități de consolidare a capacităților cibernetice și să promoveze parteneriate cu țări terțe, inclusiv prin dialoguri cibernetice specifice, pentru a contribui în mod activ la reziliența sa generală. O serie de instrumente au fost elaborate, revizuite și consolidate pentru a spori capacitatea Uniunii de a aborda în mod eficace amenințările hibride, astfel cum se descrie în cel de Al șaptelea raport intermediar privind amenințările hibride, publicat la 14 septembrie 2023[22]. Printre aceste instrumente se numără:

- setul de instrumente al UE pentru contracararea amenințărilor hibride, pentru a asigura un cadru pentru un răspuns coordonat și bine informat la amenințările hibride și campaniile hibride;
- activitatea în curs pentru a înființa echipe ale UE de răspuns rapid la amenințările hibride pentru un sprijin adaptat pe termen scurt pentru statele membre, țările partenere și misiunile și operațiunile din cadrul politicii de securitate și apărare comună (PSAC);
- Protocolul revizuit al UE pentru combaterea amenințărilor hibride („EU Playbook”)[23], care descrie procesele și structurile Uniunii care abordează amenințările hibride și campaniile hibride;
- orientările revizuite de punere în aplicare a Cadrului privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare[24] („setul de instrumente pentru diplomația cibernetică”), care permite dezvoltarea unor strategii susținute, adaptate, coerente și coordonate împotriva entităților care reprezintă amenințări cibernetice persistente;
- setul de instrumente pentru combaterea acțiunilor străine de manipulare a informațiilor și a ingerințelor străine (FIMI), pentru a consolida instrumentele existente ale Uniunii pentru prevenirea, descurajarea și răspunsul la FIMI;
- politica UE în domeniul apărării cibernetice[25], pentru a stimula capacitățile de apărare cibernetică ale UE, a spori conștientizarea situației și a coordona întreaga gamă de opțiuni defensive disponibile, pentru a consolida reziliența, a răspunde la atacurile cibernetice și a asigura solidaritatea și asistența reciprocă.

Prin urmare, statele membre sunt încurajate să își continue și să își consolideze cooperarea în acest domeniu, asigurând punerea în aplicare eficace a seturilor de instrumente menționate mai sus, inclusiv prin exerciții periodice, și ajungând la un acord cu privire la conceptul de echipe de răspuns rapid la amenințările hibride, care va oferi orientări pentru etapele ulterioare în vederea înființării acestor echipe.

IA în contextul asigurării respectării legii

[21] Documentul 7371/22 al Consiliului.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 din 8 iunie 2023.
[25] JOIN(2022) 49.

Inteligența artificială (IA) a devenit rapid o caracteristică comună a vieții de zi cu zi. Efectele utilizării IA asupra criminalității informatice și a securității cibernetice nu sunt încă pe deplin cunoscute, dar este evident că vor crea noi provocări. Deși poate aduce beneficii atunci când este utilizată într-un mod sigur și controlat, IA poate avea un potențial periculos dacă ajunge în mâinile unor răuvoitori, inclusiv prin faptul că îi ajută pe infractori să își ascundă identitatea în infracțiuni precum terorismul și abuzul sexual asupra copiilor. Prin urmare, este esențial ca autoritățile să rămână la curent cu evoluțiile pentru a preveni abuzurile și a răspunde la utilizarea abuzivă[26]. Negocierile referitoare la propunerea de lege privind inteligența artificială vizează abordarea acestor aspecte și au intrat într-o etapă crucială, colegiuitorii discutând în prezent chestiuni tehnice și politice care vor determina interacțiunile cu această tehnologie în anii următori. Va fi esențial să se găsească soluții echilibrate, în special în ceea ce privește aplicațiile cu risc ridicat, inclusiv în domeniul asigurării respectării legii.

Comisia invită Parlamentul European și Consiliul să finalizeze negocierile interinstituționale în regim de urgență, în orice caz înainte de încheierea mandatului actualului Parlament European, cu privire la următoarele dosare aflate în curs:

- propunere de regulament privind combaterea abuzului sexual online asupra copiilor;
- propunere de directivă privind combaterea violenței împotriva femeilor și a violenței domestice;
- propunere de regulament de stabilire a unor norme armonizate privind inteligența artificială (Legea privind IA).

Comisia invită statele membre:

- să finalizeze fără întârziere punerea în aplicare integrală a setului de instrumente al UE privind securitatea cibernetică a rețelelor 5G;
- să sprijine activitatea Grupului la nivel înalt privind accesul la date pentru o asigurare eficace a respectării legii, în vederea formulării unor recomandări clare, solide și realizabile pentru a aborda în mod proporțional provocările actuale și anticipate;
- să ia măsuri, în cooperare cu Înaltul Reprezentant, pentru a asigura punerea în aplicare eficace a setului de instrumente al UE pentru contracararea amenințărilor hibride, a setului de instrumente revizuit pentru diplomația cibernetică și a setului de instrumente privind FIMI, inclusiv prin exerciții periodice și ținând seama de dinamica globală;
- să ajungă la un acord cu privire la conceptul de echipe de răspuns rapid la amenințările hibride.

IV. Protejarea europenilor împotriva terorismului și a criminalității organizate

Riscul ca evenimentele globale sau locale să declanșeze noi focare de terorism este mereu prezent. În paralel, criminalitatea organizată și traficul de droguri se numără printre cele mai grave amenințări la adresa securității UE. Pentru a intensifica eforturile colective ale Uniunii de combatere a acestor amenințări, sunt în desfășurare activități colective în ceea ce privește

[26] A se vedea, de exemplu, raportul Europol publicat la 17 aprilie 2023: „ChatGPT – the impact of Large Language Models on Law Enforcement” (ChatGPT – impactul modelelor lingvistice mari asupra asigurării respectării legii).

punerea în aplicare a Strategiei UE de combatere a criminalității organizate[27], a Strategiei UE privind combaterea traficului de persoane[28], a Agendei și Planului de acțiune ale UE în materie de droguri[29] și a Agendei UE privind combaterea terorismului[30]. Cu toate acestea, pentru a răspunde unei deteriorări îngrijorătoare a situației în ceea ce privește criminalitatea organizată și traficul de droguri, este necesară o intensificare suplimentară a eforturilor statelor membre și ale UE pentru a consolida răspunsul nostru colectiv la rețelele infracționale și pentru a proteja mai bine victimele criminalității, iar o foaie de parcurs a UE pentru combaterea traficului de droguri și a criminalității organizate este publicată în același timp cu prezentul raport[31].

În domeniul combaterii terorismului, UE își consolidează, de asemenea, setul de instrumente externe[32], utilizând la maximum dialogurile la nivel înalt privind combaterea terorismului și rețeaua experților în combaterea terorismului/securitate din cadrul delegațiilor UE, precum și prin implicarea sa în forurile multilaterale, inclusiv în calitate de copreședinte al Forumului mondial pentru combaterea terorismului (*Global Counter-Terrorism Forum* – GCTF).

Traficul de droguri

Odată cu noul mandat al Agenției pentru Droguri a Uniunii Europene, care se va aplica începând din luna iulie 2024, UE va fi mai bine pregătită pentru a rezolva o problemă complexă de securitate și de sănătate care afectează milioane de persoane în UE și la nivel mondial. De asemenea, Comisia revizuiește[33] regulamentele privind precursorii de droguri[34] pentru a aborda principalele provocări identificate în evaluarea din 2020[35], care a subliniat necesitatea de a aborda provocările reprezentate de precursorii de sinteză[36] pentru a reduce oferta de droguri ilegale.

Cu toate acestea, în contextul unei creșteri fără precedent a numărului de droguri ilicite disponibile în Europa, lupta împotriva traficului de droguri trebuie să se intensifice, în cooperare cu partenerii internaționali. Sunt necesare acțiuni suplimentare din partea statelor membre și a UE pentru a dezmembra rețelele infracționale și pentru a proteja mai bine victimele criminalității. Comisia prezintă astăzi o foaie de parcurs a UE pentru combaterea traficului de droguri și a criminalității organizate. Aceasta stabilește 17 acțiuni în patru domenii prioritare: consolidarea rezilienței centrelor logistice prin intermediul unei alianțe portuare europene, dezmembrarea rețelelor infracționale, intensificarea eforturilor de prevenire și consolidarea cooperării cu partenerii internaționali. Aceste acțiuni urmează să fie puse în aplicare în 2024 și 2025.

Armele de foc

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM(2023) 641.
[32] Astfel cum se solicită în Busola strategică și în Concluziile Consiliului privind abordarea dimensiunii externe a unei amenințări teroriste și extremiste violente în continuă evoluție, cu accent pe dimensiunea externă, adoptate în iunie 2022.
[33] Precursorii de droguri – legislația UE (revizuirea normelor) (europa.eu).
[34] Regulamentul (CE) nr. 273/2004 privind precursorii drogurilor și Regulamentul (CE) nr. 111/2005 al Consiliului de stabilire a normelor de monitorizare a comerțului cu precursori de droguri între Comunitate și țările terțe.
[35] COM(2020) 768.
[36] Acțiunea 23 din Planul de acțiune în materie de droguri, COM(2020) 606.

Traficul de arme de foc alimentează criminalitatea organizată din UE, precum și din vecinătate. Potrivit estimărilor, în UE nu mai puțin decât 35 de milioane de arme de foc ilegale sunt deținute de civili, iar aproximativ 630 000 de arme de foc sunt declarate pierdute sau furate în Sistemul de informații Schengen. Odată cu dezvoltarea livrării rapide de colete și a noilor tehnologii, cum ar fi imprimarea 3D, traficul de arme de foc capătă forme noi în încercarea de a evita controalele. Războiul de agresiune al Rusiei împotriva Ucrainei a crescut, de asemenea, riscul proliferării armelor de foc. În octombrie 2022, Comisia a adoptat o propunere de actualizare a legislației existente privind importul, exportul și tranzitul de arme de foc pentru uz civil, pentru a elimina lacunele din normele existente care pot crește numărul de arme de foc introduse ilegal și deturnate către UE[37]. Pe termen mediu, aceste norme noi vor contribui la reducerea riscului de eludare a embargourilor aplicate în cazul exporturilor de arme de foc pentru uz civil și la intensificarea controalelor la importul acestui tip de arme de foc din țări din afara UE. Ambii colegiuitori trebuie în continuare să își adopte pozițiile cu privire la acest dosar, cu scopul de a ajunge la un acord referitor la acesta înainte de încheierea mandatului actualului Parlament.

Traficul de persoane

Traficul de persoane este o formă deosebit de gravă de criminalitate organizată și o încălcare gravă a drepturilor fundamentale. Victimele sunt traficate în interiorul UE, în principal în scopul exploatării sexuale și prin muncă, dar și în scopul cerșetoriei și criminalității forțate și al altor forme. În decembrie 2022, Comisia a propus modificarea Directivei privind combaterea traficului de persoane[38] cu norme actualizate pentru a remedia deficiențele cadrului juridic actual. În special, odată adoptată, directiva revizuită ar adăuga căsătoriile forțate și adopțiile ilegale în domeniul de aplicare al directivei și ar introduce o trimitere explicită la dimensiunea online a traficului de persoane. Aceasta ar include, de asemenea, un regim obligatoriu de sancțiuni pentru autorii infracțiunilor și ar oficializa instituirea unor mecanisme naționale de sesizare pentru a îmbunătăți identificarea timpurie și sesizarea transfrontalieră în vederea acordării de asistență și sprijin victimelor. Utilizarea cu bună știință a serviciilor furnizate de victimele traficului de persoane ar deveni infracțiune, iar colectarea anuală de date privind traficul de persoane, care urmează să fie publicată de Eurostat, ar deveni obligatorie. Consiliul și-a adoptat abordarea generală în iunie 2023, în timp ce Parlamentul European nu și-a adoptat încă poziția. Va fi necesară o acțiune rapidă pentru a se ajunge la un acord înainte de încheierea mandatului actualului Parlament.

Infracțiuni împotriva mediului

Infracțiunile împotriva mediului au devenit o amenințare globală, crescând cu o rată estimată cuprinsă între 5 și 7 % în fiecare an. Profiturile semnificative care pot fi generate, lacunele juridice dintre statele membre și riscul scăzut de detectare sunt toate elemente care atrag criminalitatea organizată. Potrivit Europol, există indicii potrivit cărora veniturile obținute din aceste activități sunt utilizate pentru a finanța terorismul. În decembrie 2021, Comisia a adoptat o propunere de înlocuire a Directivei din 2008 privind protecția mediului prin intermediul dreptului penal. Propunerea se concentrează pe rafinarea și actualizarea definițiilor categoriilor de infracțiuni împotriva mediului și pe definirea unor tipuri și niveluri de sancțiuni eficace, disuasive și proporționale pentru persoanele fizice și juridice. Printre noile infracțiuni se numără infracțiuni legate de defrișările ilegale, de încălcarea legislației UE privind substanțele chimice, de extragerea ilegală a apelor de suprafață sau subterane și de reciclarea ilegală a navelor. Propunerea urmărește să consolideze în mod semnificativ lanțul de asigurare a respectării legii și cooperarea transfrontalieră dintre autoritățile statelor membre și agențiile și organismele UE.

[37] COM(2022) 480.
[38] COM(2022) 732.

Parlamentul European și Consiliul și-au adoptat pozițiile cu privire la propunere și se află într-un proces de negociere pe care ar trebui să îl poată încheia până la sfârșitul anului. Un plan de acțiune revizuit[39] în materie de combatere a traficului cu specii sălbatice de faună și floră trebuie pus în aplicare pentru a consolida în continuare prevenirea și asigurarea respectării legii.

Recuperarea și confiscarea activelor

Privarea infractorilor de veniturile lor ilicite este esențială pentru anihilarea criminalității organizate. Acesta este motivul pentru care, pe lângă propunerea de acordare a accesului autorităților de aplicare a legii la informațiile privind conturile bancare în întreaga UE[40] (pentru care s-a ajuns la un acord politic în iunie 2023), Comisia a prezentat, în mai 2022, o propunere privind recuperarea și confiscarea activelor[41], pentru a consolida capacitățile de urmărire, identificare, înghețare, confiscare și gestionare a activelor. Dispozițiile-cheie ale propunerii se referă la cerințele privind investigațiile financiare și la competențele și instrumentele suplimentare ale birourilor de recuperare a activelor, precum și la măsuri mai eficace de înghețare și confiscare pentru un set extins de infracțiuni. Una dintre noile infracțiuni pentru care ar urma să se aplice aceste măsuri este încălcarea măsurilor restrictive ale Uniunii. În decembrie 2022, Comisia a adoptat o propunere separată de armonizare a definițiilor penale și a sancțiunilor pentru încălcarea măsurilor restrictive ale Uniunii. Punerea în aplicare și asigurarea eficace a respectării măsurilor restrictive ale Uniunii rămân o prioritate esențială pentru Comisie, consolidată de activitatea Grupului operativ „Înghețare și punere sub sechestru” instituit de Comisie ca răspuns la războiul de agresiune al Rusiei împotriva Ucrainei. Pentru ambele propuneri, Parlamentul European și Consiliul și-au adoptat pozițiile cu scopul de a ajunge la un acord până la sfârșitul acestui an.

Pachetul privind combaterea spălării banilor

Spălarea banilor este legată de aproape toate activitățile infracționale care generează venituri provenite din infracțiuni în UE[42] și, prin urmare, reprezintă o pârghie esențială pentru combaterea criminalității în UE. În iulie 2021, Comisia a prezentat propuneri ambițioase de consolidare a măsurilor UE de prevenire a spălării banilor și a finanțării terorismului[43], cu patru propuneri legislative menite să consolideze prevenirea și detectarea tentativelor infractorilor de a spăla venituri ilicite sau de a finanța activități teroriste prin intermediul sistemului financiar. Una dintre cele patru inițiative ale pachetului, care vizează asigurarea trasabilității transferurilor de criptoactive, a fost adoptată de colegiuitori în mai 2023[44]. Acest regulament va intra în vigoare la 30 decembrie 2024, dată până la care toți furnizorii de servicii de criptoactive vor trebui să colecteze și să dețină informații cu privire la inițiatorul și beneficiarul transferurilor de criptoactive. Celelalte trei propuneri vizează (i) instituirea unei noi autorități a UE de combatere a spălării banilor, care să asigure o supraveghere coerentă și de înaltă calitate pe piața internă, inclusiv a entităților transfrontaliere cu cel mai ridicat grad de risc, sprijinind și coordonând activitatea unităților de informații financiare, (ii) stabilirea unor norme armonizate pentru sectorul privat, inclusiv introducerea unei limite de 10 000 EUR la nivelul UE pentru plățile mari în numerar în schimbul serviciilor și bunurilor și (iii) consolidarea competențelor și a instrumentelor de cooperare pentru autoritățile competente.

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Europol, „Enterprising criminals – Europe’s fight against the global networks of financial and economic crime” (Infractori corporativi. Lupta Europei împotriva rețelelor globale de infracțiuni financiare și economice), 2020.
[43] COM(2021) 420.
[44] Regulamentul (UE) 2023/1113 din 31 mai 2023 privind informațiile care însoțesc transferurile de fonduri și de anumite criptoactive și de modificare a Directivei (UE) 2015/849.

Se preconizează că acest pachet va consolida în mod semnificativ capacitatea UE de a combate spălarea banilor și de a proteja cetățenii UE împotriva terorismului și a criminalității organizate. Cele trei propuneri restante sunt în prezent în curs de negociere de către colegiuitori, cu scopul de a ajunge la un acord cu privire la acest dosar înainte de încheierea mandatului actualului Parlament.

Comisia invită Parlamentul European și Consiliul să finalizeze negocierile interinstituționale în regim de urgență, în orice caz înainte de încheierea mandatului actualului Parlament European, cu privire la următoarele dosare aflate în curs:

- propunere de directivă privind recuperarea și confiscarea activelor;
- propunere de directivă de armonizare a definițiilor penale și a sancțiunilor pentru încălcarea măsurilor restrictive ale Uniunii;
- propunere de directivă privind combaterea traficului de persoane;
- propunere de directivă privind îmbunătățirea protecției mediului prin intermediul dreptului penal;
- propunere de pachet privind combaterea spălării banilor;
- propunere de actualizare a legislației existente privind importul, exportul și tranzitul armelor de foc pentru uz civil.

Comisia invită statele membre, agențiile și organismele UE:

- să colaboreze în vederea punerii în aplicare a celor 17 acțiuni din Foaia de parcurs a UE pentru combaterea traficului de droguri și a criminalității organizate în 2023 și 2024.

V. Un ecosistem european solid în materie de securitate

În ultimii ani, amenințările la adresa securității au un caracter transfrontalier tot mai pronunțat, necesitând sinergii suplimentare și o cooperare mai strânsă la toate nivelurile. De la adoptarea Strategiei privind uniunea securității, s-au adoptat inițiative importante pentru a maximiza cooperarea transfrontalieră, raționalizând și actualizând instrumentele și procedurile disponibile atât la frontierele externe, cât și în spațiul Schengen, precum și consolidând schimbul de informații între autoritățile de aplicare a legii și autoritățile judiciare pentru o mai bună combatere a criminalității organizate. În acest context, punerea în aplicare eficace a cadrului de interoperabilitate pentru schimbul de date reprezintă un pilon important pentru consolidarea securității și un răspuns european eficace la amenințările transfrontaliere, garantând în același timp libera circulație internă.

Îmbunătățirea schimbului de informații în spațiul Schengen: informații prealabile referitoare la pasageri (API), registrele cu numele pasagerilor (PNR) și Prüm II

Cele două propuneri API adoptate de Comisie în decembrie 2022[45] ar consolida securitatea internă a Uniunii, oferind autorităților de aplicare a legii din statele membre instrumente suplimentare de combatere a criminalității grave și a terorismului. În special, informațiile prealabile referitoare la pasageri privind zborurile intra-UE, utilizate împreună cu PNR-urile călătorilor care utilizează transportul aerian, ar permite autorităților de aplicare a legii din statele

[45] COM(2022) 729, COM(2022) 73.

membre să sporească în mod semnificativ eficiența investigațiilor lor prin intervenții mai bine direcționate. Este important ca normele propuse să fie adoptate cât mai curând posibil: acest lucru nu numai că ar sprijini lupta împotriva criminalității organizate și a terorismului, dar ar reduce în mod semnificativ necesitatea de a efectua verificări sistematice ale tuturor călătorilor în cazul unei reintroduceri temporare a controalelor la frontierele interne, facilitând călătoriile pe cale aeriană și libera circulație. La 6 septembrie 2023, Comisia Europeană a recomandat Consiliului să autorizeze negocierile cu Elveția, Islanda și Norvegia pentru acorduri privind transferul de date PNR. Adoptarea acestor trei recomandări ar sprijini o politică externă a UE privind PNR coerentă și eficace.

Schimburile Prüm sunt utilizate zilnic de poliție pentru a combate criminalitatea organizată, drogurile, terorismul, exploatarea sexuală și traficul de persoane. Propunerea de regulament privind schimbul automatizat de date în scopul cooperării polițienești („Prüm II")[46] revizuiește cadrul Prüm existent în vederea eliminării lacunelor în materie de informații și a consolidării prevenirii, depistării și cercetării infracțiunilor în UE. Normele revizuite privind schimbul automatizat de date în scopul cooperării polițienești completează propunerile privind cooperarea polițienească din prezentul mandat, alături de recomandarea Consiliului deja adoptată de consolidare a cooperării operative transfrontaliere și de Directiva privind schimbul de informații între autoritățile de aplicare a legii. Adoptarea și punerea în aplicare rapidă a acestor instrumente conexe ar îmbunătăți, facilita și accelera schimbul de date între autoritățile de aplicare a legii și ar contribui la identificarea infractorilor.

Un sistem de gestionare a frontierelor pe deplin interoperabil pentru un spațiu Schengen sigur, puternic, digital și unit

O bună funcționare a spațiului Schengen fără frontiere interne se bazează pe încrederea reciprocă între statele membre. Aceasta se bazează, la rândul său, pe controale eficiente, fie la frontierele externe ale Uniunii, fie ca măsuri alternative pe teritoriul statelor membre. Modificarea propusă de Comisie la Codul frontierelor Schengen[47] stabilește modul în care statele membre pot utiliza mai bine alternativele la controalele la frontierele interne, care pot oferi un nivel ridicat de securitate. Este important ca modificarea Codului frontierelor Schengen să fie adoptată și pusă în aplicare integral pentru a asigura un nivel ridicat și proporțional de securitate în spațiul Schengen. Noua arhitectură a sistemelor informatice ale UE continuă, de asemenea, să fie în curs de elaborare, pentru a sprijini mai bine activitatea autorităților naționale de asigurare a securității, precum și de gestionare a frontierelor. Aceasta cuprinde Sistemul de informații Schengen reînnoit, Sistemul european de informații și de autorizare privind călătoriile, Sistemul de intrare/ieșire, actualizarea Sistemului de informații privind vizele și cadrul de interoperabilitate pentru conectarea sistemelor în deplină securitate. Odată finalizată pe deplin, această nouă arhitectură ar oferi autorităților naționale informații mai cuprinzătoare și mai fiabile legate de securitate. Toate componentele cadrului de interoperabilitate sunt esențiale, ceea ce înseamnă că o întârziere într-un aspect sau într-un stat membru duce la o întârziere a punerii în aplicare pentru toți. Întârzierile în dezvoltarea tehnică a sistemului de intrare/ieșire ar trebui să fie reduse la minimum, astfel încât sistemul de intrare/ieșire să poată începe să funcționeze cât mai curând posibil și să poată fi puse în practică toate elementele-cheie ale cadrului de interoperabilitate.

[46] COM(2021) 784.
[47] COM(2021) 891.

Propunerea privind procedura de screening[48] ar consolida securitatea în spațiul Schengen prin crearea de norme uniforme privind identificarea resortisanților țărilor terțe care nu îndeplinesc condițiile de intrare menționate în Codul frontierelor Schengen și prezentarea acestor persoane la controalele medicale și de securitate de la frontierele externe. Sistemul Eurodac propus ar sprijini aceste obiective, indicând cazurile în care, în urma procedurii de screening, se constată că o persoană ar putea reprezenta o amenințare la adresa securității interne. Acest lucru ar facilita, la rândul său, punerea în aplicare a propunerii de regulament privind gestionarea situațiilor legate de azil și migrație. Comisia încurajează colegiuitorii să încheie rapid negocierile cu privire la aceste dosare înainte de încheierea actualei perioade legislative.

Combaterea corupției

Corupția este extrem de dăunătoare pentru democrațiile noastre, pentru economie și pentru securitatea noastră, deoarece acționează ca un factor favorizant al criminalității organizate și al ingerințelor străine ostile. Prevenirea și combaterea cu succes a corupției sunt esențiale atât pentru a proteja valorile UE și eficacitatea politicilor UE, cât și pentru a sprijini statul de drept și încrederea în guvernanți și în instituțiile publice. Astfel cum a anunțat președinta von der Leyen în discursul privind starea Uniunii din 2022, Comisia a adoptat, la 3 mai 2023, un pachet de măsuri anticorupție[49]**.** Propunerea de directivă a Comisiei privind combaterea corupției include norme consolidate de incriminare a infracțiunilor de corupție și de armonizare a sancțiunilor în întreaga UE. Aceasta permite, de asemenea, efectuarea de investigații și urmăriri penale eficace și pune un accent puternic pe prevenire și pe crearea unei culturi a integrității în care corupția nu este tolerată. Discuțiile cu privire la această propunere au început în cadrul Parlamentului European și al Consiliului. În plus, statele membre sunt invitate să pună în aplicare recomandările care decurg din pilonul anticorupție al Raportului din 2023 privind statul de drept, adoptat la 5 iulie 2023. O propunere din partea Înaltului Reprezentant, sprijinită de Comisie, prevede, de asemenea, instituirea unui regim specific de sancțiuni în cadrul politicii externe și de securitate comună (PESC) care să vizeze actele grave de corupție din întreaga lume.

Consolidarea drepturilor victimelor

La 12 iulie 2023, Comisia a propus modificări ale Directivei privind drepturile victimelor, pentru a consolida accesul victimelor la informații, sprijin și protecție, participarea la procedurile penale și accesul la despăgubiri. Unul dintre obiectivele generale ale revizuirii este de a contribui la un nivel ridicat de securitate prin crearea unui mediu mai sigur pentru victime pentru a încuraja raportarea infracțiunilor, reducând teama de represalii.

Comisia invită Parlamentul European și Consiliul să finalizeze negocierile interinstituționale în regim de urgență, în orice caz înainte de încheierea mandatului actualului Parlament European, cu privire la următoarele dosare aflate în curs:

- propunere privind Regulamentul Prüm II;
- propuneri privind informațiile prealabile referitoare la pasageri (API);
- propuneri privind combaterea corupției și, în special, instituirea unui regim specific de sancțiuni în cadrul politicii externe și de securitate comune (PESC);
- propunere de modificare a Regulamentului privind Codul frontierelor Schengen;
- propunere de directivă privind drepturile victimelor;
- propunere privind procedura de screening.

[48] COM(2020) 612.
[49] COM(2023) 234.

Comisia invită statele membre:

- să asigure intrarea în vigoare a sistemului de intrare/ieșire cât mai curând posibil, pentru a finaliza punerea în aplicare a arhitecturii UE privind schimbul de informații.

VI. Punerea în aplicare

Asigurarea securității Europei în ansamblu este o responsabilitate comună, în cadrul căreia fiecare parte trebuie să își îndeplinească rolul, începând cu adoptarea de către Comisie și colegiuitori a unor norme noi, solide, cuprinzătoare și practice, până la transpunerea, punerea în practică și aplicarea în timp util a acestor norme de către statele membre, precum și la activitatea operațională desfășurată pe teren de o varietate de autorități, organizații și părți interesate. Agențiile UE din domeniile justiției, afacerilor interne și securității cibernetice joacă, de asemenea, un rol esențial, care a crescut prin extinderea recentă a responsabilităților lor.

Îmbunătățirea verificării beneficiarilor fondurilor UE

Atunci când execută bugetul UE, Comisia are responsabilitatea de a se asigura că beneficiarii fondurilor UE respectă valorile UE. Mecanismele și sistemele de control care stabilesc cine poate beneficia de finanțare din partea UE sunt deja solide, iar negocierile în curs privind reformarea Regulamentului financiar urmăresc, de asemenea, să ofere Comisiei mijloace juridice mai puternice pentru a acționa la nevoie. În plus, Comisia elaborează în prezent modalități de îmbunătățire în continuare a verificării beneficiarilor actuali și potențiali ai fondurilor UE, prin ameliorarea orientărilor privind obligațiile referitoare la respectarea valorilor UE și a consecințelor care ar trebui să decurgă din încălcarea valorilor UE. Acest lucru va clarifica responsabilitățile atât ale beneficiarilor, cât și ale celor care efectuează controale la nivelul UE și poate servi drept sursă de inspirație pentru nivelul național. În cazul încălcării condițiilor de finanțare, Comisia nu ezită și nu va ezita să întrerupă cooperarea cu beneficiarii proiectului în cauză și să recupereze fondurile, dacă este necesar. Este important ca statele membre să facă schimb proactiv de informații cu Comisia atunci când au cunoștință de posibile riscuri în ceea ce privește organizațiile care solicită finanțare din partea UE.

Încălcări

În domeniul securității, Comisia a desfășurat numeroase proceduri de constatare a neîndeplinirii obligațiilor. De exemplu, în 2023, un număr mare de acțiuni în constatarea neîndeplinirii obligațiilor au fost inițiate din cauza neîndeplinirii obligațiilor care decurg din Regulamentul din 2021 privind prevenirea diseminării conținutului online cu caracter terorist (16 state membre)[50], iar în cursul anilor 2022 și 2023, 20 de state membre au primit scrisori suplimentare de punere în întârziere din cauza punerii în aplicare incorecte a Directivei din 2011 privind combaterea abuzului sexual asupra copiilor[51]. Un număr semnificativ de acțiuni în constatarea neîndeplinirii obligațiilor sunt încă deschise pentru neconformitatea legislației naționale cu Directiva din 2017 privind combaterea terorismului[52] și pentru netranspunerea normelor de facilitare a utilizării informațiilor financiare și de alt tip în scopul prevenirii, depistării,

[50] Regulamentul (UE) 2021/784 privind prevenirea diseminării conținutului online cu caracter terorist.

[51] Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor.

[52] Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului.

investigării sau urmăririi penale a anumitor infracțiuni[53]. Alte domenii în care sunt în curs proceduri de constatare a neîndeplinirii obligațiilor includ legislația privind armele de foc; normele privind substanțele psihoactive utilizate în droguri, combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar, combaterea spălării banilor, comunicarea reciprocă a cazierelor judiciare de către statele membre ale UE și Directiva privind drepturile victimelor. Sprijin (tehnic și financiar) a fost pus la dispoziția statelor membre care pun în aplicare inițiativele și acțiunile convenite, iar Comisia rămâne disponibilă pentru a colabora cu statele membre în vederea optimizării punerii în aplicare.

Monitorizarea prin intermediul evaluărilor Schengen și al noului său sistem de guvernanță

Mecanismul de evaluare și monitorizare Schengen a continuat să contribuie la punerea în aplicare eficace a normelor Schengen care vizează consolidarea securității în spațiul fără controale interne. În 2023, s-au efectuat primele evaluări în cadrul mecanismului consolidat de evaluare și monitorizare Schengen, ceea ce a permis identificarea și remedierea în timp util a vulnerabilităților strategice, care au un impact transfrontalier asupra securității și siguranței în cadrul UE. În plus, în 2023, Comisia a lansat o evaluare tematică Schengen pentru a analiza practicile statelor membre care se confruntă cu provocări similare în combaterea traficului de droguri către UE, punând accentul în special pe traficul de droguri în volum mare. Aceste evaluări au introdus un accent mai puternic și mai cuprinzător asupra elementelor de securitate ale Schengen. Pe baza rezultatelor evaluărilor Schengen periodice, tematice și inopinate, Consiliul a stabilit, în iunie 2023, prioritățile ciclului Schengen 2023-2024. Acesta stabilește domeniile prioritare care necesită un impuls suplimentar pentru un spațiu Schengen mai sigur și mai puternic. O punere în aplicare eficace și rapidă a acestor priorități, împreună cu o coordonare sporită a politicilor Consiliului Schengen, va consolida și mai mult lupta împotriva criminalității organizate și va maximiza cooperarea operațională transfrontalieră.

Rolul agențiilor și organismelor UE

Parteneriatul este esențial pentru punerea în aplicare a inițiativelor privind uniunea securității, deoarece este nevoie de activitatea diferitelor autorități și organisme naționale și europene pentru a obține rezultate concrete. De exemplu, EMPACT (Platforma multidisciplinară europeană împotriva amenințărilor infracționale) permite o cooperare multidisciplinară structurată a statelor membre, sprijinită de toate instituțiile, organele și agențiile UE (cum ar fi Europol, Frontex, Eurojust, CEPOL, OLAF, EU-LISA). Operațiunile desfășurate de EMPACT, inclusiv prin intermediul grupurilor de lucru operaționale dedicate, coordonează eforturile statelor membre și ale partenerilor operaționali de combatere a rețelelor infracționale și a criminalității grave. Numai în 2022, EMPACT a avut ca rezultat un total de 9 922 de arestări, peste 180 de milioane EUR reprezentând active și bani confiscați, 9 263 de anchete inițiate, 4 019 victime identificate, peste 62 de tone de droguri confiscate, 51 de ținte de mare importanță identificate și 12 arestate, operațiuni în contextul războiului de agresiune împotriva Ucrainei, în special pentru a combate traficul de persoane și amenințările legate de armele de foc.

Frontex, Agenția Europeană pentru Siguranță Maritimă (EMSA) și Agenția Europeană pentru Controlul Pescuitului (EFCA) continuă să își consolideze cooperarea în ceea ce privește funcțiile de pază de coastă pentru a sprijini autoritățile naționale în creșterea siguranței și securității pe mare. Aceste agenții vor avea o contribuție majoră la punerea în aplicare a strategiei UE în materie de securitate maritimă.

[53] Directiva (UE) 2019/1153 a Parlamentului European și a Consiliului din 20 iunie 2019 de stabilire a normelor de facilitare a utilizării informațiilor financiare și de alt tip în scopul prevenirii, depistării, investigării sau urmăririi penale a anumitor infracțiuni și de abrogare a Deciziei 2000/642/JAI a Consiliului.

Mai multe inițiative privind uniunea securității au adus noi responsabilități și sarcini pentru agențiile relevante, uneori cu implicații pentru resursele umane.

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

În ceea ce privește pregătirea și răspunsul la incidente pentru consolidarea securității cibernetice, Comisia a instituit o acțiune pe termen scurt pentru a sprijini statele membre, transferând fonduri de la programul „Europa digitală" (DEP) către **Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)** cu scopul de a consolida gradul de pregătire și capacitățile de răspuns la incidentele cibernetice majore. Propunerea de regulament privind solidaritatea cibernetică, adoptată în aprilie 2023, se bazează pe această acțiune și, odată adoptată de colegiuitori, poate încredința ENISA sarcini suplimentare, cum ar fi operarea și administrarea viitoarei rezerve pentru securitate cibernetică a Uniunii sau întocmirea unui raport de examinare a incidentelor în urma unor incidente de securitate cibernetică de mare amploare. Propunerea de act european privind reziliența cibernetică ar urma să încredințeze ENISA sarcina de a primi notificări de la producători cu privire la vulnerabilitățile produselor cu elemente digitale și la incidentele care au un impact asupra securității acestor produse, pe care ENISA ar trebui să le transmită echipelor CSIRT relevante sau punctelor unice de contact relevante ale statelor membre. De asemenea, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită Grupului de cooperare NIS.

Centrul european de competențe în materie de securitate cibernetică

Centrul european de competențe în materie de securitate cibernetică (ECCC), împreună cu Rețeaua de centre naționale de coordonare (CNC-uri), este noul organism al Uniunii care sprijină inovarea și politica industrială în domeniul securității cibernetice. Acest ecosistem va consolida capacitățile comunității tehnologice în materie de securitate cibernetică, va menține excelența în cercetare și va consolida competitivitatea industriei Uniunii în acest domeniu. ECCC și CNC-urile vor lua decizii de investiții strategice și vor pune în comun resurse din partea Uniunii, a statelor sale membre și, indirect, a industriei, pentru a îmbunătăți și a consolida capacitățile tehnologice și industriale în materie de securitate cibernetică. Prin urmare, ECCC joacă un rol esențial în realizarea obiectivelor ambițioase în materie de securitate cibernetică ale programelor Europa digitală și Orizont Europa.

ECCC și-a recrutat mai mult de jumătate din personal și își va recruta în curând directorul executiv. Lucrările deja în curs includ partea privind securitatea cibernetică din programul DIGITAL și o nouă agendă strategică[54] pentru dezvoltarea și implementarea tehnologiei, care stabilește acțiuni prioritare de sprijinire a IMM-urilor în dezvoltarea și utilizarea tehnologiilor, a serviciilor și a proceselor strategice de securitate cibernetică; de sprijinire și dezvoltare a forței de muncă profesioniste; și de consolidare a expertizei în materie de cercetare, dezvoltare și inovare în cadrul ecosistemului european mai larg de securitate cibernetică.

Europol

Cu un mandat complet nou, **Europol** va fi mai bine pregătit pentru a sprijini statele membre în lupta împotriva criminalității organizate. Lupta împotriva traficului de droguri este o prioritate-cheie, având în vedere importanța sa tot mai mare și impactul tot mai nefavorabil asupra securității cetățenilor UE. În urma autorizării din partea Consiliului Uniunii Europene din 15 mai 2023, Comisia a depus eforturi active în vederea încheierii unor acorduri

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_en.

internaționale cu Bolivia, Brazilia, Ecuador, Mexic și Peru privind schimbul de date cu caracter personal cu Europol în scopul prevenirii și combaterii criminalității grave și a terorismului.

Eurojust

Având peste 20 de ani de experiență în furnizarea de sprijin judiciar autorităților naționale pentru combaterea unei game largi de infracțiuni transfrontaliere grave și complexe, **Eurojust** și-a consolidat poziția în spațiul de libertate, securitate și justiție al UE. Pentru a consolida cooperarea la toate nivelurile, Comisia negociază acorduri internaționale pentru a facilita cooperarea dintre Eurojust și 13 țări terțe în vederea schimbului de date cu caracter personal în vederea combaterii criminalității organizate și a terorismului[55]. Negocierile au fost deja finalizate cu Armenia și Liban, sunt în curs cu Algeria și Columbia și au început cu Bosnia și Herțegovina. Comisia încurajează Parlamentul European și Consiliul să finalizeze încheierea de acorduri cu aceste țări înainte de sfârșitul legislaturii, pentru a consolida cooperarea judiciară transnațională și a extinde lupta împotriva criminalității transfrontaliere.

EPPO

De la începutul activităților sale operaționale, în iunie 2021, **Parchetul European (EPPO)** s-a dovedit a fi un instrument puternic în setul de instrumente al Uniunii pentru investigarea și urmărirea penală a infracțiunilor care afectează bugetul Uniunii, inclusiv a infracțiunilor legate de participarea la o organizație criminală, atunci când accentul se pune pe infracțiunile împotriva bugetului Uniunii. Comisia încurajează statele membre care nu participă încă la cooperarea consolidată a EPPO să facă acest lucru cât mai curând posibil, pentru a atinge potențialul maxim al EPPO în ceea ce privește protejarea banilor contribuabililor UE.

EUDA

Cu un nou mandat adoptat de colegiuitori în iunie 2023, actualul Observator European pentru Droguri și Toxicomanie (OEDT) se va transforma într-o agenție cu drepturi depline – **Agenția pentru Droguri a Uniunii Europene (EUDA*)*** – cu un rol consolidat. Agenția va putea să evalueze noile provocări în materie de sănătate și securitate generate de drogurile ilicite într-un mod mai cuprinzător și să contribuie mai eficient la activitățile desfășurate la nivelul statelor membre și la nivel internațional. Colectarea, analiza și diseminarea datelor vor continua să fie principala sarcină a agenției, dar mandatul consolidat îi va permite, de asemenea, agenției să dezvolte capacități generale de evaluare a amenințărilor la adresa sănătății și a securității pentru a identifica amenințările emergente, inclusiv policonsumul de droguri, să își consolideze cooperarea prin intermediul punctelor focale naționale și să instituie o rețea de laboratoare care să furnizeze agenției informații criminalistice și toxicologice. Acest lucru va ajuta agenția să emită alerte atunci când apar pe piață substanțe deosebit de periculoase și să crească gradul de conștientizare.

[55] Algeria, Argentina, Armenia, Bosnia și Herțegovina, Brazilia, Columbia, Egipt, Israel, Iordania, Liban, Maroc, Tunisia și Turcia.

Comisia invită Parlamentul European și Consiliul să finalizeze negocierile interinstituționale în regim de urgență, în orice caz înainte de încheierea mandatului actualului Parlament European, cu privire la următoarele dosare aflate în curs:

- propunere de reformare a Regulamentului financiar.

Comisia invită statele membre:

- să facă schimb proactiv de informații cu Comisia atunci când au cunoștință de posibile riscuri în ceea ce privește organizațiile care solicită finanțare din partea UE;
- să pună rapid în aplicare prioritățile ciclului Schengen 2023-2024 pentru un spațiu Schengen mai sigur și mai puternic;
- să abordeze procedurile de constatare a neîndeplinirii obligațiilor deschise împotriva lor pentru a asigura transpunerea corectă a legislației în cauză.

VII. Concluzie

Ultimii trei ani au fost marcați de un efort constant și susținut de a da viață ambiției de a crea o uniune a securității pentru UE. S-au obținut progrese uriașe în întregul spectru al domeniului politicii de securitate. În prezent, realitatea amenințărilor în continuă evoluție necesită eforturi continue, cu o motivație reînnoită. Lucrările privind cadrul legislativ trebuie să fie finalizate în timp util, înainte de încheierea legislaturii parlamentare, în primăvara anului 2024. Statele membre au responsabilități constante de transpunere, punere în aplicare și aplicare a noilor legi. Punerea în aplicare necesită eforturi concertate, inclusiv cu sprijinul agențiilor UE – și, foarte adesea, o cooperare tot mai strânsă cu partenerii noștri internaționali.

Numai prin eforturile colective și susținute ale tuturor părților interesate vom atinge în UE nivelurile de siguranță și securitate pe care le așteaptă cetățenii – iar în contextul de astăzi, fiecare parte ar trebui să îndeplinească un rol prioritar în consolidarea securității UE.