COMISIA
EUROPEANĂ

Bruxelles, 24.7.2020
COM(2020) 605 final

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

referitoare la Strategia UE privind uniunea securității

I. Introducere

În Orientările politice, Comisia a precizat fără echivoc că nu trebuie neglijat niciun aspect atunci când vine vorba de protejarea cetățenilor noștri. Securitatea nu reprezintă doar baza siguranței personale, ci contribuie, de asemenea, la protejarea drepturilor fundamentale și constituie temelia încrederii în economia noastră, în societatea noastră și democrația noastră, precum și a dinamismului acestora. În prezent, situația în materie de securitate este în continuă schimbare în Europa, fiind afectată de amenințările în evoluție, precum și de alți factori printre care schimbările climatice, tendințele demografice și instabilitatea politică din afara frontierelor noastre. Globalizarea, libera circulație și transformarea digitală continuă să aducă prosperitate, să ne ușureze viața și să stimuleze inovarea și creșterea economică. Aceste avantaje implică însă și riscuri și costuri inerente. Avantajele pot fi manipulate de terorism, de criminalitatea organizată, de comerțul cu droguri și de traficul de persoane, toate acestea fiind amenințări directe la adresa cetățenilor și a modului nostru de viață european. Atacurile cibernetice și criminalitatea informatică continuă să ia amploare. Amenințările la adresa securității devin, de asemenea, tot mai complexe: ele sunt alimentate de capacitatea de a interveni la nivel transfrontalier și de interconectivitate, exploatează estomparea limitelor dintre lumea fizică și cea digitală și se folosesc de grupurile vulnerabile, divergențele sociale și economice. Atacurile pot surveni în orice moment și pot lăsa foarte puține urme sau nicio urmă; atât actorii statali, cât și cei nestatali pot recurge la o serie de amenințări hibride[1], iar evenimentele din afara UE pot avea un impact critic asupra securității din interiorul UE.

Criza provocată de pandemia de COVID-19 a dus, de asemenea, la reevaluarea noțiunii de amenințări la adresa siguranței și securității și a politicilor aferente. Criza sanitară a evidențiat necesitatea de a garanta securitatea atât în mediul fizic, cât și în cel digital. A pus în evidență importanța unei autonomii strategice deschise pentru lanțurile noastre de aprovizionare în ceea ce privește produsele, serviciile, infrastructurile și tehnologiile critice. A consolidat necesitatea de a implica fiecare sector și fiecare persoană în efortul comun de asigurare a faptului că UE este mai pregătită și mai reziliență a priori și că dispune de instrumente mai bune care să îi permită să răspundă atunci când este necesar.

Cetățenii nu pot fi protejați numai prin acțiunea individuală a statelor membre. Este mai important decât oricând să ne valorificăm atuurile pentru a lucra împreună, iar UE are acum mai mult decât oricând potențialul de a face diferența. UE poate să ofere un exemplu, consolidând sistemul său general de gestionare a crizelor și acționând în interiorul și în afara frontierelor sale, pentru a contribui la stabilitatea mondială. Deși responsabilitatea principală pentru securitate revine statelor membre, în ultimii ani a fost tot mai clar că securitatea unui stat membru înseamnă securitatea tuturor. UE poate să aducă un răspuns multidisciplinar și integrat, venind în ajutorul actorilor din domeniul securității din statele membre cu instrumentele și informațiile de care au nevoie[2].

---

[1] Deși există mai multe definiții pentru amenințările hibride, această noțiune dorește să surprindă asocierea activităților coercitive și subversive cu metodele convenționale și neconvenționale (de exemplu, diplomatice, militare, economice, tehnologice) care pot fi utilizate în mod coordonat de actori statali sau nestatali pentru a atinge obiective specifice (fără să se ajungă la stadiul de stare de război declarată în mod oficial). A se vedea JOIN(2016) 18 (final).

[2] De exemplu, prin intermediul serviciilor furnizate de programul spațial al UE, cum ar fi Copernicus, care furnizează date și aplicații de observare a Pământului pentru supravegherea frontierelor, securitatea maritimă, asigurarea aplicării legii, combaterea pirateriei, prevenirea contrabandei cu droguri și gestionarea situațiilor de urgență.

UE se poate asigura, de asemenea, că politica de securitate este în continuare ancorată în valorile europene comune – respectarea și protejarea statului de drept, a egalității[3] și a drepturilor fundamentale și garantarea transparenței, responsabilității și a controlului democratic – astfel încât politicile să se bucure de încrederea adecvată. UE poate crea o uniune a securității efectivă și autentică, în care drepturile și libertățile persoanelor să fie protejate în mod corespunzător. Securitatea și respectarea drepturilor fundamentale nu sunt obiective diametral opuse, ele sunt obiective coerente și complementare. Valorile și drepturile fundamentale trebuie să fie temelia politicilor de securitate care trebuie să respecte principiile necesității, proporționalității și legalității și care trebuie să prevadă garanții adecvate în materie de responsabilitate și căi de atac, permițând, în același timp, un răspuns eficace în vederea protejării persoanelor, în special a celor mai vulnerabile.

S-au instituit deja instrumente juridice, practice și de sprijin semnificative, însă acestea trebuie să fie consolidate și puse în aplicare mai bine. S-au înregistrat progrese importante în ceea ce privește îmbunătățirea schimbului de informații și a cooperării în materie de informații cu statele membre și restrângerea perimetrului de acțiune al teroriștilor și infractorilor. Cu toate acestea rămâne un anumit grad de fragmentare.

Eforturile trebuie, de asemenea, extinse în afara granițelor UE. Protejarea Uniunii și a cetățenilor săi nu se mai limitează doar la asigurarea securității în interiorul frontierelor UE, ci presupune și abordarea dimensiunii externe a securității. Abordarea UE în ceea ce privește securitatea externă în cadrul politicii externe și de securitate comune (PESC) și al politicii de securitate și apărare comune (PSAC) va rămâne o componentă esențială a eforturilor UE de consolidare a securității în cadrul UE. Cooperarea cu țările terțe și cooperarea la nivel mondial pentru a aborda provocările comune este un element central al unui răspuns eficace și cuprinzător, stabilitatea și securitatea în vecinătatea UE fiind esențiale pentru securitatea UE.

Plecând de la activitatea anterioară a Parlamentului European[4], a Consiliului[5] și a Comisiei[6], această nouă strategie arată că pentru ca uniunea securității să fie autentică și efectivă este necesar un nucleu solid de instrumente și politici care să asigure securitatea în practică, ținând seama de faptul că securitatea are implicații pentru toate părțile societății și pentru toate politicile publice. UE trebuie să asigure un mediu sigur pentru toți, indiferent de originea rasială sau etnică, religie, convingeri, gen, vârstă sau orientare sexuală.

Prezenta strategie vizează perioada 2020-2025 și pune accentul pe consolidarea capacităților, astfel încât să se asigure un mediu de securitate adaptat exigențelor viitorului. Prezenta strategie stabilește o abordare în materie de securitate la nivelul întregii societăți, care să poată să răspundă în mod eficient și coordonat la amenințările în rapidă evoluție. Strategia definește prioritățile strategice și acțiunile corespunzătoare menite să abordeze riscurile digitale și fizice în mod integrat în întregul ecosistem al uniunii securității, punând accentul pe domeniile în care UE poate aduce o valoare suplimentară. Obiectivul strategiei

[3] O Uniune a egalității: Strategia privind egalitatea de gen 2020-2025, COM(2020) 152.

[4] De exemplu, activitatea comisiei TERR a Parlamentului European, care și-a prezentat raportul în noiembrie 2018.

[5] De la concluziile Consiliului din iunie 2015 privind „Strategia reînnoită de securitate internă” la rezultatele mai recente ale Consiliului din decembrie 2019.

[6] „Punerea în aplicare a Agendei europene privind securitatea pentru a combate terorismul și a deschide calea către o uniune a securității efectivă și autentică”, COM (2016) 230 final, 20.4.2016. A se vedea recenta evaluare a punerii în aplicare a legislației în domeniul securității interne: *Implementation of Home Affairs legislation in the field of internal security* – 2017-2020 [SWD(2020)135].

este obținerea de rezultate concrete în materie de securitate pentru a-i proteja pe toți cetățenii UE.

II. Amenințări la adresa securității în evoluție rapidă în Europa

Pentru a asigura siguranța, prosperitatea și bunăstarea cetățenilor, pericolele trebuie înlăturate. Riscul de apariție a amenințărilor la adresa securității depinde de gradul de vulnerabilitate al modului de viață și al mijloacelor de subzistență. Cu cât gradul de vulnerabilitate este mai mare, cu atât este mai mare riscul ca această vulnerabilitate să fie exploatată. Atât vulnerabilitățile, cât și amenințările sunt în continuă evoluție, iar UE trebuie să se adapteze.

Viața noastră de zi cu zi depinde de o gamă largă de servicii – ca de exemplu, energia, transporturile și finanțele, precum și asistența medicală. Aceste servicii se bazează atât pe infrastructura fizică, cât și pe cea digitală, ceea ce amplifică gradul de vulnerabilitate și potențialul de perturbare. În timpul pandemiei de COVID-19, noile tehnologii au permis funcționarea multor întreprinderi și servicii publice, fie prin asigurarea conexiunii pentru lucrul la distanță, fie prin menținerea logisticii lanțurilor de aprovizionare. Însă acest lucru a deschis calea către o creștere extraordinară a atacurilor rău intenționate, în încercarea de a profita în scopuri infracționale de pe urma perturbărilor provocate de pandemie și de trecerea la lucrul la distanță de acasă[7]. Penuria de bunuri a creat noi ocazii pentru criminalitatea organizată. Consecințele ar fi putut fi fatale, perturbând serviciile esențiale de sănătate într-un moment în care presiunea era imensă.

În urma creșterii necontenite a utilității pe care tehnologiile digitale o au în viața de zi cu zi, **securitatea cibernetică** a tehnologiilor a devenit, de asemenea, un aspect de importanță strategică[8]. Gospodăriile, băncile, serviciile financiare și întreprinderile (în special întreprinderile mici și mijlocii) sunt puternic afectate de atacurile cibernetice. Prejudiciul potențial este amplificat de interdependența sistemelor fizice și digitale: orice impact fizic va afecta sistemele digitale, în timp ce atacurile cibernetice asupra sistemelor informatice și a infrastructurilor digitale pot duce la sistarea serviciilor esențiale[9]. Dezvoltarea internetului obiectelor și creșterea utilizării inteligenței artificiale vor aduce noi beneficii, dar și o nouă serie de riscuri.

Lumea depinde de infrastructuri, tehnologii și sisteme online digitale, care ne permit să lansăm o afacere, să consumăm produse și să beneficiem de servicii. Pentru toate acestea este nevoie de comunicare și interacțiune. Dependența de mediul online a deschis calea către un val de acte de **criminalitate informatică**[10]. „Criminalitatea informatică ca serviciu” și

---

[7] Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (aprilie 2020).

[8] Recomandarea Comisiei intitulată „Securitatea cibernetică a rețelelor 5G”, C(2019) 2335; Comunicarea intitulată „Implementarea rețelelor 5G în condiții de siguranță în UE – Punerea în aplicare a setului de instrumente al UE”, COM(2020) 50.

[9] În martie 2020, Spitalul Universitar din Brno, Cehia a suferit un atac cibernetic în urma căruia spitalul a fost nevoit să redirecționeze pacienți și să amâne intervenții chirurgicale (Europol: *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). Inteligența artificială poate fi utilizată în mod abuziv pentru atacuri digitale, politice și fizice, precum și în scopul supravegherii. Colectarea datelor în cadrul internetului obiectelor poate fi utilizată pentru supravegherea persoanelor (ceasuri inteligente, asistenți virtuali etc.).

[10] Potrivit unor previziuni, costurile aferente încălcării securității datelor vor fi de 5 mii de miliarde USD anual până în 2024, în creștere de la 3 mii de miliarde USD în 2015 (Juniper Research, *The Future of Cybercrime & Security*).

economia subterană aferentă criminalității informatice facilitează accesul online la produse și servicii ale criminalității informatice. Infractorii se adaptează rapid pentru a utiliza noile tehnologii în scopuri proprii. De exemplu, medicamentele contrafăcute și falsificate au pătruns în lanțul legal de aprovizionare cu produse farmaceutice[11]. Creșterea exponențială în mediul online a materialelor care conțin abuzuri sexuale asupra copiilor[12] a pus în evidență consecințele sociale ale schimbării tiparelor de criminalitate. Conform unui sondaj recent, majoritatea persoanelor din UE (55 %) sunt îngrijorate că datele lor sunt accesate de infractori și autori de fraude[13].

Contextul mondial accentuează, de asemenea, aceste amenințări. Politicile industriale asertive ale țărilor terțe, corelate cu furtul continuu de proprietate intelectuală facilitat de mediul cibernetic au impact asupra paradigmei strategice de protejare și promovare a intereselor europene. Acest lucru este accentuat de creșterea aplicațiilor cu dublă utilizare, ceea ce face ca un sector solid al tehnologiei civile să constituie un atu important pentru capacitatea de apărare și securitate. Spionajul industrial are un impact semnificativ asupra economiei, a locurilor de muncă și a creșterii economice a UE: se estimează că furtul cibernetic de secrete comerciale cauzează UE costuri în valoare de 60 de miliarde EUR[14]. Acest lucru necesită o analiză detaliată a modului în care dependențele și expunerea mai mare la amenințările cibernetice afectează capacitatea UE de a proteja atât persoanele, cât și întreprinderile.

Criza provocată de pandemia de COVID-19 a pus, de asemenea, în evidență modul în care diviziunile sociale și incertitudinile creează o vulnerabilitate în materie de securitate. Acest lucru contribuie la creșterea potențialului de atacuri mai sofisticate și de **atacuri hibride** lansate de actori statali și nestatali, vulnerabilitățile fiind exploatate prin corelarea atacurilor cibernetice, a daunelor aduse infrastructurii critice[15], a campaniilor de dezinformare și a radicalizării discursurilor politice.[16]

În același timp, amenințările mai vechi sunt în continuă evoluție. În 2019, s-a înregistrat o tendință de scădere a **atacurilor teroriste** în UE. Cu toate acestea, se menține la un nivel ridicat amenințarea la adresa cetățenilor UE a unui atac jihadist comis de Da'esh și Al-Qaida și de grupările afiliate acestora sau inspirat de acestea[17]. În paralel, este în creștere și amenințarea extremismului de dreapta violent[18]. Atacurile inspirate de rasism trebuie să reprezinte un motiv serios de îngrijorare: atacurile teroriste antisemite mortale din Halle au reamintit că este necesar să se intensifice răspunsul în conformitate cu Declarația Consiliului

---

[11] Conform estimărilor unui studiu din 2016 (Legiscript), la nivel mondial, numai 4 % din farmaciile online funcționează în mod legal, consumatorii UE fiind ținta principală a celor 30 000-35 000 de farmacii online care își desfășoară activitatea în mod ilegal în mediul online.

[12] Strategia UE pentru o combatere mai eficace a abuzului sexual asupra copiilor, COM(2020) 607.

[13] Agenția pentru Drepturi Fundamentale a Uniunii Europene (2020), *Your rights matter: Security concerns and experiences*, *Fundamental Rights Survey*, Luxemburg, Oficiul pentru Publicații.

[14] *The scale and impact of industrial espionage and theft of trade secrets through cyber*, 2018.

[15] Infrastructurile critice sunt esențiale pentru funcțiile vitale ale societății, sănătate, siguranță, securitate, bunăstare economică sau socială, iar perturbarea/distrugerea acestor infrastructuri are un impact semnificativ (Directiva 2008/114/CE a Consiliului).

[16] Un procent de 97 % din cetățenii UE s-au confruntat cu știri false, iar 38 % s-au confruntat zilnic cu știri false. A se vedea JOIN(2020)8 final.

[17] Un număr de 13 state membre ale UE au raportat în total 119 atacuri teroriste săvârșite, eșuate și dejucate care s-au soldat cu zece morți și 27 de răniți (Europol, *European Union Terrorism Situation and Trend Report*, 2020).

[18] În 2019 s-au înregistrat șase atacuri teroriste de dreapta (unul a fost dus la capăt, unul a eșuat, patru au fost dejucate: trei state membre), comparativ cu un singur atac în 2018 și mai multe decese survenite în cazuri care nu au fost clasificate drept acte de terorism (Europol, 2020).

din 2018[19]. Una din cinci persoane din UE este foarte îngrijorată în privința unui atac terorist în următoarele 12 luni[20]. Marea majoritate a atacurilor teroriste recente au fost atacuri „cu tehnologie redusă”, actori singuratici care au vizat persoane din spații publice, în timp ce propaganda teroristă online a dobândit o nouă dimensiune odată cu difuzarea în direct pe internet a atacurilor din Christchurch[21]. Amenințarea pe care o reprezintă persoanele radicalizate este ridicată – și poate fi amplificată de luptătorii teroriști străini care se întorc și de extremiștii eliberați din închisoare[22].

Criza a arătat, de asemenea, modul în care amenințările existente pot evolua în noi circumstanțe. Grupurile **infracționale organizate** au exploatat penuriile de bunuri care le-au oferit posibilitatea de a crea noi piețe ilicite. Comerțul cu droguri ilegale rămâne cea mai mare piață infracțională din UE, valoarea minimă a vânzărilor cu amănuntul pe an în UE fiind estimată la 30 de miliarde EUR[23]. Activitățile de trafic de persoane persistă: conform estimărilor, profitul anual global obținut din toate formele de exploatare este de aproape 30 de miliarde EUR[24]. Comerțul internațional cu produse farmaceutice contrafăcute a ajuns la 38,9 miliarde EUR[25]. În același timp, ratele scăzute de confiscare permit infractorilor să continue să își extindă activitățile infracționale și să se infiltreze în economia legală[26]. Infractorii și teroriștii au acces mai ușor la arme de foc pe piața online și prin intermediul noilor tehnologii, cum ar fi imprimarea 3D[27]. Utilizarea inteligenței artificiale, a noilor tehnologii și a roboticii va crește și mai mult riscul ca infractorii să exploateze beneficiile inovării în scopuri răuvoitoare[28].

Aceste amenințări transcend categoriile și afectează diverse părți ale societății în moduri diferite. Ele reprezintă un pericol major pentru cetățeni și întreprinderi și necesită un răspuns global și coerent la nivelul UE. Atunci când vulnerabilitățile în materie de securitate pot apărea chiar și din cauza unor mici aparate domestice interconectate, cum ar fi un frigider sau o mașină de cafea conectate la internet, nu ne mai putem baza doar pe actorii statali tradiționali pentru a ne asigura securitatea. Operatorii economici trebuie să își asume o mai mare responsabilitate pentru securitatea cibernetică a produselor și a serviciilor pe care le introduc pe piață, iar cetățenii trebuie, la rândul lor, să aibă cel puțin cunoștințe de bază în materie de securitate cibernetică pentru a putea să se protejeze.

---

19 A se vedea, de asemenea, Declarația Consiliului privind combaterea antisemitismului și elaborarea unei abordări comune în materie de securitate pentru a proteja mai bine instituțiile și comunitățile evreiești din Europa.

20 Agenția pentru Drepturi Fundamentale a UE: *Your rights matter: Security concerns and experiences*, 2020.

21 Din iulie 2015 până la sfârșitul anului 2019, Europol a identificat conținut cu caracter terorist pe 361 platforme (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*, 2019.

23 *EU Drugs Market Report 2019*, OEDT și Europol.

24 *Report on Trafficking in Human Beings, Financial Business Model*, Europol (2015).

25 Raportul Oficiului Uniunii Europene pentru Proprietate Intelectuală și al OCDE intitulat Trade in counterfeit pharmaceutical products

26 Raport intitulat „Recuperarea și confiscarea activelor: Asigurarea faptului că nu este rentabil să se săvârșească infracțiuni”, COM (2020) 217.

27 În 2017, s-au folosit arme de foc în 41 % din toate atacurile teroriste (Europol, 2018).

28 În iulie 2020, autoritățile de aplicare a legii și autoritățile judiciare din Franța și Țările de Jos, alături de Europol și Eurojust, au prezentat o anchetă comună pentru a demantela EncroChat, o rețea de telefonie criptată utilizată de rețelele infracționale implicate în atacuri violente, în corupție, în tentative de asasinate și în transporturi de droguri pe scară largă.

III. Un răspuns coordonat al UE pentru întreaga societate

UE a demonstrat deja modalitățile prin care poate aduce o veritabilă valoare adăugată. Începând din 2015, uniunea securității a creat noi corelări în modul în care politicile de securitate sunt abordate la nivelul UE. Sunt însă necesare mai multe eforturi pentru a implica întreaga societate, inclusiv administrațiile de la toate nivelurile, mediul de afaceri din toate sectoarele și cetățenii din toate statele membre. Creșterea gradului de sensibilizare cu privire la riscurile pe care le implică dependența[29] și necesitatea unei strategii industriale europene solide[30] sunt argumente pentru o UE cu o masă critică a producției industriale și tehnologice și pentru reziliența lanțului de aprovizionare. Forța constă, de asemenea, în respectarea deplină a drepturilor fundamentale și a valorilor UE: acestea sunt o condiție prealabilă a unor politici de securitate legitime, eficiente și durabile. Prezenta strategie a uniunii securității stabilește direcții de lucru concrete de transpus în practică. Strategia are la bază următoarele obiective comune:

- ***consolidarea capacităților de depistare timpurie, de prevenire și de răspuns rapid la situații de criză:*** Europa trebuie să fie mai rezilientă pentru a preveni, proteja și a face față șocurilor viitoare. Trebuie să creăm capacități pentru detectarea timpurie și răspunsul rapid la crizele de securitate printr-o abordare integrată și coordonată, atât la nivel mondial, cât și prin inițiative sectoriale specifice (de exemplu, pentru sectoarele financiar, energetic, judiciar, al aplicării legii, al asistenței medicale, maritim, al transporturilor), plecând de la instrumentele și inițiativele existente[31]. Comisia va prezenta propuneri privind un sistem amplu de gestionare a crizelor în cadrul UE, care ar putea prezenta relevanță și pentru securitate;
- ***punerea accentului pe rezultate***: o strategie axată pe performanță trebuie să aibă la bază o evaluare atentă a amenințărilor și a riscurilor, pentru a îndrepta eforturile către obținerea efectului optim. Strategia trebuie să definească și să aplice normele corespunzătoare și instrumentele adecvate. Sunt necesare informații strategice fiabile ca bază pentru politicile de securitate ale UE. În cazul în care este necesar un act legislativ al UE, acesta trebuie să fie monitorizat, astfel încât să fie aplicat integral, pentru a se evita fragmentarea și lacunele susceptibile a fi exploatate. Aplicarea eficientă a prezentei strategii va depinde, de asemenea, de asigurarea unei finanțări adecvate în următoarea perioadă de programare, respectiv 2021-2027, inclusiv pentru agențiile conexe ale UE;
- ***asocierea tuturor actorilor din sectoarele public și privat la un efort comun:*** actorii cheie, atât din sectorul public, cât și din cel privat, au fost reticenți în a împărtăși informații relevante din punctul de vedere al securității, din teama de a nu compromite securitatea națională sau din considerente legate de competitivitate.[32] Însă cel mai ridicat grad de eficiență se poate atinge doar dacă toate informațiile sunt valorificate pentru a

[29] Riscurile care derivă din dependența externă implică o expunere mai mare la amenințări potențiale, care variază de la exploatarea vulnerabilităților infrastructurii informatice pentru a compromite infrastructurile critice (de exemplu, energie, transporturi, servicii bancare, sănătate) sau preluarea controlului asupra sistemelor de control industrial la creșterea capacității de furt de date sau spionaj.

[30] Comunicarea Comisiei intitulată „O nouă Strategie industrială pentru Europa”, COM (2020) 102.

[31] Cum ar fi mecanismul integrat pentru un răspuns politic la crize (IPCR), Centrul de coordonare a răspunsului la situații de urgență, Recomandarea Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare [C(2017)6100], Protocolul operațional al UE pentru combaterea amenințărilor hibride, SWD(2016) 227.

[32] Comunicarea comună intitulată „Reziliență, prevenire și apărare: asigurarea unei securități cibernetice solide pentru UE”, JOIN(2017) 450.

ne sprijini reciproc. Aceasta înseamnă în primul rând intensificarea cooperării între statele membre, cooptând autoritățile de aplicare a legii, autoritățile judiciare și alte autorități publice, precum și a cooperării cu instituțiile și agențiile UE, pentru a dobândi cunoștințele necesare și a efectua schimburile de informații necesare pentru identificarea unor soluții comune. Cooperarea cu sectorul privat este, de asemenea, esențială, cu atât mai mult cu cât industria deține o parte importantă a infrastructurii digitale și nedigitale care este esențială pentru combaterea eficientă a criminalității și a terorismului. De asemenea, cetățenii își pot aduce contribuția, de exemplu, prin consolidarea competențelor și a sensibilizării în sensul combaterii criminalității informatice sau a dezinformării. În fine, acest efort comun nu trebuie să se limiteze la frontierele noastre, ci trebuie create legături mai strânse cu parteneri care împărtășesc aceeași viziune.

IV. Protejarea tuturor cetățenilor din UE: prioritățile strategice ale uniunii securității

UE beneficiază de o poziție unică care îi permite să răspundă acestor amenințări și provocări mondiale noi. Analiza amenințărilor de mai sus indică patru priorități strategice interdependente care urmează să fie asumate la nivelul UE, cu respectarea deplină a drepturilor fundamentale: (i) un mediu de securitate adaptat exigențelor viitorului; (ii) combaterea amenințărilor în continuă evoluție; (iii) protejarea europenilor împotriva terorismului și a criminalității organizate; (iv) un ecosistem european solid în materie de securitate.

1. Un mediu de securitate adaptat exigențelor viitorului

Protejarea și reziliența infrastructurilor critice

Cetățenii depind de infrastructurile-cheie în viața lor de zi cu zi, pentru a călători, lucra, beneficia de servicii publice esențiale, cum ar fi spitalele, transporturile, aprovizionarea cu energie, sau pentru a-și exercita drepturile democratice. Dacă aceste infrastructuri nu sunt suficient de bine protejate și suficient de reziliente, atacurile pot provoca perturbări importante – fizice sau digitale – atât în fiecare stat membru, cât și în mod potențial în întreaga UE.

Cadrul existent al UE în materie de protejare și reziliență a infrastructurilor critice[33] nu a ținut pasul cu evoluția riscurilor. Interdependențele tot mai mari înseamnă că perturbările dintr-un sector pot avea un impact imediat asupra operațiunilor din alte sectoare: un atac asupra producției de energie electrică ar putea afecta telecomunicațiile, spitalele, băncile sau aeroporturile, în timp ce un atac asupra infrastructurii digitale ar putea duce la perturbări în rețelele de energie electrică sau financiare. Pe măsură ce economia și societatea transferă o parte tot mai mare a activității în mediul online, aceste riscuri sunt exacerbate. Cadrul legislativ trebuie să abordeze gradul ridicat de interconexiune și interdependență, prin intermediul unor măsuri solide de protecție a infrastructurii critice și al măsurilor de reziliență, atât pe plan cibernetic, cât și fizic. Serviciile esențiale, inclusiv cele care au la bază infrastructuri spațiale, trebuie să fie protejate în mod corespunzător împotriva amenințărilor curente și preconizate, dar trebuie, de asemenea, să fie reziliente. Acest lucru

[33] Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, JO L 194, 19.7.2016; Directiva 2008/114/CE a Consiliului privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora.

implică capacitatea unui sistem de a se pregăti și prevedea, de a absorbi evenimentele adverse, de a se redresa în urma acestora și de a se adapta mai bine la ele.

În același timp, statele membre și-au exercitat marja de apreciere prin punerea în aplicare a legislației existente în diferite feluri. Fragmentarea rezultată poate submina piața internă și poate îngreuna coordonarea transfrontalieră – mai ales în regiunile de frontieră. Operatorii care furnizează servicii esențiale în diferite state membre trebuie să se conformeze unor regimuri de raportare diferite. Comisia analizează dacă **noi cadre, atât pentru infrastructurile fizice, cât și pentru cele digitale** ar putea conferi o mai mare consecvență și o abordare mai coerentă în ceea ce privește asigurarea furnizării fiabile de servicii esențiale. Acest cadru trebuie să fie însoțit de **inițiative sectoriale** care să abordeze riscurile specifice cu care se confruntă infrastructurile critice, cum ar fi transporturile, spațiul, energia, finanțele și sănătatea[34]. Dat fiind gradul ridicat de dependență a sectorului financiar de serviciile informatice și vulnerabilitatea sa ridicată la atacurile cibernetice, primul pas va fi o inițiativă privind reziliența operațională digitală pentru sectoarele financiare. Având în vedere sensibilitatea și impactul particulare ale sistemului energetic, o inițiativă specifică va sprijini o reziliență mai puternică a infrastructurii energetice critice împotriva amenințărilor fizice, cibernetice și hibride, asigurând condiții de concurență echitabile pentru operatorii de energie la nivel transfrontalier.

Efectele cu relevanță în materie de securitate ale investițiilor străine directe care ar putea afecta infrastructurile critice sau tehnologiile critice vor face, de asemenea, obiectul evaluărilor efectuate de statele membre ale UE și de Comisie în temeiul noului cadru european pentru examinarea investițiilor străine directe[35].

UE poate, de asemenea, să creeze noi instrumente care să sprijine reziliența infrastructurilor critice. Internetul mondial a demonstrat până în prezent un nivel ridicat de reziliență, în special în ceea ce privește capacitatea de a sprijini creșterea volumului de trafic. Cu toate acestea, trebuie să fim pregătiți pentru eventualele crize viitoare care amenință securitatea, stabilitatea și reziliența internetului. Pentru a asigurarea continuitatea funcționării internetului este nevoie de soliditate în fața incidentelor cibernetice și a activităților online răuvoitoare și de limitarea dependenței de infrastructuri și servicii situate în afara Europei. Pentru aceasta este nevoie de o combinație de acte legislative, prin revizuirea normelor existente pentru a asigura un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în UE, de investiții suplimentare pentru cercetare și inovare și de luarea în considerare a implementării sau întăririi infrastructurilor și resurselor de internet de bază, în special a sistemului de nume de domenii[36].

---

[34] Având în vedere faptul că sectorul sănătății a fost pus sub presiune în special în timpul crizei provocate de pandemia de COVID-19, Comisia va lua în considerare, de asemenea, inițiative de consolidare a cadrului UE de securitate sanitară și a agențiilor UE responsabile, pentru a răspunde amenințărilor transfrontaliere grave la adresa sănătății.

[35] Odată cu aplicarea sa integrală începând din 11 octombrie 2020, Regulamentul (UE) 2019/452 al Parlamentului European și al Consiliului din 19 martie 2019 de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniune va oferi UE un nou mecanism de cooperare privind investițiile directe din afara UE care ar putea afecta securitatea sau ordinea publică. În temeiul regulamentului, statele membre și Comisia vor evalua riscurile potențiale aferente acestor investiții străine directe și, atunci când este oportun și relevant pentru mai mult de un stat membru, vor propune mijloace adecvate de atenuare a acestor riscuri.

[36] Sistemul de nume de domenii (*domain name system* – DNS) este un sistem de nume ierarhic și descentralizat pentru calculatoare, servicii sau alte resurse conectate la internet sau la o rețea privată. Acest sistem transpune numele de domenii în adresele IP necesare pentru localizarea și identificarea serviciilor și dispozitivelor informatice.

Un element esențial pentru protejarea activelor digitale naționale și ale UE cheie este de a oferi infrastructurilor critice un canal pentru comunicare securizată. Comisia colaborează cu statele membre pentru a institui o infrastructură cuantică *end-to-end*, securizată, certificată, terestră și spațială, alături de sistemul guvernamental securizat de comunicații prin satelit prevăzut în regulamentul privind programul spațial[37].

Securitatea cibernetică

Numărul atacurilor cibernetice este în creștere[38]. Aceste atacuri sunt mai sofisticate ca oricând, provin dintr-o gamă largă de surse din interiorul și din afara UE și vizează segmente în care vulnerabilitatea este maximă. Actorii statali sau susținuți de stat sunt adesea implicați, vizând infrastructurile-cheie digitale, cum ar fi furnizorii importanți de servicii *cloud*[39]. Riscurile cibernetice au devenit, de asemenea, o amenințare semnificativă la adresa sistemului financiar. Fondul Monetar Internațional a estimat pierderea anuală ca urmare a atacurilor cibernetice la 9 % din venitul net al băncilor la nivel mondial, respectiv aproximativ 100 de miliarde USD[40]. Trecerea la dispozitive conectate va aduce beneficii importante utilizatorilor: mai puține date vor fi stocate și prelucrate în centrele de date, tendința fiind de a procesa datele mai aproape de utilizatorul „de la margine”[41], iar securitatea cibernetică nu va mai putea să se concentreze asupra protejării punctelor centrale[42].

În 2017, UE a prezentat o abordare în materie de securitate cibernetică al cărei element central este consolidarea rezilienței, răspunsul rapid și un efect de descurajare eficace[43]. În prezent, UE trebuie să examineze în ce măsură capacitățile sale în materie de securitate cibernetică țin pasul cu realitatea, astfel încât să se asigure atât reziliența, cât și răspunsul. Pentru aceasta este necesară o veritabilă abordare la nivelul întregii societăți, iar instituțiile, agențiile și organele UE, statele membre, industria, mediul academic și persoanele fizice trebuie să acorde securității cibernetice prioritatea cuvenită[44]. Această abordare orizontală trebuie, de asemenea, să fie completată cu abordări sectoriale în materie de securitate cibernetică pentru domenii precum energia, serviciile financiare, transporturile sau sănătatea. Următoarea etapă a activității UE ar trebui regrupată în cadrul Strategiei europene de securitate cibernetică revizuite.

Analizarea unor forme noi și îmbunătățite de cooperare între serviciile de informații, INTCEN UE și alte organizații implicate în securitate ar trebui să facă parte din eforturile de îmbunătățire a securității cibernetice, precum și de combatere a terorismului, a extremismului, a radicalismului și a amenințărilor hibride.

---

[37] Propunere de regulament de instituire a programului spațial al Uniunii și a Agenției Uniunii Europene pentru Programul spațial. COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Atacurile *Distributed Denial of Service (DDoS)* continuă să reprezinte o amenințare permanentă: marii furnizorii au trebuit să atenueze atacurile DDoS masive, ca de exemplu atacul împotriva serviciilor web ale Amazon în februarie 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] Tehnica de calcul la margine (*edge computing*) este o arhitectură IT deschisă, distribuită, caracterizată printr-o capacitate de procesare descentralizată, care înlesnește tehnologiile mobile și ale internetului obiectelor. În tehnica de calcul la margine, datele se prelucrează de către dispozitiv sau de către un calculator sau un server local, în loc să fie transmise unui centru de date.

[42] Comunicarea intitulată „O strategie europeană privind datele”, COM (2020) 66 final.

[43] Comunicarea comună intitulată „Reziliență, prevenire și apărare: asigurarea unei securități cibernetice solide pentru UE”, JOIN(2017) 450.

[44] Raportul „*Cybersecurity – our digital Anchor*” elaborat de Centrul Comun de Cercetare oferă perspective multidimensionale asupra creșterii importanței securității cibernetice în ultimii 40 de ani.

Având în vedere introducerea treptată a **infrastructurii 5G** în UE și potențiala dependență a multor servicii critice de rețelele 5G, consecințele unei perturbări sistemice și de amploare ar fi deosebit de grave. Procesul instituit prin Recomandarea din 2019 a Comisiei privind securitatea cibernetică a rețelelor 5G[45] a stimulat acum acțiunile specifice ale statelor membre cu privire la măsurile-cheie prevăzute într-un set de instrumente 5G[46].

Una dintre cele mai importante nevoi pe termen lung este dezvoltarea unei culturi a **securității cibernetice de la stadiul conceperii** (*cybersecurity by design*), aspectele legate de securitate fiind integrate în produse și servicii încă de la început. O contribuție importantă în acest demers o va avea noul cadru de certificare a securității cibernetice în temeiul Regulamentului privind securitatea cibernetică[47]. Cadrul se aplică deja, două sisteme de certificare fiind în curs de pregătire, iar prioritățile pentru alte sisteme urmează să fie definite mai târziu în cursul acestui an. Cooperarea dintre Agenția UE pentru Securitate Cibernetică (ENISA), autoritățile pentru protecția datelor și Comitetul european pentru protecția datelor[48] este extrem de importantă în acest domeniu.

Comisia a identificat deja necesitatea creării unei **unități comune de securitate cibernetică** care să asigure cooperarea operațională structurată și coordonată. Ar putea fi avut în vedere un mecanism de asistență reciprocă în perioade de criză la nivelul UE. Pornind de la punerea în aplicare a recomandării referitoare la Planul de acțiune privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare[49], unitatea comună de securitate cibernetică ar putea consolida încrederea între diferiții actori din ecosistemul european al securității cibernetice și ar putea oferi un serviciu esențial pentru statele membre. Comisia va iniția discuții cu părțile interesate relevante (începând cu statele membre) și va stabili un proces, etape și termene clare până la sfârșitul anului 2020.

De asemenea, sunt importante normele comune privind securitatea informațiilor și securitatea cibernetică pentru toate instituțiile, organele și agențiile UE. Scopul ar trebui să fie crearea de standarde comune obligatorii și ridicate pentru schimbul securizat de informații și securitatea infrastructurilor și sistemelor digitale în toate instituțiile, organele și agențiile UE. Acest nou cadru ar trebui să stea la baza unei cooperări operaționale solide și eficiente în materie de securitate cibernetică în instituțiile, organele și agențiile UE, punând accentul pe rolul Centrului de răspuns la incidente de securitate cibernetică (CERT-UE) pentru instituțiile, organele și agențiile UE.

Având în vedere caracterul mondial al atacurilor cibernetice, crearea și menținerea unor **parteneriate internaționale** solide este fundamentală pentru acțiunile ulterioare de prevenire, descurajare și răspuns la atacurile cibernetice. Cadrul privind un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică”)[50] stabilește măsuri în cadrul politicii externe și de securitate comune, inclusiv măsuri restrictive (sancțiuni), care pot fi aplicate ca recurs împotriva unor

[45] Recomandarea Comisiei intitulată „Securitatea cibernetică a rețelelor 5G”, C(2019) 2335 final. Revizuirea recomandării este prevăzută în ultimul trimestru al anului 2020.

[46] A se vedea Raportul din 24 iulie 2020 al Grupului de cooperare NIS privind punerea în aplicare a setului de instrumente.

[47] Regulamentul 2019/881 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (Regulamentul privind securitatea cibernetică).

[48] Comunicarea intitulată „Protecția datelor ca pilon al capacitării cetățenilor și al abordării UE privind tranziția digitală – doi ani de aplicare a Regulamentului general privind protecția datelor”, COM(2020) 264.

[49] Recomandarea 2017/1584 a Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/ro/pdf

activități care dăunează intereselor politice, de securitate și economice ale UE. UE ar trebui, de asemenea, să își aprofundeze activitatea prin intermediul fondurilor de dezvoltare și cooperare pentru a asigura consolidarea capacității de sprijinire a statelor partenere în întărirea ecosistemelor lor digitale, adoptarea reformelor legislative naționale și aderarea la standardele internaționale. Astfel crește reziliența întregii comunități și capacitatea de contracarare și răspuns eficace la amenințările cibernetice. Aceasta presupune acțiuni specifice de promovare a standardelor UE și a legislației relevante menite să asigure un grad mai mare al securității cibernetice în țările partenere care sunt vizate de politica de vecinătate[51].

Protejarea spațiilor publice

Atacurile teroriste recente s-au concentrat asupra **spațiilor publice**, inclusiv asupra lăcașurilor de cult și a nodurilor de transport, exploatând caracterul deschis și accesibil al acestora. Intensificarea terorismului, declanșată de extremismul politic sau ideologic, a exacerbat această amenințare. Este, așadar, necesar să se asigure atât o mai bună protecție fizică a acestor locuri, cât și sisteme de detectare adecvate, fără a submina libertățile cetățenilor[52]. Comisia va consolida cooperarea dintre sectorul public și cel privat pentru a proteja spațiile publice, cu ajutorul finanțării, al schimbului de experiență și de bune practici, al orientărilor specifice[53] și al recomandărilor[54]. Abordarea va prevedea, de asemenea, acțiuni de sensibilizare, cerințe în materie de performanță și testarea echipamentelor de detectare, precum și intensificarea verificărilor antecedentelor pentru a aborda amenințările interne. Un aspect important care trebuie avut în vedere este faptul că minoritățile și persoanele vulnerabile pot fi afectate în mod disproporționat, inclusiv persoanele vizate din cauza religiei sau a genului și, prin urmare, trebuie să se acorde o atenție deosebită acestui aspect. Autoritățile publice locale și regionale au un rol important în îmbunătățirea securității spațiilor publice. Comisia contribuie, de asemenea, la promovarea demersurilor de inovare depuse de orașe în materie de securitate în spațiile publice[55]. Lansarea, în noiembrie 2018, în cadrul Agendei urbane[56] a unui nou parteneriat privind „securitatea în spațiile publice" reflectă angajamentul solid al statelor membre, al Comisiei și orașelor de a aborda mai bine amenințările la adresa securității în spațiul urban.

Piața **dronelor** continuă să se extindă, dronele fiind frecvent utilizate în mod avantajos și legitim. Cu toate acestea, dronele pot fi, de asemenea, utilizate în mod abuziv de către infractori și teroriști, spațiile publice fiind expuse în mod special riscului. Pot fi vizate persoane, adunări de persoane, infrastructuri critice, autorități de aplicare a legii, frontiere

---

[51] A se vedea Orientările privind consolidarea capacităților cibernetice externe ale UE, adoptate în concluziile Consiliului din 26 iunie 2018.

[52] Sistemele de identificare biometrică la distanță trebuie monitorizate în mod specific. Punctele de vedere inițiale ale Comisiei sunt prezentate în Cartea albă a Comisiei din 19 februarie 2020 privind inteligența artificială, COM (2020) 65.

[53] De exemplu, Orientările privind selectarea unor soluții adecvate pentru barierele de securitate pentru protecția spațiului public (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Orientările privind bunele practici sunt prezentate în SWD(2019) 140, inclusiv o secțiune privind cooperarea dintre sectorul public și cel privat. Finanțarea în cadrul FSI-Poliție se axează în special pe consolidarea cooperării dintre sectorul public și cel privat.

[55] Trei orașe (Pireu în Grecia, Tampere în Finlanda și Torino în Italia) vor testa noi soluții în cadrul Acțiunilor urbane inovatoare, care beneficiază de cofinanțare de la Fondul European de Dezvoltare Regională (FEDR).

[56] Agenda urbană a UE reprezintă o nouă metodă de lucru pe mai multe niveluri, care promovează cooperarea între statele membre, orașe, Comisia Europeană și alte părți interesate, pentru a stimula creșterea, calitatea vieții și inovarea în orașele Europei și pentru a identifica și a aborda cu succes provocările sociale.

sau spații publice. Cunoștințele privind modalitățile de utilizare a dronelor în conflicte ar putea ajunge în Europa fie direct (prin intermediul luptătorilor teroriști străini care se întorc), fie prin mediul online. Normele elaborate deja de Agenția Europeană de Siguranță a Aviației sunt un prim pas important în domenii precum înregistrarea operatorilor de drone și identificarea obligatorie la distanță a dronelor. În contextul în care dronele sunt disponibile pe scară mai largă, mai accesibile din punctul de vedere al costului și mai performante, se impun măsuri suplimentare. Printre acestea s-ar putea număra schimbul de informații, orientări și bune practici care să fie utilizate de către toți, inclusiv în materie de aplicare a legii, precum și mai multe teste ale măsurilor antidrone[57]. În plus, ar trebui analizate și abordate în continuare implicațiile utilizării dronelor în spațiile publice asupra protecției vieții private și a datelor.

Acțiuni-cheie
• Legislație privind protejarea infrastructurii critice și reziliența acesteia • Revizuirea Directivei privind securitatea rețelelor și a sistemelor informatice • O inițiativă privind reziliența operațională a sectorului financiar • Protecția și securitatea cibernetică a infrastructurii energetice critice și cod de rețea privind securitatea cibernetică pentru fluxurile transfrontaliere de energie electrică • O strategie europeană de securitate cibernetică • Următoarele etape în vederea creării unei unități comune de securitate cibernetică • Norme comune privind securitatea informațiilor și securitatea cibernetică pentru instituțiile, organele și agențiile UE • Intensificarea cooperării pentru protejarea spațiilor publice, inclusiv a lăcașurilor de cult • Schimbul de bune practici în materie de combatere a utilizării abuzive a dronelor

2. Combaterea amenințărilor în continuă evoluție

Criminalitatea informatică

Tehnologia oferă noi oportunități pentru societate. De asemenea, oferă noi instrumente pentru sistemul judiciar și pentru aplicarea legii. Însă, în același timp, lasă loc de acțiune pentru infractori. Programele malware, furtul de date cu caracter personal sau de date comerciale prin intermediul pirateriei informatice și blocarea activității digitale, cauzând daune financiare sau de reputație, toate aceste fenomene sunt în creștere. Primul mijloc de apărare este un mediu rezilient creat de o securitate cibernetică solidă. Autoritățile de aplicare a legii trebuie să fie în măsură să intervină în sfera anchetelor digitale, în baza unor norme clare de investigare și urmărire penală a infracțiunilor și care prevăd protecția adecvată a victimelor. Acest demers ar trebui să aibă ca temei activitatea Grupului operativ privind acțiunea comună de combatere a criminalității informatice din cadrul Europol și Protocolul privind răspunsul în caz de urgență al autorităților de aplicare a legii, creat pentru a coordona răspunsul la atacurile cibernetice de mare amploare. Existența unor mecanisme eficiente care să faciliteze parteneriatele public-privat și cooperarea dintre sectorul public și cel privat este, de asemenea, esențială.

În paralel, lupta împotriva criminalității informatice ar trebui să devină o prioritate strategică în materie de comunicare în întreaga UE, pentru a atrage atenția europenilor asupra

[57] S-a instituit recent un program multianual de testare pentru a sprijini statele membre în elaborarea unei metodologii comune și a unei platforme de testare în acest domeniu.

riscurilor și asupra măsurilor preventive pe care ar putea să le ia. Acest demers ar trebui să fie parte a unei abordări proactive. O etapă esențială este, de asemenea, aplicarea integrală a cadrului juridic actual[58]: Comisia va fi pregătită să recurgă la proceduri de constatare a neîndeplinirii obligațiilor, dacă este cazul, precum și să revizuiască acest cadru pentru a se asigura că este în continuare adecvat scopului. Comisia va analiza, de asemenea, împreună cu Europol și Agenția UE pentru Securitate Cibernetică, ENISA, fezabilitatea unui sistem de alertă rapidă al UE cu privire la criminalitatea informatică, care ar putea asigura fluxul de informații și reacția rapidă atunci când se intensifică acțiunile de criminalitate informatică.

Criminalitatea informatică este o problemă mondială, cooperarea internațională eficace fiind necesară. UE sprijină Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică, care este un cadru eficient și consacrat, care permite tuturor țărilor să identifice sistemele și canalele de comunicare de care au nevoie pentru a putea coopera eficient.

Aproape jumătate din cetățenii UE se tem că datele ar putea fi utilizate în mod abuziv[59], iar **furtul de identitate** reprezintă o preocupare majoră[60]. Utilizarea frauduloasă a identității în scopul obținerii unui câștig financiar este doar un aspect, căci pot apărea, de asemenea, consecințe majore de ordin personal și psihologic, postările ilegale făcute de persoana care a comis furtul de identitate putând să rămână în mediul online timp de mai mulți ani. Comisia va analiza potențialele măsuri practice de protejare a victimelor împotriva tuturor formelor de furt de identitate, ținând seama de viitoarea inițiativă privind identitatea digitală europeană[61].

Combaterea criminalității informatice înseamnă o abordare orientată spre viitor. Pe măsură ce societatea recurge la noi evoluții tehnologice pentru a consolida economia și societatea, infractorii pot încerca, de asemenea, să exploateze aceste instrumente în scopuri răuvoitoare. De exemplu, infractorii pot utiliza inteligența artificială pentru a detecta și identifica parole sau pentru a simplifica crearea de programe malware, pentru a exploata imaginile și înregistrările audio care pot fi apoi utilizate pentru furtul de identitate sau fraudă.

Modernizarea aplicării legii

Autoritățile de aplicare a legii și practicienii din domeniul justiției trebuie să se adapteze la noile tehnologii. Date fiind evoluțiile tehnologice și amenințările emergente, autoritățile de aplicare a legii trebuie să aibă acces la noi instrumente, să dobândească noi competențe și să dezvolte tehnici de investigare alternative. Pentru a completa acțiunile legislative menite să îmbunătățească accesul transfrontalier la probele electronice în cadrul anchetelor penale, UE poate veni în ajutorul autorităților de aplicare a legii în scopul de a crea capacitatea necesară în vederea identificării, obținerii și citirii datelor necesare pentru investigarea infracțiunilor și în vederea utilizării acestor date ca probe în instanță. Comisia va analiza măsurile de **consolidare a capacității de aplicare a legii în anchetele digitale**, definind modul de utilizare optimă a cercetării și dezvoltării pentru a crea noi instrumente pentru aplicarea legii și modul în care formarea poate pune la dispoziția autorităților de aplicare a legii și a

[58] Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice.

[59] Un procent de 46 % (Eurobarometru privind atitudinea europenilor față de securitatea cibernetică, ianuarie 2020).

[60] Marea majoritate a respondenților la sondajul Eurobarometru din 2018 „Atitudinea europenilor față de securitatea internetului” (95 %) a considerat furtul de identitate drept o infracțiune gravă, iar șapte din zece respondenți au declarat că este o infracțiune foarte gravă. Sondajul Eurobarometru publicat în ianuarie 2020 a confirmat preocupările legate de criminalitatea informatică, frauda online și furtul de identitate: două treimi dintre respondenți și-au exprimat îngrijorarea în legătură cu frauda bancară (67 %) sau furtul de identitate (66 %).

[61] Comunicarea din 19 februarie 2020 intitulată „Conturarea viitorului digital al Europei”, COM (2020) 67.

sistemului judiciar setul adecvat de competențe. Acest demers va presupune, de asemenea, furnizarea de evaluări și metode de testare științifice riguroase, prin intermediul Centrului Comun de Cercetare al Comisiei.

Abordările comune pot asigura, de asemenea, **integrarea** în politica de securitate a **inteligenței artificiale, a capacităților spațiale, a volumelor mari de date și a calculului de înaltă performanță**, în așa fel încât acestea să fie eficiente atât în ceea ce privește combaterea infracțiunilor, cât și în asigurarea drepturilor fundamentale. Inteligența artificială ar putea servi drept un instrument solid de combatere a criminalității, creând capacități enorme de investigație prin analizarea unui volum mare de informații și prin identificarea tiparelor și a anomaliilor[62]. De asemenea, inteligența artificială poate pune la dispoziție instrumente concrete, de exemplu, pentru a contribui la identificarea conținutului online cu caracter terorist, pentru a descoperi tranzacțiile suspecte din vânzarea de produse periculoase sau pentru a oferi asistență cetățenilor în situații de urgență. Pentru a putea valorifica acest potențial este necesar să se reunească cercetarea, inovarea și utilizatorii de inteligență artificială cu guvernanța și infrastructura tehnică adecvată, implicând în mod activ sectorul privat și mediul academic. Aceasta înseamnă, de asemenea, asigurarea celor mai înalte standarde de conformitate cu drepturile fundamentale, garantând în același timp o protecție eficace a cetățenilor. În special, deciziile care afectează persoanele trebuie să facă obiectul controlului uman și să respecte legislația UE aplicabilă în acest domeniu[63].

Informațiile și elementele de probă electronice sunt necesare în aproximativ 85 % din investigațiile privind infracțiuni grave, în timp ce 65 % din totalul cererilor sunt adresate furnizorilor care își au sediul într-o altă jurisdicție[64]. Dat fiind că urmele fizice tradiționale se regăsesc acum în mediul online, se adâncește și mai mult decalajul dintre capacitățile autorităților de aplicare a legii și cele ale infractorilor. Este esențial să se stabilească norme clare pentru accesul transfrontalier la probe electronice în cadrul urmăririlor penale. De aceea, pentru ca practicienii să aibă la dispoziție un instrument eficient, este esențial ca Parlamentul European și Consiliu să adopte cu celeritate propunerile privind probele electronice. De asemenea, pentru a stabili norme compatibile la nivel internațional, este esențial accesul transfrontalier la probele electronice prin negocieri internaționale multilaterale și bilaterale[65].

Accesul la probe digitale depinde, de asemenea, de disponibilitatea informațiilor. Dacă datele sunt șterse prea repede, pot dispărea probe importante și nu va mai fi posibil să se identifice și să se localizeze suspecții și rețelele infracționale (și nici victimele). Pe de altă parte, sistemele de păstrare a datelor implică probleme de protecție a vieții private. În funcție de rezultatul cauzelor aflate pe rolul Curții de Justiție a Uniunii Europene, Comisia va evalua calea de urmat în ceea ce privește păstrarea datelor.

Accesul la informațiile privind înregistrarea numelor de domenii de internet („date WHOIS”)[66] este important pentru urmăririle penale, securitatea cibernetică și protecția

[62] De exemplu, în infracțiunile financiare.

[63] Aceasta înseamnă respectarea legislației existente, inclusiv a Regulamentului (UE) 2016/679 privind protecția generală a datelor, precum și a Directivei (UE) 2016/680 privind protecția datelor în materie de asigurare a respectării legii care reglementează prelucrarea datelor cu caracter personal în scopul depistării, al prevenirii, al investigării și al urmăririi penale a infracțiunilor sau al executării pedepselor.

[64] Documentul SWD(2018) 118 final al Comisiei.

[65] În particular, Al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică și un acord între UE și Statele Unite privind accesul transfrontalier la probele electronice.

[66] Stocate în baze de date menținute de 2 500 de operatori de registre din întreaga lume.

consumatorilor. Cu toate acestea, obținerea accesului la aceste informații devine tot mai dificilă, în așteptarea adoptării unei noi politici WHOIS de către Corporația pentru alocarea de nume și numere de domenii internet (ICANN). Comisia va continua colaborarea cu ICANN și cu comunitatea multiparticipativă pentru a se asigura că persoanele care solicită accesul legitim la date, inclusiv autoritățile de aplicare a legii, pot să obțină accesul efectiv la datele WHOIS în conformitate cu reglementările în materie de protecție a datelor de la nivelul UE și internațional. Acest demers va presupune evaluarea soluțiilor posibile, inclusiv necesitatea unor acte legislative care să clarifice normele de acces la aceste informații.

Autoritățile de aplicare a legii și autoritățile judiciare trebuie, de asemenea, să dispună de mijloacele de obținere a datelor și probelor necesare de îndată ce **arhitectura 5G pentru telecomunicații mobile** este implementată pe deplin în UE, într-un mod care respectă confidențialitatea comunicațiilor. Comisia va sprijini o abordare consolidată și coordonată în momentul stabilirii standardelor internaționale, definind cele mai bune practici, procesul și interoperabilitatea tehnică în domenii tehnologice cheie precum IA, internetul obiectelor sau tehnologiile *blockchain*.

În prezent, o mare parte a anchetelor privind toate formele de criminalitate și terorism au o componentă legată de **informații criptate**. Criptarea este esențială pentru lumea digitală, contribuind la securizarea sistemelor și tranzacțiilor digitale și, de asemenea, la protejarea unei serii de drepturi fundamentale, inclusiv a libertății de exprimare, a vieții private și a protecției datelor. Cu toate acestea, dacă este utilizată în scopuri infracționale, criptarea poate să camufleze identitatea infractorilor și conținutul comunicațiilor lor. Comisia va analiza și va sprijini soluțiile tehnice, operaționale și juridice echilibrate la aceste provocări și va promova o abordare care să mențină eficacitatea criptării în protejarea vieții private și a securității comunicațiilor, oferind, în același timp, un răspuns eficace la criminalitate și terorism.

Combaterea conținutului online ilegal

Alinierea securității în mediul online și în cel fizic presupun eforturi continue în materie de **combatere a conținutului online ilegal**. Tot mai frecvent, amenințările majore la adresa cetățenilor, cum ar fi terorismul, extremismul sau abuzul sexual asupra copiilor, se bazează pe mediul digital: sunt, așadar, necesare acțiuni concrete și un cadru care să asigure respectarea drepturilor fundamentale. Un prim pas esențial este încheierea rapidă a negocierilor cu privire la legislația propusă în materie de conținut online cu caracter terorist[67] și asigurarea punerii sale în aplicare. Consolidarea cooperării voluntare între autoritățile de aplicare a legii și sectorul privat în cadrul **Forumului UE pentru internet** este, de asemenea, o componentă indispensabilă pentru combaterea utilizării abuzive a internetului de către teroriști, extremiști violenți și infractori. Unitatea UE de semnalare a conținutului online din cadrul Europol va avea în continuare un rol fundamental în monitorizarea activității grupurilor teroriste în mediul online și a acțiunilor întreprinse de platforme[68], precum și în dezvoltarea în continuare a **Protocolului UE pentru situații de criză**[69]. Totodată, Comisia va continua să stabilească contacte cu partenerii internaționali, inclusiv prin participarea la **Forumul global al internetului pentru combaterea terorismului**, pentru a combate aceste provocări la nivel mondial. Va continua activitatea de

[67] Propunere privind prevenirea diseminării conținutului online cu caracter terorist, COM (2018) 640, 12 septembrie 2018.

[68] Europol, noiembrie 2019.

[69] O Europă care protejează – Protocolul UE pentru situații de criză: răspunsul la conținutul online cu caracter terorist (octombrie 2019).

sprijinire a dezvoltării de discursuri alternative și de contradiscursuri prin Programul de capacitare a societății civile[70].

Pentru a preveni și a contracara răspândirea discursurilor ilegale de incitare la ură din mediul online, Comisia a lansat în 2016 Codul de conduită privind combaterea discursului ilegal de incitare la ură din mediul online, platformele online asumându-și în mod voluntar angajamentul de a înlătura conținuturile care constau în discursuri de incitare la ură. Cea mai recentă evaluare arată că într-un interval de 24 de ore companiile evaluează 90 % din conținutul semnalat și înlătură 71 % din conținutul considerat a fi discurs ilegal de incitare la ură. Cu toate acestea, platformele trebuie să îmbunătățească în continuare transparența și feedbackul către utilizatori și să asigure evaluarea consecventă a conținutului semnalat[71].

De asemenea, Forumul UE pentru internet va facilita schimburile cu privire la tehnologia existentă și dezvoltarea de tehnologii pentru a aborda provocările legate de abuzuri sexuale asupra copiilor în mediul online. Combaterea abuzurilor sexuale asupra copiilor în mediul online se află în centrul unei noi strategii de intensificare a **luptei împotriva abuzurilor sexuale asupra copiilor**[72], care va urmări să maximizeze utilizarea instrumentelor disponibile la nivelul UE pentru a combate aceste infracțiuni. Companiile trebuie să își poată continua activitatea de depistare și înlăturare a materialelor care conțin abuzuri sexuale asupra copiilor din mediul online, iar daunele cauzate de aceste materiale impun definirea unui cadru care să stabilească obligații clare și permanente pentru soluționarea problemei. Strategia va menționa că, pentru a combate în mod mai eficace abuzurile sexuale asupra copiilor în mediul online, Comisia va începe să pregătească legislație specifică sectorului, cu respectarea deplină a drepturilor fundamentale.

La un nivel mai general, viitorul act legislativ privind serviciile digitale va clarifica și actualiza, de asemenea, normele privind răspunderea și siguranța care se aplică în cazul serviciilor digitale și va elimina măsurile de descurajare care îngrădesc acțiunile de combatere a conținuturilor, bunurilor sau serviciilor ilegale.

Totodată, Comisia va continua să stabilească contacte cu partenerii internaționali și cu **Forumul global al internetului pentru combaterea terorismului**, inclusiv prin intermediul comitetului consultativ independent, pentru a discuta despre modalitățile de combatere a acestor provocări la nivel mondial, menținând în același timp valorile și drepturile fundamentale ale UE. De asemenea, ar trebui abordate teme noi, cum ar fi algoritmii sau jocurile online[73].

Amenințările hibride

Amploarea și diversitatea amenințărilor hibride sunt, în prezent, fără precedent. Criza provocată de pandemia de COVID-19 a confirmat acest lucru, mai mulți actori statali și nestatali încercând să instrumentalizeze pandemia – în special prin manipularea mediului informațional și prin punerea la încercare a infrastructurilor de bază. Acest lucru creează riscul de reducere a coeziunii sociale și de subminare a încrederii în instituțiile UE și guvernele statelor membre.

---

[70] Legat de activitatea programului pentru sensibilizarea publicului cu privire la radicalizare, a se vedea secțiunea IV.3 de mai jos.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Strategia UE pentru o combatere mai eficace a abuzului sexual asupra copiilor, COM(2020) 607.

[73] Teroriștii folosesc tot mai frecvent sistemul de mesagerie al platformelor de jocuri pentru schimburi și tinerii teroriști reiau atacurile violente în cadrul jocurilor video.

Abordarea UE cu privire la amenințările hibride este prezentată în Cadrul comun din 2016[74] și în Comunicarea comună din 2018 privind consolidarea rezilienței la amenințările hibride[75]. Acțiunea la nivelul UE este susținută de un set amplu de instrumente care acoperă legătura intern-extern și are la bază o abordare la nivelul întregii societăți și cooperarea strânsă cu partenerii strategici, în special NATO și G7. Un raport privind punerea în aplicare a abordării UE cu privire la amenințările hibride este publicat împreună cu prezenta strategie[76]. Pe baza cartografierii[77] prezentate în paralel cu prezenta strategie, serviciile Comisiei și Serviciul European de Acțiune Externă vor crea o **platformă online restricționată** ca referință pentru statele membre cu privire la instrumentele și măsurile de combatere a amenințărilor hibride la nivelul UE.

Întrucât responsabilitatea contracarării amenințărilor hibride le revine în primul rând statelor membre – date fiind legăturile intrinseci cu politicile naționale de securitate și apărare – unele puncte vulnerabile sunt comune tuturor statelor membre și unele amenințări se extind la nivel transfrontalier, cum ar fi vizarea rețelelor sau a infrastructurii transfrontaliere. Comisia și Înaltul Reprezentant vor prezenta o abordare a UE cu privire la amenințările hibride care integrează dimensiunea externă și internă în mod unitar și care reunește considerentele naționale și cele de la nivelul UE. Abordarea trebuie să acopere întregul spectru de acțiuni – de la depistare timpurie, analiză, sensibilizare, consolidarea rezilienței și prevenire până la răspunsul în caz de criză și gestionarea consecințelor.

Pe lângă consolidarea punerii în aplicare, amenințările hibride fiind în continuă evoluție, se va pune un accent deosebit pe **integrarea considerentelor legate de amenințările hibride în procesul de elaborare a politicilor**, pe obținerea celor mai recente informații cu privire la evoluțiile dinamice și pe asigurarea faptului că nu este trecută cu vederea nicio inițiativă care ar putea fi relevantă. Efectele noilor inițiative vor fi evaluate, de asemenea, din perspectiva amenințărilor hibride, inclusiv prin inițiative în domenii care, până în prezent, nu au intrat în sfera de aplicare a cadrului privind contracararea amenințărilor hibride, cum ar fi educația, tehnologia și cercetarea. Această abordare ar beneficia de pe urma activității desfășurate cu privire la conceptualizarea amenințărilor hibride, care oferă o imagine cuprinzătoare asupra diferitelor instrumente pe care le pot utiliza adversarii[78]. Scopul ar trebui să fie asigurarea faptului că procesul decizional este fundamentat pe rapoarte privind evoluția amenințărilor hibride, periodice, cuprinzătoare și bazate pe informații. Raportarea se va face în mare măsură în baza informațiilor de la statele membre și a consolidării ulterioare a cooperării în materie de informații cu serviciile competente ale statelor membre, prin intermediul INTCEN UE.

Pentru a dispune de elementele necesare pentru **conștientizarea diverselor situații**, serviciile Comisiei și Serviciul European de Acțiune Externă vor analiza opțiunile de integrare a fluxurilor de informații din diferite surse, inclusiv de la statele membre, precum și de la agențiile UE, cum ar fi ENISA, Europol și Frontex. Celula de fuziune a UE

---

[74] Cadrul comun privind contracararea amenințărilor hibride – Un răspuns al Uniunii Europene, JOIN(2016) 18.

[75] Creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride, JOIN (2018) 16.

[76] SWD(2020) 153, Raport privind punerea în aplicare a Cadrului comun din 2016 privind contracararea amenințărilor hibride și a Comunicării comune din 2018 privind creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride.

[77] SWD (2020) 152, Cartografierea măsurilor legate de creșterea rezilienței și de combatere a amenințărilor hibride.

[78] *The Landscape of Hybrid Threats: A conceptual Model*, JRC117280, document elaborat în comun de Centrul Comun de Cercetare și Centrul de Excelență pentru Contracararea Amenințărilor Hibride.

împotriva amenințărilor hibride va rămâne punctul central al UE pentru evaluarea amenințărilor hibride. **Consolidarea rezilienței** este esențială pentru prevenirea și protejarea împotriva amenințărilor hibride. Prin urmare, este esențial să se urmărească în mod sistematic și să se măsoare în mod obiectiv progresele înregistrate în acest domeniu. Un prim pas va fi identificarea scenariilor de referință sectoriale în materie de reziliență la amenințările hibride atât pentru statele membre, cât și pentru instituțiile și organele UE. În fine, pentru a intensifica **pregătirea și răspunsul la situațiile de criză provocate de atacurile hibride**, protocolul existent ar trebui revizuit, astfel cum se prevede în Protocolul operațional al UE din 2016 pentru combaterea amenințărilor hibride[79], pentru a ține seama de revizuirea și consolidarea mai ample a sistemului UE de răspuns la situații de criză, care face în prezent obiectul unei analize[80]. Scopul este de a maximiza efectul acțiunii UE prin reunirea rapidă a răspunsurilor sectoriale și asigurarea unei cooperări armonioase cu partenerii noștri și în primul rând cu NATO.

Acțiuni-cheie
• Asigurarea faptului că legislația în materie de criminalitate informatică este pusă în aplicare și adecvată scopului • O strategie a UE pentru combaterea mai eficace a abuzurilor sexuale asupra copiilor • Propuneri privind detectarea și înlăturarea materialelor care conțin abuzuri sexuale asupra copiilor • O abordare a UE privind contracararea amenințărilor hibride • Revizuirea Protocolului operațional al UE pentru combaterea amenințărilor hibride • Evaluarea modalităților de consolidare a capacității de asigurare a aplicării legii în cadrul investigațiilor digitale

3. Protejarea europenilor împotriva terorismului și a criminalității organizate

Terorismul și radicalizarea

Amenințarea teroristă în UE se menține la un nivel ridicat. În pofida scăderii numărului de atacuri în general, acestea pot avea încă un efect devastator. În sens mai general, radicalizarea poate, de asemenea, să polarizeze și să destabilizeze coeziunea socială. Statelor membre le revine responsabilitatea principală de combatere a terorismului și a radicalizării. Cu toate acestea, dimensiunea preponderent transfrontalieră/intersectorială a amenințării reclamă măsuri suplimentare în demersul de cooperare și coordonare la nivelul UE. Punerea efectivă în aplicare a legislației UE privind combaterea terorismului, inclusiv a măsurilor restrictive[81], reprezintă o prioritate. Se dorește în continuare extinderea mandatului Parchetului European, astfel încât să includă infracțiunile de terorism transfrontaliere.

Primul pas în combaterea terorismului este abordarea cauzelor profunde. Polarizarea societății, discriminarea reală sau percepută și alți factori psihologici și sociologici pot întări

[79] Protocolul operațional al UE pentru combaterea amenințărilor hibride, SWD(2016) 227.

[80] În urma conferinței video din 26 martie 2020, membrii Consiliului European au adoptat o declarație privind acțiunile UE ca răspuns la epidemia de COVID-19, invitând Comisia să prezinte propuneri pentru un sistem mai ambițios și mai amplu de gestionare a crizelor în cadrul UE.

[81] Consiliul a adoptat măsuri restrictive cu privire la ISIL (Da'esh) și Al-Qaida, precum și măsuri restrictive specifice îndreptate împotriva anumitor persoane și entități în vederea combaterii terorismului. A se vedea EU Sanctions Map (https://www.sanctionsmap.eu/#/main) pentru o prezentare generală a tuturor măsurilor restrictive.

vulnerabilitatea oamenilor la discursurile radicale. În acest context, combaterea **radicalizării** este strâns corelată cu promovarea coeziunii sociale la nivel local, național și european. În ultimii zece ani s-au elaborat mai multe inițiative și politici care au avut un impact important, în special prin intermediul Rețelei UE pentru sensibilizarea publicului cu privire la radicalizare și al Inițiativei „Orașele din UE împotriva radicalizării”[82]. Este momentul să se ia în considerare acțiuni de optimizare a politicilor, inițiativelor și fondurilor UE pentru combaterea radicalizării. Aceste acțiuni pot sprijini dezvoltarea capacităților și a competențelor, consolida cooperarea, întări baza de cunoștințe și contribui la evaluarea progreselor, implicând toate părțile interesate relevante, inclusiv practicienii din prima linie, factorii de decizie politică și mediul academic[83]. Politicile necoercitive, cum ar fi educația, cultura, tineretul și sportul, ar putea contribui la prevenirea radicalizării, oferind oportunități pentru tinerii expuși riscurilor și asigurând coeziunea în interiorul UE[84]. Printre domeniile prioritare se numără activități de detectare timpurie și de gestionare a riscurilor, de consolidare a rezilienței și de dezangajare, precum și de reabilitare și reintegrare în societate.

Teroriștii au încercat să obțină și să folosească pe post de arme materiale **chimice, biologice, radiologice și nucleare** (CBRN)[85], precum și să dobândească cunoștințele și capacitatea pentru a le putea utiliza[86]. Potențialul atacurilor CBRN are un rol important în propaganda teroristă. În contextul în care potențialul de cauzare de prejudicii este atât de ridicat, este necesar să se acorde o atenție specială. Pe baza abordării utilizate pentru a reglementa accesul la precursorii de explozivi, Comisia va analiza posibilitatea de a restricționa accesul la anumite substanțe chimice periculoase care ar putea fi folosite pentru a comite atacuri. Dezvoltarea capacităților UE de răspuns în materie de protecție civilă (rescEU) în domeniul CBRN va fi, de asemenea, esențială. Cooperarea cu țările terțe este, de asemenea, importantă pentru a consolida o cultură comună a siguranței și securității în domeniul CBRN, utilizând pe deplin centrele de excelență în domeniul CBRN ale UE de anvergură mondială. Această cooperare va include evaluări naționale ale decalajelor și ale riscurilor, sprijin pentru planurile de acțiune naționale și regionale în domeniul CBRN, schimburi de bune practici și activități de consolidare a capacităților în domeniul CBRN.

UE a elaborat cele mai avansate acte legislative din lume de restricționare a accesului la **precursorii de explozivi**[87] și de detectare a tranzacțiilor suspecte care vizau construirea de dispozitive explozive improvizate. Însă amenințarea reprezentată de explozivii artizanali este în continuare ridicată, aceștia fiind utilizați în numeroase atacuri din UE[88]. Primul pas trebuie să fie punerea în aplicare a normelor, precum și asigurarea faptului că mediul online nu permite eludarea controalelor.

---

[82] Inițiativa-pilot „Orașele din UE împotriva radicalizării” are obiectivul dublu de a promova schimbul de expertiză între orașele din UE și de a colecta feedback cu privire la cele mai adecvate modalități de sprijinire a comunităților locale la nivelul UE.

[83] De exemplu, finanțarea în cadrul Fondului european de securitate și al programului „Cetățenie”.

[84] Acțiuni ale UE, precum schimburile virtuale Erasmus+, e-twinning.

[85] În ultimii doi ani s-au înregistrat, de exemplu, mai multe cazuri atât în Europa (Franța, Germania, Italia), cât și în alte părți (Tunisia, Indonezia) în care s-au folosit agenți biologici (de obicei toxine pe bază de plante).

[86] Consiliul a adoptat măsuri restrictive împotriva proliferării și utilizării armelor chimice.

[87] Substanțe chimice care ar putea fi utilizate în mod abuziv pentru fabricarea de explozivi artizanali. Aceste substanțe sunt reglementate de Regulamentul (UE) 2019/1148 privind comercializarea și utilizarea precursorilor de explozivi.

[88] Câteva exemple de astfel de atacuri devastatoare: atacurile de la Oslo (2011), de la Paris (2015), de la Bruxelles (2016) și de la Manchester (2017). În urma unui atac comis cu ajutorul unui exploziv artizanal la Lyon (2019) au fost rănite 13 persoane.

Urmărirea penală eficace a celor care au comis infracțiuni de terorism, inclusiv a **luptătorilor teroriști străini** aflați în prezent în Siria și în Irak, este, de asemenea, un element important al politicii de combatere a terorismului. Deși aceste aspecte intră în principal în sfera de responsabilitate a statelor membre, coordonarea și sprijinul la nivelul UE pot ajuta statele membre în demersul de abordare a provocărilor comune. Măsurile în curs pentru aplicarea integrală a legislației privind securitatea frontierelor[89] și pentru valorificarea deplină a tuturor bazelor de date relevante ale UE pentru schimbul de informații cu privire la suspecții cunoscuți vor reprezenta un pas important. Pe lângă identificarea persoanelor cu un grad ridicat de risc, este necesară o politică de reintegrare și de reabilitare. Cooperarea interprofesională, inclusiv cu personalul din penitenciare și cu personalul de probațiune, va consolida înțelegerea judiciară a proceselor radicalizării violente, precum și abordarea sectorului judiciar în ceea ce privește pedepsele și alternativele la detenție.

Provocarea reprezentată de luptătorii teroriști străini este emblematică pentru legătura dintre **securitatea** internă și cea **externă.** Cooperarea în materie de combatere a terorismului, precum și prevenirea și combaterea radicalizării și a extremismului violent sunt elemente esențiale ale asigurării securității în interiorul UE[90]. Sunt necesare măsuri suplimentare de dezvoltare a parteneriatelor de combatere a terorismului și a cooperării cu țările din vecinătatea UE și nu numai, pe baza expertizei Rețelei experților UE în materie de combatere a terorismului/securitate. Planul comun de acțiune privind combaterea terorismului în Balcanii de Vest este o referință elocventă pentru acest tip de cooperare specifică. În particular, ar trebui să se depună eforturi pentru a sprijini capacitatea țărilor partenere de a identifica și de a localiza luptătorii teroriști străini. UE va continua, de asemenea, să promoveze cooperarea multilaterală, colaborând cu principalii actori mondiali din acest domeniu, cum ar fi Organizația Națiunilor Unite, NATO, Consiliul Europei, Interpol și OSCE. UE va stabili, de asemenea, contacte cu Forumul mondial pentru combaterea terorismului și cu coaliția internațională pentru contracararea Da'esh, precum și cu actorii relevanți ai societății civile. Instrumentele de politică externă ale Uniunii, inclusiv dezvoltarea și cooperarea, îndeplinesc, de asemenea, un rol important în cooperarea cu țările terțe în vederea prevenirii terorismului și a pirateriei. Cooperarea internațională este, de asemenea, esențială pentru eliminarea tuturor surselor de **finanțare a terorismului**, de exemplu cooperarea în cadrul Grupului de Acțiune Financiară Internațională.

Criminalitatea organizată

Criminalitatea organizată cauzează costuri economice și personale enorme. S-a estimat că pierderea economică ocazionată de criminalitatea organizată și de corupție reprezintă între 218 și 282 de miliarde EUR pe an[91]. În 2017, peste 5 000 de grupuri infracționale organizate au făcut obiectul unei investigații în Europa, ceea ce reprezintă o creștere cu 50 % față de 2013[92]. Criminalitatea organizată își desfășoară tot mai frecvent activitățile la nivel transfrontalier, inclusiv din vecinătatea imediată a UE, ceea ce înseamnă că este necesar să se intensifice cooperarea operațională și schimbul de informații cu partenerii din vecinătate.

---

89 Inclusiv noul mandat al Agenției Europene pentru Poliția de Frontieră și Garda de Coastă (Frontex).

90 Concluziile Consiliului din 16 iunie 2020 au subliniat necesitatea de a proteja cetățenii UE împotriva terorismului și a extremismului violent, indiferent de forma și originea acestora, și de a consolida în continuare angajamentul și acțiunea externe ale UE în materie de combatere a terorismului în anumite zone geografice și domenii tematice prioritare.

91 Ca valoare din produsul intern brut (PIB); raportul Europol: *Does crime still pay? – Criminal asset recovery in the EU*, 2016.

92 Europol, *Serious and Organized Threat Assessments (SOCTA)*, 2013 și 2017.

Apar noi provocări și noi forme de infracțiuni în mediul online: în contextul pandemiei de COVID-19 s-a înregistrat o creștere uriașă a înșelătoriilor în mediul online care vizau grupurile vulnerabile, iar produsele pentru sănătate și produsele sanitare au făcut obiectul furturilor și efracțiilor[93]. UE trebuie să își intensifice eforturile de combatere a criminalității organizate, inclusiv la nivel internațional, cu ajutorul mai multor instrumente de destrămare a modelului de afaceri al criminalității organizate. Combaterea criminalității organizate presupune, de asemenea, cooperarea strânsă cu administrațiile locale și regionale, precum și cu societatea civilă, care sunt parteneri-cheie în prevenirea criminalității, precum și în acordarea de asistență și sprijin victimelor, mai ales cu administrațiile din regiunile de frontieră. Aceste acțiuni vor fi reunite în cadrul unei **agende pentru combaterea criminalității organizate**.

Peste o treime din grupurile infracționale organizate active în UE sunt implicate în producția, traficul sau distribuția de droguri. Dependența de droguri a cauzat moartea prin supradoză a peste opt mii de persoane în UE în 2019. Cea mai mare parte a **traficului de droguri** are loc la nivel transfrontalier, multe dintre profituri ajungând în circuitul economiei legale[94]. Noua agendă a UE privind drogurile[95] va consolida eforturile UE și ale statelor membre în domeniul reducerii cererii și ofertei de droguri, definind acțiuni comune care abordează o problemă comună și consolidând dialogul și cooperarea dintre UE și partenerii săi externi în materie de droguri. În urma unei evaluări a Observatorului European pentru Droguri și Toxicomanie, Comisia va analiza dacă este necesară actualizarea mandatului observatorului, astfel încât să poată să răspundă noilor provocări.

Grupurile infracționale organizate și teroriștii sunt, de asemenea, actori-cheie în comerțul cu **arme de foc ilegale**. În perioada 2009-2018, au avut loc 23 de atacuri armate în masă în Europa, care s-au soldat cu moartea a peste 340 de persoane[96]. Armele de foc fac adesea obiectului traficului în UE din vecinătatea sa imediată[97], ceea ce arată că este necesar să se consolideze coordonarea și cooperarea atât în cadrul UE, cât și cu partenerii internaționali, în special cu Interpol, pentru a armoniza colectarea de informații și raportarea cu privire la confiscările de arme de foc. Este, de asemenea, esențial să se îmbunătățească trasabilitatea armelor de foc, inclusiv pe internet, și să se asigure schimbul de informații între autoritățile de acordare a autorizațiilor și cele de aplicare a legii. Comisia prezintă un nou **plan de acțiune al UE de combatere a traficului cu arme de foc**[98] și va evalua, de asemenea, dacă normele privind autorizațiile de export și măsurile de import și de tranzit pentru armele de foc sunt în continuare adecvate scopului[99].

Organizațiile infracționale tratează migranții și persoanele care au nevoie de protecție internațională ca pe o marfă. Din totalul migranților în situație neregulamentară care sosesc în UE, 90 % au intrat în UE prin intermediul unei rețele infracționale[100]. De asemenea,

---

93 Europol, 2020.

94 OEDT și Europol, *EU Drug Markets Report 2019* (noiembrie 2019).

95 Agenda și Planul de acțiune ale UE în materie de droguri pentru perioada 2021-2025, COM (2020) 606.

96 Flemish Peace Institute, *Armed to kill* (octombrie 2019).

97 UE a finanțat lupta împotriva proliferării și traficului de arme de calibru mic și de armament ușor în regiune începând din 2002; a finanțat în special Rețeaua de experți în materie de arme de foc în Europa de Sud-Est (SEEFEN). Din 2019, partenerii din Balcanii de Vest au fost pe deplin implicați în acțiunea prioritară privind armele de foc a Platformei multidisciplinare europene împotriva amenințărilor infracționale (EMPACT).

98 COM(2020) 608.

99 Regulamentul (UE) nr. 258/2012 privind punerea în aplicare a articolului 10 din Protocolul Organizației Națiunilor Unite împotriva fabricării și traficului ilegale de arme de foc.

100 Sursa: Europol.

introducerea ilegală de migranți este adesea corelată cu alte forme de criminalitate organizată, în special traficul de persoane[101]. Pe lângă costurile umane uriașe ale acestui tip de trafic, Europol estimează că, la nivel mondial, profitul anual generat de toate formele de exploatare a traficului de persoane se ridică la 29,4 miliarde EUR. Traficul de persoane este o infracțiune transnațională alimentată de cererile ilegale din interiorul și din afara UE și afectează toate statele membre ale UE. Rezultatele slabe în ceea ce privește identificarea, urmărirea penală și condamnarea acestor infracțiuni arată că este nevoie de o nouă abordare în vederea intensificării acțiunilor. Noua **abordare cuprinzătoare privind traficul de persoane** va reuni liniile de acțiune. De asemenea, Comisia va prezenta un **nou plan de acțiune al UE de combatere a introducerii ilegale de migranți** pentru perioada 2021-2025. Ambele componente vor pune accentul pe combaterea rețelelor infracționale, stimularea cooperării și sprijinirea activității autorităților de aplicare a legii.

Grupurile infracționale organizate – precum și teroriștii – caută, de asemenea, oportunități în alte domenii, în special în cele care generează profituri ridicate cu un risc de detectare scăzut, de exemplu **infracțiunile ecologice**. Vânătoarea și comerțul ilegal cu specii din fauna sălbatică, exploatarea minieră ilegală, exploatarea forestieră, precum și eliminarea și expedierea ilegală a deșeurilor au devenit a patra cea mai mare activitate infracțională din lume[102]. De asemenea, sistemele de comercializare a certificatelor de emisii și sistemele de certificare a energiei au fost exploatate în scopuri infracționale, iar fondurile alocate rezilienței în materie de mediu și dezvoltării durabile au fost utilizate în mod abuziv. Pe lângă promovarea acțiunii desfășurate de UE, statele membre și comunitatea internațională în vederea intensificării eforturilor de combatere a infracțiunilor ecologice[103], Comisia evaluează dacă Directiva privind infracțiunile ecologice[104] este în continuare adecvată scopului. **Traficul de bunuri culturale**, în creștere, a devenit, de asemenea, una dintre cele mai lucrative activități infracționale, o sursă de finanțare atât pentru teroriști, cât și pentru criminalitatea organizată. Ar trebui analizate modalitățile de îmbunătățire a trasabilității online și offline a bunurilor culturale pe piața internă și a cooperării cu țările terțe în care bunurile culturale fac obiectul jafurilor, precum și posibilitățile de oferire a unui sprijin activ autorităților de aplicare a legii și mediului academic.

Infracțiunile economice și financiare sunt extrem de complexe și afectează în fiecare an milioane de cetățeni și mii de întreprinderi din UE. Combaterea fraudei este esențială și pentru aceasta este necesară acțiunea la nivelul UE. Europol, alături de Eurojust, Parchetul European și Oficiul European de Luptă Antifraudă sprijină statele membre și UE în demersurile lor de protejare a pieței economice și financiare și de protejare a banilor contribuabililor din UE. Parchetul European va deveni pe deplin operațional în 2020 și va cerceta, va urmări penal și va trimite în judecată persoanele învinuite de săvârșirea unor infracțiuni care aduc prejudicii bugetului UE, cum ar fi actele de fraudă, corupție și spălare de bani. Parchetul European va trata, de asemenea, cazurile transfrontaliere de fraudă în materie de TVA, care generează costuri pentru contribuabili de cel puțin 50 de miliarde EUR pe an.

Comisia va sprijini, de asemenea, dezvoltarea expertizei și a unui cadru legislativ în materie de riscuri emergente, cum ar fi criptoactivele și noile sisteme de plată. În particular, Comisia va analiza răspunsul privind apariția criptoactivelor precum bitcoin și efectul acestor noi

[101] Europol, EMSC, Al 4-lea raport anual.
[102] *UNEP-INTERPOL Rapid Response Assessment*: *The Rise of Environmental Crime*, iunie 2016.
[103] A se vedea Pactul verde european, COM (2019) 640 final.
[104] Directiva 2008/99/CE privind protecția mediului prin intermediul dreptului penal.

tehnologii asupra modului în care activele financiare sunt emise, schimbate, partajate și accesate.

Atitudinea în ceea ce privește banii iliciți în Uniunea Europeană ar trebui să fie de zero toleranță. Într-un interval de treizeci de ani, UE a elaborat un cadru de reglementare solid pentru prevenirea și combaterea **spălării banilor** și a finanțării terorismului, cu respectarea deplină a necesității de a proteja datele cu caracter personal. Cu toate acestea, există un consens tot mai larg cu privire la faptul că punerea în aplicare a cadrului actual trebuie îmbunătățită în mod semnificativ. Trebuie abordate divergențele majore în ceea ce privește modul în care cadrul este aplicat și deficiențele grave în punerea în aplicare a normelor. După cum se precizează în detaliu în planul de acțiune din mai 2020[105], sunt în curs de desfășurare activități de evaluare a opțiunilor de consolidare a cadrului UE de combatere a spălării banilor și a finanțării terorismului. Printre domeniile de analizat se numără interconectarea registrelor naționale centralizate de conturi bancare, ceea ce ar putea accelera în mod semnificativ accesul unităților de informații financiare și al autorităților competente la informațiile financiare.

Profiturile grupurilor de criminalitate organizată sunt estimate la 110 miliarde EUR pe an în UE. Răspunsul actual constă în acte legislative armonizate privind confiscarea și recuperarea activelor[106], îmbunătățirea procedurilor de înghețare și de confiscare a activelor provenite din săvârșirea de infracțiuni în UE și facilitarea încrederii reciproce și a unei cooperări transfrontaliere eficiente între statele membre. Cu toate acestea, doar aproximativ 1 % din aceste profituri sunt confiscate[107], ceea ce permite grupurilor de criminalitate organizată să investească în extinderea activităților lor infracționale și să se infiltreze în economia legală, iar întreprinderile mici și mijlocii, care se confruntă cu dificultăți în ceea ce privește accesul la credite, sunt principala țintă a operațiunilor de spălare de bani. Comisia va analiza punerea în aplicare a legislației[108] și eventuala necesitate a unor norme comune suplimentare, inclusiv privind confiscarea care nu se bazează pe o sentință de condamnare. Birourile de recuperare a activelor[109], actori-cheie în procesul de recuperare a activelor, ar putea, de asemenea, să aibă la dispoziție instrumente mai bune de identificare și urmărire mai rapidă a activelor pe întreg teritoriul UE, astfel încât ratele de confiscare să fie mai mari.

Între criminalitatea organizată și **corupție** există o legătură puternică. Conform estimărilor, doar corupția cauzează costuri economiei UE în valoare de 120 de miliarde EUR pe an[110]. Prevenirea și combaterea corupției vor face în continuare obiectul unei monitorizări regulate în cadrul mecanismului privind statul de drept, precum și al semestrului european. Semestrul european a evaluat provocările în lupta împotriva corupției, cum ar fi achizițiile publice, administrația publică, mediul de afaceri sau asistența medicală. Noul raport anual al Comisiei privind statul de drept va trata aspecte legate de combaterea corupției și va facilita un dialog preventiv cu autoritățile naționale și părțile interesate de la nivelul UE și de la

[105] Plan de acțiune privind prevenirea spălării banilor și a finanțării terorismului, C(2020) 2800.

[106] Legislația UE prevede obligația instituirii de birouri de recuperare a activelor în toate statele membre.

[107] Raport intitulat „Recuperarea și confiscarea activelor: Asigurarea faptului că nu este rentabil să se săvârșească infracțiuni”, COM (2020) 217 final.

[108] Directiva 2014/42/UE privind înghețarea și confiscarea instrumentelor și produselor infracțiunilor.

[109] Decizia 2007/845/JAI a Consiliului privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile.

[110] Este dificil de estimat costul economic total al corupției, deși s-au depus eforturi în acest sens, inclusiv de către Camera Internațională de Comerț, *Transparency International*, Pactul mondial al ONU și Forumul Economic Mondial, din care rezultă că corupția reprezintă 5 % din PIB-ul mondial.

nivel național. Organizațiile societății civile pot avea, de asemenea, un rol esențial în stimularea acțiunii autorităților publice de prevenire și combatere a criminalității organizate și a corupției, iar aceste grupuri ar putea fi reunite în mod eficace în cadrul unui forum comun. Având în vedere caracterul transfrontalier al criminalității organizate și al corupției, un alt aspect important este cooperarea și asistența cu privire la aceste chestiuni cu regiunile din vecinătatea UE.

Acțiuni-cheie
• Agenda UE privind combaterea terorismului, inclusiv acțiuni reînnoite de combatere a radicalizării în UE • O nouă cooperare cu țări terțe și organizații internaționale esențiale în lupta împotriva terorismului • Agenda privind combaterea criminalității organizate, inclusiv a traficului de persoane • Agenda UE privind combaterea drogurilor și planul de acțiune pentru 2021-2025 • Evaluarea Observatorului European pentru Droguri și Toxicomanie • Planul de acțiune al UE privind combaterea traficului de arme de foc pentru 2020-2025 • Revizuirea legislației privind înghețarea și confiscarea și privind birourile de recuperare a activelor • Evaluarea Directivei privind infracțiunile ecologice • Planul de acțiune al UE împotriva introducerii ilegale de migranți pentru perioada 2021-2025

4. Un ecosistem european solid în materie de securitate

Pentru crearea unei uniuni a securității autentice și efective, toate părțile societății trebuie să își aducă contribuția. Administrațiile publice, autoritățile de aplicare a legii, sectorul privat, sectorul învățământului și cetățenii înșiși trebuie să fie implicați în acțiunile de consolidare a nivelului de pregătire și reziliență al tuturor categoriilor, în special al celor mai vulnerabile persoane, al victimelor și martorilor, trebuie să dispună de mijloacele necesare și să fie bine conectați pentru a putea participa la aceste acțiuni.

Toate politicile trebuie să țină seama de aspectele legate de securitate, iar UE poate aduce o contribuție la toate nivelurile. În familie, unul dintre cele mai importante riscuri în materie de securitate este violența domestică. În UE, 22 % dintre femei au fost victime ale actelor de violență săvârșite de un partener intim[111]. Aderarea UE la Convenția de la Istanbul privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice rămâne o prioritate-cheie. În cazul în care nu se depășește blocajul la care s-a ajuns în procesul de negociere, Comisia va lua alte măsuri pentru a atinge aceleași obiective similare celor cele prevăzute de convenție și va propune inclusiv adăugarea violenței împotriva femeilor pe lista actelor considerate drept infracțiune în UE, definite în tratat.

Cooperarea și schimbul de informații

Facilitarea bunei cooperări între părțile cu responsabilități în materie de securitate este una dintre cele mai importante contribuții pe care UE le poate aduce la eforturile de protejare a cetățenilor. Cooperarea și schimbul de informații sunt cele mai puternice instrumente de combatere a criminalității și a terorismului și de a îndeplini actul de justiție. Pentru a fi

[111] O Uniune a egalității: Strategia privind egalitatea de gen 2020-2025, COM(2020) 152.

eficiente, aceste demersuri trebuie să fie bine direcționate și oportune. Pentru a beneficia de încredere, trebuie să se prevadă garanții și controale comune cu privire la aceste demersuri.

O serie de instrumente și strategii sectoriale ale UE[112] au fost instituite pentru a dezvolta în continuare **cooperarea operațională în materie de aplicare a legii** dintre statele membre. Unul dintre principalele instrumente ale UE de sprijinire a cooperării în materie de aplicare a legii între statele membre este Sistemul de Informații Schengen, utilizat pentru schimbul de date în timp real cu privire la persoanele și obiectele căutate și dispărute. Rezultatele cooperării au constat în arestarea criminalilor, confiscarea drogurilor și salvarea potențialelor victime[113]. Cu toate acestea, s-ar putea ameliora nivelul cooperării prin raționalizarea și modernizarea instrumentelor disponibile. Cea mai mare parte a cadrului juridic al UE care stă la baza cooperării operaționale în materie de aplicare a legii s-a elaborat în urmă cu 30 de ani. O rețea complexă de acorduri bilaterale între statele membre, multe dintre acestea învechite sau neutilizate pe deplin, creează un risc de fragmentare. În țările mai mici sau în țările fără ieșire la mare, agenții responsabili cu aplicarea legii care își desfășoară activitatea la nivel transfrontalier trebuie să desfășoare acțiuni operaționale respectând, în unele cazuri, până la șapte seturi diferite de norme: consecința este că unele operațiuni, cum ar fi urmărirea peste frontierele interne a persoanelor suspectate, nu au loc. Cooperarea operațională cu privire la noile tehnologii, cum ar fi dronele, nu intră sub incidența cadrului actual al UE.

Eficacitatea operațională poate fi sprijinită de o cooperare specifică în domeniul aplicării legii, care ar putea contribui, de asemenea, la furnizarea unui sprijin esențial pentru alte obiective de politică, cum ar fi furnizarea de informații în materie de securitate pentru noua evaluare a investițiilor străine directe. Comisia va analiza modul în care Codul de cooperare polițienească ar putea contribui la acest demers. Autoritățile de aplicare a legii din statele membre au recurs tot mai frecvent la sprijinul și expertiza de la nivelul UE, în timp ce INTCEN UE a avut un rol important în promovarea schimbului de informații strategice între serviciile de informații și de securitate ale statelor membre, punând la dispoziția instituțiilor UE elementele specifice necesare pentru conștientizarea situației[114]. **Europol** poate îndeplini, de asemenea, un rol esențial în extinderea cooperării sale cu țările terțe pentru a combate criminalitatea și terorismul, în concordanță cu alte politici și instrumente externe ale UE. Cu toate acestea, Europol se confruntă în prezent cu o serie de constrângeri importante – în special în ceea ce privește schimbul direct de date cu caracter personal cu părți private – ceea ce nu îi permite să sprijine în mod eficace statele membre în demersurile de combatere a terorismului și a criminalității. Mandatul Europol este evaluat în prezent pentru a identifica modalitățile de îmbunătățire, astfel încât agenția să își poată îndeplini integral atribuțiile. În acest context, autoritățile relevante de la nivelul UE (de exemplu, OLAF, Europol, Eurojust și Parchetul European) ar trebui, de asemenea, să coopereze mai strâns și să îmbunătățească schimbul de informații.

O altă legătură esențială este dezvoltarea în continuare a **Eurojust** pentru a maximiza sinergia dintre cooperarea în materie de aplicare a legii și cooperarea judiciară. De

[112] De exemplu, Planul de acțiune privind Strategia UE în materie de securitate maritimă, care a contribuit la obținerea de rezultate importante prin cooperarea cu privire la funcțiile de pază de coastă dintre agențiile UE relevante.

[113] Combaterea criminalității organizate la nivelul UE în 2019 (Consiliul, 2020).

[114] INTCEN UE servește drept singurul punct de contact pentru serviciile de informații și de securitate ale statelor membre pentru a furniza UE elementele bazate pe informații necesare pentru conștientizarea situației.

asemenea, o mai mare coerență strategică ar fi, de asemenea, în folosul UE: **EMPACT**[115], ciclul de politici ale UE privind criminalitatea internațională organizată și gravă, oferă autorităților o metodologie în materie penală bazată pe informații care să le permită să abordeze în comun cele mai importante amenințări infracționale care afectează UE. Această platformă a contribuit la obținerea de rezultate operaționale importante[116] în ultimii zece ani. Pentru noul ciclu de politici pentru perioada 2022-2025, mecanismul existent ar trebui să fie raționalizat și simplificat, pe baza experienței practicienilor, pentru a răspunde mai bine amenințărilor infracționale foarte urgente și în continuă evoluție.

Informațiile oportune și relevante sunt esențiale în activitatea zilnică a autorităților de asigurare a aplicării legii. Deși s-au creat noi baze de date la nivelul UE în materie de securitate și gestionare a frontierelor, multe informații sunt stocate încă în bazele de date naționale sau fac obiectul schimbului de informații în afara acestor instrumente. Consecința este un volum de muncă suplimentar semnificativ, întârzieri și un risc mai mare de a nu lua în considerare informații esențiale. Procesele optimizate, accelerate și simplificate, care implică întreaga comunitate din domeniul securității ar aduce rezultate mai bune. Pentru valorificarea potențialului deplin al schimbului de informații în combaterea eficientă a infracționalității, sunt esențiale instrumente adecvate, prevăzute cu garanțiile necesare, astfel încât schimbul de date să respecte legislația în materie de protecție a datelor și drepturile fundamentale. Având în vedere evoluțiile tehnologice, criminalistice și în materie de protecție a datelor, precum și modificarea nevoilor operaționale, UE ar putea lua în considerare necesitatea modernizării unor instrumente precum **Deciziile Prüm din 2008** de instituire de schimburi automate de date privind ADN, de date dactiloscopice și de date privind înmatricularea vehiculelor, astfel încât în sfera schimbului automatizat să poată să intre categorii de date suplimentare care sunt deja disponibile în bazele de date penale sau de alt tip ale statelor membre în scopul anchetelor penale. În plus, Comisia va analiza posibilitatea schimbului de informații privind cazierele judiciare, astfel încât să se poată verifica dacă o persoană are cazier judiciar în alte state membre, și posibilitățile de facilitare a accesului la cazierele judiciare identificate, cu respectarea tuturor garanțiilor necesare.

Informațiile privind călătorii au contribuit la îmbunătățirea controalelor la frontieră, la reducerea migrației neregulamentare și la identificarea persoanelor care prezintă riscuri în materie de securitate. Datele legate de informațiile prealabile referitoare la pasageri sunt datele biografice ale fiecărui pasager colectate de transportatorii aerieni în cursul procedurii de înregistrare a pasagerilor și transmise în prealabil autorităților de supraveghere a frontierelor din țara de destinație. Revizuirea cadrului juridic[117] ar putea contribui la utilizarea mai eficace a informațiilor, asigurând în același timp respectarea legislației în materie de protecție a datelor și înlesnind fluxurile de pasageri. Registrul cu numele pasagerilor (PNR) reprezintă datele furnizate de pasageri în momentul rezervării zborurilor. Punerea în aplicare a Directivei privind PNR[118] este esențială, iar Comisia va continua să sprijine și să asigure aplicarea acesteia. De asemenea, ca acțiune la jumătatea perioadei, Comisia va lansa o revizuire a abordării actuale privind **transferul de date PNR în țări terțe**.

---

[115] EMPACT este abrevierea pentru European Multidisciplinary Platform Against Criminal Threats (Platforma multidisciplinară europeană împotriva amenințărilor infracționale).

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

[117] Directiva 2004/82/CE a Consiliului privind obligația operatorilor de transport de a comunica datele privind pasagerii.

[118] Directiva (UE) 2016/681 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave.

Cooperarea judiciară trebuie să completeze eforturile de combatere a criminalității transfrontaliere depuse de forțele de poliție. În ultimii 20 de ani, cooperarea judiciară a cunoscut o profundă transformare. Organisme precum **Parchetul European** și **Eurojust** trebuie să dispună de mijloacele necesare pentru a funcționa la capacitate deplină sau pentru a fi consolidate. Cooperarea dintre practicienii din domeniul judiciar ar putea fi, de asemenea, consolidată, prin intermediul unor măsuri suplimentare privind recunoașterea reciprocă a hotărârilor judecătorești, formarea judiciară și schimbul de informații. Obiectivul ar trebui să fie creșterea încrederii reciproce în rândul judecătorilor și procurorilor, element esențial al unor proceduri transfrontaliere armonioase. Utilizarea **tehnologiilor digitale** poate, de asemenea, să îmbunătățească eficiența sistemelor noastre de justiție. Este în curs de instituire un nou sistem de schimb digital pentru transmiterea ordinelor europene de anchetă, a cererilor de asistență judiciară reciprocă și a comunicărilor aferente între statele membre, cu sprijinul Eurojust. Comisia va colabora cu statele membre pentru a accelera introducerea sistemelor informatice necesare la nivel național.

Cooperarea internațională este, de asemenea, esențială pentru eficiența aplicării legii și a cooperării judiciare. Acordurile bilaterale cu parteneri-cheie au un rol fundamental în obținerea de informații și probe din afara UE. **Interpol**, una dintre cele mai mari organizații interguvernamentale de poliție judiciară, îndeplinește un rol important. Comisia va analiza posibilitățile de consolidare a cooperării cu Interpol, inclusiv posibilitatea de a avea acces la bazele de date ale Interpol și întărirea cooperării operaționale și strategice. Autoritățile de aplicare a legii din UE se bazează, de asemenea, pe principalele țări partenere pentru a detecta și a ancheta infractorii și teroriștii. **Parteneriatele în materie de securitate dintre UE și țări terțe** ar putea fi intensificate pentru a spori cooperarea în vederea combaterii amenințărilor comune, ca de exemplu, terorismul, criminalitatea organizată, criminalitatea informatică, abuzurile sexuale asupra copiilor și traficul de persoane. O astfel de abordare ar avea ca temei interese comune în materie de securitate și s-ar baza pe dialogurile stabilite în materie de cooperare și securitate.

Pe lângă schimbul de informații, schimbul de expertiză poate avea o valoare deosebită în creșterea gradului de pregătire a autorităților de aplicare a legii în ceea ce privește **amenințările netradiționale**. Pe lângă încurajarea schimburilor de bune practici, Comisia va analiza posibilitatea creării unui **mecanism de coordonare la nivelul UE a forțelor de poliție** în caz de evenimente de forță majoră, cum ar fi pandemiile. Pandemia a dovedit, de asemenea, că poliția de proximitate adaptată mediului online, însoțită de cadre juridice de facilitare a activităților de ordin polițienesc în mediul online, va fi fundamentală pentru combaterea criminalității și a terorismului. Parteneriatele dintre forțele de poliție și comunități, atât în mediul offline, cât și online pot preveni infracțiunile și atenua impactul criminalității organizate, al radicalizării și al activităților teroriste. Corelarea soluțiilor polițienești de la nivel local, regional, național și european este un factor-cheie al succesului Strategiei UE privind o uniune a securității în ansamblu.

Contribuția unor frontiere externe solide

Gestionarea modernă și eficientă a frontierelor externe are un dublu avantaj: menținerea integrității spațiului Schengen și garantarea securității cetățenilor noștri. Implicarea tuturor actorilor relevanți pentru a pune un accent mai mare pe securitatea la frontiere poate avea un impact real asupra prevenirii criminalității transfrontaliere și a terorismului. Activitățile operaționale comune ale poliției de frontieră și gărzii de coastă la nivel european recent

consolidate[119] contribuie la prevenirea și depistarea criminalității transfrontaliere la **frontierele externe** și în afara UE. Activitățile vamale de detectare a riscurilor de siguranță și securitate aferente tuturor bunurilor înainte de intrarea acestora în UE și de control al bunurilor la intrare sunt esențiale pentru combaterea criminalității transfrontaliere și a terorismului. Viitorul plan de acțiune privind uniunea vamală va anunța, de asemenea, acțiuni de consolidare a managementului riscurilor și a securității interne, inclusiv, în special, prin evaluarea fezabilității unei legături între sistemele de informații relevante pentru analiza riscurilor în materie de securitate.

Cadrul pentru **interoperabilitatea între sistemele de informații ale UE** în domeniul justiției și afacerilor interne a fost adoptat în mai 2019. Scopul acestei noi arhitecturi este ameliorarea eficienței și a eficacității sistemelor de informații noi sau modernizate[120]. Noua arhitectură va pune mai rapid și mai sistematic informații la dispoziția personalului responsabil cu aplicarea legii, polițiștilor de frontieră și funcționarilor din domeniul migrației. Va contribui la identificarea corectă și la combaterea fraudei de identitate. Pentru a transpune în practică aceste măsuri, punerea în aplicare a cadrului pentru interoperabilitate ar trebui să fie o prioritate, atât la nivel politic, cât și la nivel tehnic. Cooperarea strânsă dintre agențiile UE și toate statele membre va fi esențială pentru atingerea până în 2023 a obiectivului de interoperabilitate deplină.

Fraudarea documentelor de călătorie este considerată una dintre infracțiunile săvârșite cel mai frecvent. Această infracțiune facilitează circulația clandestină a infractorilor și a teroriștilor și are un rol esențial în traficul de persoane și în comerțul de droguri[121]. Comisia va analiza modalitățile de extindere a sferei activității existente cu privire la standardele de securitate ale documentelor de călătorie și de ședere ale UE, inclusiv prin digitalizare. Începând din august 2021, statele membre vor începe să elibereze cărți de identitate și documente de ședere conforme cu standardele de securitate armonizate, care includ un cip care conține elemente biometrice de identificare, care pot fi verificate de toate autoritățile de frontieră ale UE. Comisia va monitoriza punerea în aplicare a acestor noi norme, inclusiv înlocuirea treptată a documentelor aflate în prezent în circulație.

Consolidarea cercetării și inovării în domeniul securității

Activitatea de asigurare a securității cibernetice și de combatere a criminalității organizate, a criminalității informatice și a terorismului se bazează în mare măsură pe dezvoltarea de instrumente pentru viitor, care să contribuie la crearea de noi tehnologii mai sigure, să abordeze provocările generate de tehnologii și să sprijine activitatea de aplicare a legii. Acest demers depinde la rândul său de partenerii și industriile private.

Inovarea ar trebui privită ca un instrument strategic de contracarare a amenințărilor actuale și de anticipare atât a riscurilor, cât și a oportunităților viitoare. Inovațiile tehnologice pot contribui la crearea de noi instrumente care să vină în sprijinul autorităților de aplicare a legii și a altor actori din domeniul securității. Inteligența artificială și analiza volumelor mari de date ar putea valorifica tehnica de calcul de înaltă performanță pentru o mai bună

[119] Cuprinde Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex) și autoritățile care asigură poliția de frontieră și garda de coastă ale statelor membre.

[120] Sistemul de intrare/ieșire (EES), Sistemul european de informații și de autorizare privind călătoriile (ETIAS), Sistemul european extins de informații cu privire la cazierele judiciare (ECRIS-TCN), Sistemul de informații Schengen, Sistemul de informații privind vizele și viitoarea versiune actualizată a Eurodac.

[121] Legătura dintre fraudarea documentelor și traficul de persoane este prezentată în Al doilea raport privind progresele înregistrate cu privire la combaterea traficului de persoane, COM(2018) 777 și în documentul de însoțire SWD(2018) 473, precum și în raportul Europol din 2016, *Situation Report Trafficking in human beings in the EU*.

detectare și o analiză cuprinzătoare rapidă[122]. O condiție prealabilă esențială pentru dezvoltarea de tehnologii fiabile o reprezintă seturile de date de înaltă calitate, la care pot să recurgă autoritățile competente pentru a forma, testa și valida algoritmi[123]. În general, riscul de dependență tehnologică este în prezent ridicat – UE este, de exemplu, un importator net de produse și servicii de securitate cibernetică, cu toate implicațiile pe care acest fapt le are pentru economie și infrastructurile critice. Pentru a stăpâni tehnologia și pentru a garanta continuitatea aprovizionării și în caz de evenimente adverse și de crize, Europa trebuie să asigure prezența și capacitatea în părțile critice ale lanțurilor valorice relevante.

Pe măsură ce aceste tehnologii sunt dezvoltate și aplicate, **cercetarea, inovarea și dezvoltarea tehnologică** a UE oferă posibilitatea de a lua în considerare aspectele legate de securitate. Următoarea generație de propuneri de finanțare ale UE poate acționa ca un stimul important[124]. Inițiativele privind spațiile de date și infrastructurile *cloud* europene integrează aspectele legate de securitate încă de la început. Centrul european de competențe industriale, tehnologice și de cercetare industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare[125] au scopul de a institui o structură eficace și eficientă pentru a reuni și a face schimb de capacități și rezultate în domeniul cercetării în materie de securitate cibernetică. Programul spațial al UE furnizează servicii care vin în sprijinul securității UE, a statelor sale membre și a persoanelor fizice[126].

Cu peste 600 de proiecte lansate începând din 2007 în valoare totală de aproape 3 miliarde EUR, cercetarea în domeniul securității finanțată de UE este un instrument-cheie pentru stimularea tehnologiei și a cunoștințelor care sprijină soluțiile de securitate. Cu ocazia revizuirii mandatului Europol, Comisia va analiza oportunitatea creării **unui centru european de inovare pentru securitatea internă**[127], care să aibă scopul de a propune soluții comune la provocările și oportunitățile comune în materie de securitate, pe care statele membre nu le-ar putea exploata în mod individual. Cooperarea este fundamentală pentru direcționarea optimă a investițiilor și pentru dezvoltarea de inovații tehnologice care sunt atât în folosul securității, cât și al economiei.

Competențe și acțiuni de sensibilizare

Luarea la cunoștință a problemelor de securitate și dobândirea competențelor pentru a face față amenințărilor potențiale sunt esențiale pentru crearea unei societăți mai reziliente, în care întreprinderile, administrațiile și persoanele fizice sunt mai bine pregătite. Provocările legate de infrastructura informatică și de sistemele electronice au evidențiat necesitatea de a ne ameliora capitalul uman în materie de pregătire și de răspuns în domeniul securității

[122] Punctul de plecare ar trebui să fie Strategia Comisiei privind inteligența artificială.

[123] O strategie europeană privind datele, COM (2020) 66 final.

[124] Propunerile Comisiei privind programul Orizont Europa, Fondul pentru securitate internă, Fondul de gestionare integrată a frontierelor, programul EUInvest, Fondul european de dezvoltare regională și programul Europa digitală vor sprijini dezvoltarea și introducerea de tehnologii și soluții inovatoare în domeniul securității în lanțul valoric al securității.

[125] Propunerea din 12 septembrie 2018 de instituire a Centrului european de competențe industriale, tehnologice și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare, COM(2018) 630.

[126] De exemplu, programul Copernicus oferă servicii care permit supravegherea frontierelor externe ale UE și supravegherea maritimă, contribuind la acțiunile de combatere a pirateriei și a introducerii ilegale de migranți, precum și sprijinind infrastructurile critice. De îndată ce va fi pe deplin operațional, acest program va fi un important factor de facilitare a misiunilor și operațiilor civile și militare.

[127] Centrul ar colabora, de asemenea, cu Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (Frontex), CEPOL, eu-LISA și Centrul Comun de Cercetare.

cibernetice. Pandemia a evidențiat, de asemenea, importanța digitalizării în toate domeniile economiei și societății UE.

Chiar și **cunoștințele de bază privind amenințările la adresa securității** și modul de combatere a acestora pot avea un impact real asupra rezilienței societății. Conștientizarea riscurilor pe care le reprezintă criminalitatea informatică și necesitatea de autoprotecție împotriva acesteia pot acționa în sinergie cu protecția oferită de furnizorii de servicii pentru a contracara atacurile cibernetice. Informațiile cu privire la pericolele și riscurile pe care le reprezintă traficul de droguri pot îngreuna reușita acțiunilor comise de infractori. UE poate stimula diseminarea celor mai bune practici, de exemplu prin intermediul rețelei de centre pentru un internet mai sigur[128] și se poate asigura că aceste obiective sunt integrate în propriile programe.

Viitorul Plan de acțiune pentru educația digitală ar trebui să includă măsuri specifice menite să asigure consolidarea competențelor în materie de securitate informatică ale întregii populații. Agenda pentru competențe adoptată recent[129] sprijină consolidarea competențelor pe tot parcursul vieții. Agenda prevede acțiuni specifice pentru creșterea numărului de absolvenți în domeniile științei, tehnologiei, ingineriei, artelor și matematicii, necesare în domenii de vârf, cum ar fi securitatea cibernetică. Acțiunile suplimentare, finanțate prin programul Europa digitală, vor permite profesioniștilor să țină pasul cu evoluțiile în materie de amenințări la adresa securității și, în același timp, vor contribui la eliminarea deficitului din acest domeniu pe piața forței de muncă din UE. Obiectivul general urmărit va fi dobândirea de către cetățeni a competențelor pentru a face față amenințărilor la adresa securității și posibilitatea de identificare de către întreprinderi a profesioniștilor de care au nevoie în acest domeniu. Viitorul spațiu european de cercetare și viitorul spațiu european al educației vor promova, de asemenea, carierele în știință, tehnologie, inginerie, arte și matematică.

Este, de asemenea, important ca **victimele** să poată să exercite accesul la drepturile lor; victimele trebuie să primească asistența și sprijinul de care au nevoie, în funcție de circumstanțele specifice ale situației lor. Sunt necesare eforturi speciale atunci când este vorba de minorități și de cele mai vulnerabile victime, ca de exemplu copiii sau femeile care au fost traficate în scopul exploatării sexuale sau care sunt expuse violenței domestice[130].

Competențele consolidate **în materie de aplicare a legii** au un rol special. Amenințările tehnologice curente și viitoare fac necesară intensificarea investițiilor în perfecționarea personalului din domeniul aplicării legii, într-o etapă cât mai incipientă și de-a lungul întregii lor cariere. CEPOL este un partener esențial care poate să asiste statele membre în acest demers. Formarea autorităților de aplicare a legii cu privire la aspectele legate de rasism și xenofobie, precum și cu privire la drepturile cetățenilor în general, trebuie să constituie o componentă esențială a unei culturi a securității în UE. Sistemele naționale de justiție și practicienii din domeniul justiției trebuie, de asemenea, să fie pregătiți să se adapteze și să răspundă la provocări fără precedent. Programele de formare sunt esențiale pentru a permite autorităților de pe teren să valorifice aceste instrumente într-o situație

[128] A se vedea www.betterinternetforkids.eu: în prezent, portalul central și centrele naționale pentru un internet mai sigur sunt finanțate în temeiul MIE/Telecomunicații, iar în viitor se propune asigurarea finanțării în cadrul programului Europa digitală.

[129] Agenda pentru competențe în Europa în vederea obținerii unei competitivități durabile, a echității sociale și a rezilienței, COM (2020) 274 final.

[130] A se vedea Strategia privind egalitatea de gen, COM (2020) 152; Strategia privind drepturile victimelor, COM (2020) 258 și Strategia europeană pentru un internet mai bun pentru copii, COM(2012) 196.

operațională. De asemenea, ar trebui să se depună toate eforturile pentru a consolida integrarea aspectelor legate de gen și a consolida participarea femeilor la aplicarea legii.

Acțiuni-cheie
• Consolidarea mandatului Europol • Analizarea oportunității unui „Cod de cooperare polițienească” al UE și a coordonării polițienești în perioade de criză • Consolidarea Eurojust pentru a crea o legătură între autoritățile judiciare și autoritățile de aplicare a legii • Revizuirea Directivei privind informațiile prealabile referitoare la pasageri • Comunicarea privind dimensiunea externă a registrelor cu numele pasagerilor • Consolidarea cooperării dintre UE și Interpol • Un cadru de negociere cu principalele țări terțe cu privire la schimbul de informații • Standarde de securitate mai bune pentru documentele de călătorie • Analizarea oportunității unui centru european de inovare pentru securitatea internă

V. Concluzii

Într-o lume tot mai frământată, Uniunea Europeană este considerată în mare măsură unul dintre cele mai sigure locuri. Însă, acest lucru nu poate fi considerat ca fiind de la sine înțeles.

Noua strategie privind uniunea securității pune bazele unui ecosistem în materie de securitate care acoperă întreaga societate europeană. Noua strategie pleacă de la premisa că securitatea este o responsabilitate comună. Securitatea este o problemă care afectează pe toată lumea. Pentru ca societățile să fie mai sigure, toate organele guvernamentale, întreprinderile, organizațiile sociale, instituțiile și cetățenii trebuie să își îndeplinească responsabilitățile care le revin.

Aspectele legate de securitate trebuie acum privite dintr-o perspectivă mult mai amplă decât în trecut. Distincțiile artificiale între dimensiunea fizică și cea digitală trebuie depășite. Strategia UE privind uniunea securității reunește întreaga gamă de nevoi în materie de securitate și pune accentul pe domeniile cele mai critice pentru securitatea UE în anii următori. Strategia recunoaște, de asemenea, faptul că amenințările la adresa securității nu se limitează la frontierele geografice, precum și interdependența tot mai mare dintre securitatea internă și cea externă[131]. În acest context, va fi important ca UE să coopereze cu partenerii internaționali pentru protejarea tuturor cetățenilor UE și să asigure în continuare coordonarea strânsă cu acțiunea externă a UE în punerea în aplicare a acestei strategii.

Securitatea noastră este corelată cu valorile noastre fundamentale. Toate acțiunile și inițiativele propuse în această strategie vor respecta pe deplin drepturile fundamentale și valorile noastre europene. Aceste drepturi și valori sunt temelia modului nostru de viață european și trebuie să fie în centrul tuturor acțiunilor noastre.

În fine, Comisia este pe deplin conștientă de faptul că orice politică sau acțiune este utilă doar în măsura aplicării sale. Prin urmare, este necesar să se pună necontenit accentul pe punerea în aplicare corespunzătoare a legislației existente și viitoare și pe asigurarea respectării acesteia. Acest lucru va fi monitorizat prin rapoarte periodice privind uniunea securității, iar Comisia va informa pe deplin Parlamentul European, Consiliul și părțile

[131] A se vedea Strategia globală a UE

interesate și le va implica în toate acțiunile relevante. De asemenea, Comisia este pregătită să participe la dezbateri comune cu instituțiile referitoare la strategia privind uniunea securității și să organizeze astfel de dezbateri, pentru a evalua împreună progresele realizate și a avea în vedere provocările viitoare.

Comisia invită Parlamentul European și Consiliul să aprobe prezenta strategie a uniunii securității ca bază a cooperării și a acțiunii comune privind securitatea în următorii cinci ani.