COMISIA
EUROPEANĂ

Bruxelles, 30.10.2019
COM(2019) 552 final

COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIUL EUROPEAN ȘI CONSILIU

Al douăzecilea raport privind progresele înregistrate către o Uniune a securității efectivă și autentică

I. INTRODUCERE

Prezentul document este cel de al douăzecilea raport privind progresele înregistrate către o Uniune a securității efectivă și autentică. Raportul prezintă evoluțiile înregistrate în domeniul a doi piloni principali: combaterea terorismului și a criminalității organizate, precum și a mijloacelor care le susțin și consolidarea mijloacelor noastre de apărare și a rezilienței împotriva acestor amenințări.

Securitatea a fost o prioritate absolută pentru Comisia Juncker încă din prima zi a mandatului său. Pe baza Agendei europene privind securitatea[1] din aprilie 2015 și a Comunicării din aprilie 2016 care a deschis calea către o Uniune a securității efectivă și autentică[2], UE a răspuns în mod coordonat la o serie de atacuri teroriste și la alte provocări din ce în ce mai mari în materie de securitate, realizând progrese semnificative în ceea ce privește întărirea securității noastre colective.[3] A devenit din ce în ce mai clar că provocările actuale în materie de securitate – fie că este vorba despre terorism, criminalitate organizată, atacuri cibernetice, dezinformare sau alte amenințări cibernetice aflate în permanentă evoluție – constituie amenințări comune. Numai acționând împreună vom putea atinge nivelul de securitate colectivă pe care cetățenii noștri îl cer și îl așteaptă în mod legitim. Această concepție comună a stat la baza progreselor înregistrate către o Uniune a securității efectivă și autentică. Având în vedere nevoile autorităților naționale însărcinate cu asigurarea siguranței cetățenilor, sprijinul la nivelul UE s-a concentrat pe măsuri legislative și operaționale în cazul cărora acțiunea comună poate avea un impact asupra securității statelor membre. Aceste acțiuni au fost desfășurate în strânsă colaborare cu Parlamentul European și cu Consiliul și în deplină transparență față de publicul larg. Respectarea deplină a drepturilor fundamentale s-a aflat în centrul acestei activități, întrucât securitatea Uniunii poate fi asigurată numai atunci când cetățenii sunt convinși că drepturile lor fundamentale sunt pe deplin respectate.

UE a depus eforturi pentru a **combate terorismul** prin închiderea spațiului în care teroriștii își desfășoară activitatea, cu noi norme care le îngreunează acestora accesul la explozivi, arme de foc și finanțare, precum și prin restricționarea circulației acestora. UE a intensificat **schimbul de informații** pentru a le oferi persoanelor aflate în prima linie, ofițerilor de poliție și polițiștilor de frontieră, un acces eficient la date exacte și complete, utilizând în mod optim informațiile existente și eliminând lacunele și unghiurile moarte. Protecția solidă a frontierelor externe este o condiție prealabilă pentru garantarea securității în zona de liberă circulație fără controale la frontierele interne. În martie 2019, Parlamentul European și Consiliu au ajuns la un acord cu privire la o **Poliție de frontieră și o Gardă de coastă la nivel european** consolidate în continuare și complet echipate, iar noul regulament este preconizat să intre în vigoare la începutul lunii decembrie 2019. UE a oferit o platformă și finanțare pentru cei care lucrează în comunitățile locale pentru a face schimb de cele mai bune practici privind **combaterea radicalizării și prevenirea extremismului violent**, precum și pentru a propune noi norme care să elimine în mod eficace conținutul terorist online. Sprijinul UE a contribuit la **o mai mare reziliență a orașelor** împotriva atacurilor, prin planuri de acțiune menite să sprijine protejarea spațiilor publice și să sporească gradul de pregătire împotriva riscurilor de securitate chimică, biologică, radiologică și nucleară. UE a abordat **securitatea cibernetică și amenințările facilitate de tehnologiile informatice** prin punerea în aplicare a unei noi

[1] COM(2015) 185 final (28.4.2015).
[2] COM(2016) 230 final (20.4.2016).
[3] Pentru rapoartele anterioare privind progresele înregistrate către o Uniune a securității efectivă și autentică, a se vedea: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

strategii a UE în materie de securitate cibernetică și prin adoptarea legislației relevante, precum și prin combaterea **dezinformării** pentru a proteja mai bine alegerile noastre. Activitatea derulată continuă să consolideze securitatea **infrastructurii noastre digitale de importanță critică**, inclusiv cooperarea consolidată privind **securitatea cibernetică a rețelelor 5G** în întreaga Europă.

Mai sunt încă multe de făcut. Atacul transmis în direct împotriva unei sinagogi și uciderea a doi cetățeni în Halle, Germania, la 9 octombrie 2019 au constituit un memento șocant al amenințării reprezentate de extremismul violent de dreapta și de antisemitism. De asemenea, acestea au evidențiat încă o dată utilizarea abuzivă a internetului pentru propaganda teroristă și, prin urmare, **necesitatea unor norme la nivelul UE pentru eliminarea conținutului online cu caracter terorist**. Consiliul Justiție și Afaceri Interne din 7-8 octombrie 2019 a dezbătut extremismul violent de dreapta și terorismul, subliniind necesitatea continuării acțiunilor, inclusiv cu privire la combaterea răspândirii, online și offline, a conținutului extremist de dreapta ilegal. În același timp, uciderea a trei ofițeri de poliție și a unui alt membru al personalului în sediul poliției din Paris, la 3 octombrie 2019, arată că amenințarea reprezentată de terorismul jihadist rămâne în continuare una reală și că eforturile depuse în prezent pentru a sprijini statele membre în abordarea acestei amenințări trebuie să continue. Evadarea membrilor ISIS/Daesh aflați în închisoare în contextul evenimentelor recente din nordul Siriei ar putea avea un impact grav asupra securității în Europa. Este important ca statele membre să utilizeze pe deplin sistemele de informații existente pentru a detecta și a identifica luptătorii teroriști străini la trecerea frontierelor externe. De asemenea, se lucrează la utilizarea informațiilor din teatrele de luptă pentru urmărirea luptătorilor teroriști străini.

Prezentul raport prezintă progresele recente înregistrate către o Uniune a securității efectivă și autentică, evidențiind domeniile în care sunt necesare acțiuni suplimentare. Acesta oferă informații actualizate cu privire la punerea în aplicare a măsurilor convenite în materie de **securitate cibernetică a rețelelor 5G**, în special în referitor la **Raportul de evaluare a riscurilor al UE** care a fost publicat la 9 octombrie 2019, precum și cu privire la **combaterea dezinformării**.

Prezentul raport se concentrează în special asupra **dimensiunii externe** a cooperării în Uniunea securității, odată cu semnarea a două **acorduri** bilaterale **de combatere a terorismului** cu Albania și Republica Macedonia de Nord și cu progresele înregistrate în cooperarea cu țările terțe partenere în ceea ce privește schimbul de **date din registrul cu numele pasagerilor.** În plus, împreună cu prezentul raport, Comisia a adoptat o cerere de autorizare pentru lansarea negocierilor pentru un acord între UE și **Noua Zeelandă** cu privire la schimbul de date cu caracter personal pentru combaterea formelor grave de criminalitate și a terorismului.

II. PROGRESELE ÎNREGISTRATE ÎN CEEA CE PRIVEȘTE PRIORITĂȚILE LEGISLATIVE

1. Prevenirea radicalizării online și în comunități

Prevenirea radicalizării constituie o piatră de temelie a răspunsului Uniunii la amenințările terorismului. În această privință, internetul a fost cel mai important câmp de luptă pe care s-au desfășurat acțiunile teroriștilor în secolul XXI. Spațiile în care persoanele radicalizate pot să comunice și să facă schimb de conținut permit dezvoltarea la nivel mondial a unor rețele din ce în ce mai extinse, atât ale jihadiștilor, cât și ale extremiștilor violenți de dreapta. Acesta este motivul pentru care Comisia își continuă abordarea pe două planuri împotriva

radicalizării online, în care normele propuse privind eliminarea conținutului online ilegal cu caracter terorist ar trebui să consolideze parteneriatul voluntar cu platformele online.

Esențială în acest sens este **propunerea legislativă de prevenire a diseminării conținutului online cu caracter terorist**, cu norme și garanții clare care ar impune obligația ca platformele de internet să elimine conținutul cu caracter terorist în termen de o oră de la primirea unei cereri motivate din partea autorităților competente și să ia măsuri proactive proporționale cu nivelul de expunere la conținutul cu caracter terorist.[4] Negocierile interinstituționale sunt în curs de desfășurare între Parlamentul European și Consiliu, un prim trilog având loc la 17 octombrie 2019. Având în vedere amenințarea reprezentată de conținutul online cu caracter terorist, Comisia invită colegiuitorii să ajungă la un acord cu privire la legislația propusă până la sfârșitul anului 2019.

Legislația propusă completează parteneriatul voluntar cu industria internetului și cu alte părți interesate care are loc în cadrul **Forumului UE pentru internet**. De la crearea sa în 2015, forumul a fost un catalizator pentru ca întreprinderile furnizoare de servicii de internet să acționeze în mod proactiv pentru a identifica și a elimina conținutul online cu caracter terorist, deschizând calea pentru inițiativa propusă de industrie cu privire la o „bază de date comună a distribuirilor”[5] și crearea Forumului mondial pentru internet pentru combaterea terorismului. Unitatea UE de semnalare a conținutului online, care face parte din agenția UE de aplicare a legii, Europol, a avut un rol esențial în consolidarea cooperării cu companiile de internet și în realizarea obiectivelor generale ale Forumului UE pentru internet. În cadrul ultimei reuniuni ministeriale a Forumului UE pentru internet din 7 octombrie 2019, statele membre ale UE și reprezentanții de rang înalt ai societăților de internet s-au angajat să colaboreze în cadrul așa-numitului **Protocol UE privind situațiile de criză**. Protocolul UE privind situațiile de criză identifică praguri pentru cooperarea consolidată și stabilește noi modalități de îmbunătățire a răspunsului la situațiile de criză. Acesta face parte din eforturile depuse la nivel internațional pentru punerea în aplicare a „Apelului la acțiune în urma atentatului de la Christchurch”[6], urmărind să asigure o reacție coordonată și rapidă pentru a limita răspândirea conținutului online cu caracter terorist sau a celui extremist violent.

Pe lângă aceste măsuri împotriva radicalizării online, Comisia continuă să sprijine eforturile depuse la nivel național și local pentru **a preveni și a combate radicalizarea pe teren.** Pe baza experienței bogate și a expertizei acumulate în cadrul Rețelei pentru sensibilizarea publicului cu privire la radicalizare, UE oferă sprijin specific actorilor locali, inclusiv orașelor[7], și oferă oportunități de schimburi între practicieni, cercetători și factorii de decizie politică. De exemplu, rețeaua a elaborat orientări specifice și a organizat ateliere pentru a sprijini autoritățile competente în abordarea copiilor proveniți din zone de conflict.[8] Pentru a asigura continuitatea activităților desfășurate în cadrul Rețelei pentru sensibilizarea publicului

---

4 COM(2018) 640 final (12.9.2018).

5 Un instrument instituit de un consorțiu de întreprinderi pentru a facilita cooperarea astfel încât să se prevină diseminarea conținutului cu caracter terorist pe mai multe platforme.

6 Ca răspuns la atacurile comise în Christchurch, Noua Zeelandă la 15 martie 2019, președintele Franței, Emmanuel Macron, și prim-ministrul Noii Zeelande, Jacinda Ardern, au invitat liderii și platformele online la Paris, la 15 mai 2019, pentru a lansa „Apelul la acțiune în urma atentatului de la Christchurch”. Președintele Juncker a sprijinit apelul și a anunțat elaborarea unui protocol al UE privind situațiile de criză.

7 În ceea ce privește cooperarea cu orașele în materie de securitate, a se vedea, de asemenea, secțiunea V.2 privind gradul de pregătire și de protecție, în special referitor la protecția spațiilor publice.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

cu privire la radicalizare, Comisia a lansat procedura pentru un nou contract-cadru cu o valoare estimată de 61 de milioane EUR pe o perioadă de patru ani, începând din 2020.[9]

Pentru a contracara amenințarea reprezentată de conținutul online cu caracter terorist, Comisia invită Parlamentul European și Consiliul:

- să încheie, înainte de sfârșitul anului, negocierile privind propunerea legislativă de prevenire a diseminării **conținutului online cu caracter terorist**.

2. *Sisteme de informații mai puternice și mai inteligente pentru asigurarea securității și gestionarea frontierelor și a migrației*

UE a intensificat schimbul de informații, facilitând combaterea fraudei de identitate[10], consolidând verificările la frontiere[11], modernizând bazele de date de aplicare a legii la nivel european[12], eliminând lacunele în materie de informații[13] și consolidând agenția UE de aplicare a legii, Europol[14]. Elementul central în acest sens îl reprezintă **interoperabilitatea sistemelor de informații ale UE**[15], ceea ce înseamnă utilizarea optimă a informațiilor existente și eliminarea unghiurilor moarte. Răspunzând nevoilor celor care lucrează în prima linie, interoperabilitatea va conduce la un acces mai rapid și mai sistematic la informații

9 Contractul-cadru este împărțit în două loturi: 29 000 000 EUR pentru sprijinirea activităților Rețelei pentru sensibilizarea publicului cu privire la radicalizare pentru următorii patru ani și 32 000 000 EUR pentru consolidarea capacităților statelor membre, ale autorităților naționale, regionale și locale și ale țărilor terțe prioritare în ceea ce privește combaterea eficace a radicalizării, în special prin oferirea de oportunități de colaborare în rețea, de servicii specifice și orientate către nevoi și prin cercetare și analiză.

10 Regulamentul (UE) 2019/1157 (20.6.2019) privind consolidarea securității cărților de identitate ale cetățenilor Uniunii și a documentelor de ședere eliberate cetățenilor Uniunii și membrilor de familie ai acestora care își exercită dreptul la liberă circulație.

11 Introducerea controalelor sistematice efectuate la frontierele externe asupra tuturor cetățenilor care folosesc Sistemul de Informații Schengen. Toate statele Schengen, precum și România, Bulgaria, Croația și Cipru aplică normele privind verificările sistematice prin consultarea bazelor de date relevante la frontierele externe, astfel cum au fost introduse în aprilie 2017. În conformitate cu aceste norme, sunt posibile derogări temporare la frontierele terestre sau maritime, dar numai în ceea ce privește cetățenii UE, având în vedere impactul disproporționat asupra fluidității traficului. În prezent, astfel de derogări au fost notificate de șase state membre/țări asociate spațiului Schengen (Croația, Finlanda, Ungaria, Letonia, Norvegia și Slovenia). În ceea ce privește frontierele aeriene, posibilitatea de derogare de la normele privind controalele sistematice a expirat în aprilie 2019.

12 Sistemul consolidat de Informații Schengen [Regulamentul (UE) 2018/1860 (28.11.2018), Regulamentul (UE) 2018/1861 (28.11.2018), Regulamentul (UE) 2018/1862 (28.11.2018)] și Sistemul european de informații cu privire la cazierele judiciare extinse la resortisanții țărilor terțe [Regulamentul (UE) 2019/816 (17.4.2019)]. Consolidarea Sistemului de Informații Schengen include o obligație generală de introducere în sistem a alertelor legate de terorism.

13 Sistemul de intrare/ieșire al UE [Regulamentul (UE) 2017/2226 (30.11.2017)] și Sistemul european de informații și de autorizare privind călătoriile [Regulamentul (UE) 2018/1240 (12.9.2018) și Regulamentul (UE) 2018/1241 (12.9.2018)].

14 În ultimii ani, rolul Europol a fost consolidat în mod considerabil în ceea ce privește atât domeniul de aplicare, cât și complexitatea acestuia. Agenția a fost consolidată prin adoptarea Regulamentului privind Europol în 2016 [Regulamentul (UE) 2016/794 (11.5.2016)]. Statele membre au sporit în mod semnificativ volumul de informații partajate cu ajutorul și prin intermediul Europol. Instituirea Centrului Europol de combatere a terorismului (ECTC) a consolidat capacitățile analitice ale Europol în cazurile de terorism. Bugetul Europol a crescut considerabil în ultimii ani, de la 82 de milioane EUR în 2014 la 138 de milioane EUR în 2019. Negocierile privind bugetul pentru 2020 sunt în curs de desfășurare.

15 Regulamentul (UE) 2019/817 (20.5.2019) și Regulamentul (UE) 2019/818 (20.5.2019).

pentru agenții responsabili cu aplicarea legii, polițiștii de frontieră și funcționarii din domeniul migrației, contribuind astfel la îmbunătățirea securității interne și a gestionării frontierelor.

Cu toate acestea, interoperabilitatea și toate inovațiile pe care le implică aceasta vor avea un impact în ceea ce privește asigurarea securității și gestionarea frontierelor și a migrației pe teren numai dacă fiecare stat membru pune în aplicare pe deplin legislația aferentă. Din acest motiv, punerea în aplicare a interoperabilității constituie o prioritate de prim rang a Uniunii securității, atât la nivel politic, cât și la nivel tehnic. Comisia și Agenția UE pentru gestionarea operațională a sistemelor informatice la scară largă în spațiul de libertate, securitate și justiție (eu-LISA) sprijină statele membre cu expertiză și schimb de cele mai bune practici, utilizând o rețea de coordonatori naționali și dezvoltând un tablou de bord pentru a permite modalități eficace de monitorizare și coordonare. Cooperarea strânsă dintre agențiile UE, toate statele membre și țările asociate spațiului Schengen va fi esențială pentru atingerea obiectivului ambițios de realizare a unei interoperabilități depline a sistemelor de informații ale UE pentru asigurarea securității și gestionarea frontierelor și a migrației până în 2020.

Între timp, Parlamentul European și Consiliul trebuie încă **să finalizeze activitatea legislativă** în acest sens. Ajungerea rapidă la un acord cu privire la toate propunerile legislative în curs de adoptare este esențială pentru a asigura implementarea completă și la timp a interoperabilității. În primul rând, ca parte a punerii tehnice în aplicare a **Sistemului european de informații și de autorizare privind călătoriile**, este necesar să se aducă modificări tehnice regulamentelor aferente[16] în vederea instituirii complete a sistemului. Comisia invită Parlamentul European să își accelereze lucrările cu privire la aceste modificări tehnice pentru a începe negocierile interinstituționale cât mai curând posibil. În al doilea rând, sunt încă în curs de desfășurare negocierile interinstituționale cu privire la propunerea din mai 2018 de consolidare și de modernizare a **Sistemului de informații privind vizele** existent.[17] Pe baza primului trilog care a avut loc la 22 octombrie 2019, Comisia invită ambii colegiuitori să încheie rapid negocierile. În al treilea rând, se așteaptă în continuare un acord cu privire la propunerea Comisiei din mai 2016 de extindere a domeniului de aplicare a **Eurodac**[18] în sensul stocării nu numai a amprentelor digitale și a datelor relevante ale solicitanților de azil și ale persoanelor reținute în legătură cu trecerea neregulamentară a frontierei externe, ci și ale resortisanților țărilor terțe aflați în situație de ședere ilegală. Modificările propuse ar extinde, de asemenea, perioada de stocare a amprentelor digitale și a datelor relevante ale persoanelor care intră în UE în mod neregulamentar. Comisia invită colegiuitorii să procedeze la adoptarea propunerii.

În vederea consolidării sistemelor de informații ale UE pentru asigurarea securității și gestionarea frontierelor și a migrației, Comisia invită Parlamentul European și Consiliul:

- să își intensifice eforturile pentru a ajunge la un acord rapid asupra modificărilor tehnice propuse, care sunt necesare pentru instituirea **Sistemului european de informații și de autorizare privind călătoriile**.
- să desfășoare rapid și să încheie negocierile privind propunerea de consolidare a actualului **Sistem de informații privind vizele**.
- să adopte propunerea legislativă privind **Eurodac** (*prioritate stabilită în Declarația comună*).

16 Regulamentul (UE) 2018/1240 (12.9.2018) și Regulamentul (UE) 2018/1241 (12.9.2018).
17 COM (2018) 302 final (16.5.2018).
18 COM (2016) 272 final (4.5.2016).

3. Limitarea marjei de manevră a teroriștilor

UE a luat măsuri ferme pentru a limita marja de manevră a teroriștilor, prin noi norme care fac mai dificil accesul teroriștilor și al altor infractori la explozivi[19], arme de foc și finanțare[20], precum și pentru a restricționa circulația acestora.[21]

Pentru a consolida răspunsul judiciar la terorism, Agenția UE pentru Cooperare în Materie de Justiție Penală (Eurojust) a înființat, la 1 septembrie 2019, un Registru judiciar european de combatere a terorismului. Registrul va colecta informații judiciare pentru a stabili legături în cadrul procedurilor împotriva persoanelor suspectate de infracțiuni de terorism, consolidând astfel coordonarea dintre procurori în investigațiile de combatere a terorismului cu potențiale implicații transfrontaliere.

Cu toate acestea, sunt necesare eforturi suplimentare pentru a sprijini și a facilita anchetele în cazurile transfrontaliere, în special în ceea ce privește **accesul** autorităților de aplicare a legii **la probele electronice**. În ceea ce privește propunerile legislative din aprilie 2018 de îmbunătățire a accesului transfrontalier la probele electronice în cadrul anchetelor penale[22], Parlamentul European urmează încă să își adopte poziția de negociere înainte ca colegiuitorii să poată iniția negocieri. Comisia îndeamnă Parlamentul European să facă progrese în ceea ce privește această propunere legislativă, astfel încât colegiuitorii să poată lucra în vederea adoptării sale rapide. Pe baza propunerii sale de norme interne ale UE, Comisia se angajează, de asemenea, în **negocieri internaționale** pentru a îmbunătăți accesul transfrontalier la probele electronice. La 25 septembrie 2019, Comisia și autoritățile Statelor Unite ale Americii au organizat prima rundă de negocieri oficiale cu privire la un **acord între UE și SUA privind accesul transfrontalier la probele electronice**. O nouă rundă este programată pentru 6 noiembrie 2019. În contextul negocierilor în curs privind un **al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică**, Comisia a participat în numele Uniunii la trei runde de negocieri în iulie, septembrie și octombrie 2019. Deși s-au înregistrat progrese semnificative în cadrul acestor negocieri, o serie de subiecte importante de interes semnificativ pentru Uniune încă urmează să fie abordate, cum ar fi garanțiile privind protecția datelor. Negocierea unui al doilea protocol adițional va continua în noiembrie 2019 și pe parcursul anului 2020. Este important să se treacă rapid la ambele negocieri pentru a înregistra rezultate în ceea ce privește cooperarea internațională privind schimbul de probe electronice, asigurând în același timp compatibilitatea cu legislația UE și cu obligațiile statelor membre în temeiul acesteia, ținând seama, de asemenea, de modul în care va evolua legislația UE.

Reflectând preocupările actuale cu privire la spălarea banilor, Parlamentul European a adoptat, la 19 septembrie 2019, o **rezoluție referitoare la stadiul punerii în aplicare a legislației Uniunii privind combaterea spălării banilor**[23], răspunzând pachetului de patru

---

19 Regulamentul (UE) 2019/1148 (20.6.2019) privind comercializarea și utilizarea precursorilor de explozivi. Regulamentul a intrat în vigoare la 31 iulie 2019 și se aplică după 18 luni de la intrarea sa în vigoare.

20 Directiva (UE) 2019/1153 (11.7.2019) de stabilire a normelor de facilitare a utilizării informațiilor financiare și de alt tip pentru prevenirea, depistarea, investigarea sau urmărirea penală a anumitor infracțiuni.

21 Introducerea controalelor sistematice efectuate la frontierele externe asupra tuturor cetățenilor care folosesc Sistemul de Informații Schengen.

22 COM(2018) 225 final (17.4.2018) și COM(2018) 226 final (17.4.2018).

23 https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_EN.html

rapoarte privind combaterea spălării banilor, adoptat de Comisie la 24 iulie 2019[24]. Parlamentul European a invitat statele membre să asigure punerea în aplicare adecvată și rapidă a directivelor privind combaterea spălării banilor. De asemenea, Parlamentul European a solicitat Comisiei să evalueze dacă un regulament privind combaterea spălării banilor ar fi mai adecvat decât o directivă și să evalueze necesitatea unui mecanism de coordonare și sprijin pentru unitățile de informații financiare.

Pentru a îmbunătăți accesul autorităților de aplicare a legii la probele electronice, Comisia invită Parlamentul European și Consiliul:

- să ajungă la un acord rapid asupra propunerilor legislative privind **probele electronice** *(prioritate stabilită în Declarația comună)*.

4. Întărirea securității cibernetice

Întărirea securității cibernetice rămâne un aspect esențial al activității desfășurate pentru realizarea unei Uniuni a securității efective și autentice. Prin punerea în aplicare a Strategiei de securitate cibernetică a UE din 2017[25], Uniunea și-a întărit atât reziliența, devenind mai greu de atacat și dobândind o capacitate de recuperare mai rapidă, cât și efectul de descurajare, prin sporirea șanselor ca atacatorii să fie prinși și pedepsiți, inclusiv printr-un cadru pentru un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare. Uniunea sprijină, de asemenea, statele membre în domeniul apărării cibernetice, prin punerea în aplicare a cadrului de politică al UE în domeniul apărării cibernetice.[26]

Odată cu intrarea în vigoare a Legii privind securitatea cibernetică[27] în iunie 2019, **cadrul UE de certificare a securității cibernetice** prinde contur. Certificarea joacă un rol esențial în sporirea încrederii consumatorilor și în îmbunătățirea securității produselor și serviciilor care sunt cruciale pentru piața unică digitală. Cadrul de certificare va furniza sisteme de certificare la nivelul UE sub forma unui set cuprinzător de norme, cerințe tehnice, standarde și proceduri. Acesta implică două grupuri de experți, și anume Grupul european pentru certificarea securității cibernetice, care reprezintă autoritățile statelor membre, și Grupul părților interesate pentru certificarea securității cibernetice, care reprezintă industria. Acesta din urmă reunește atât partea de cerere, cât și partea de ofertă de produse și servicii legate de tehnologia informației și comunicațiilor, inclusiv întreprinderile mici și mijlocii, furnizorii de servicii digitale, organismele europene și internaționale de standardizare, organismele naționale de acreditare, autoritățile de supraveghere a protecției datelor și organismele de evaluare a conformității.

Între timp, Parlamentul European și Consiliul trebuie încă să ajungă la un acord cu privire la inițiativa legislativă[28] privind **Centrul de competențe european industrial, tehnologic și de**

---

[24] Raport privind evaluarea riscului de spălare a banilor și de finanțare a terorismului care afectează piața internă și se referă la activități transfrontaliere [COM (2019) 370 (24.7.2019)], Raport privind interconectarea mecanismelor automatizate naționale centralizate (registre centrale sau sisteme centrale de extragere a datelor electronice) din statele membre în ceea ce privește conturile bancare [COM (2019) 372 final (24.7.2019)], Raport privind evaluarea presupuselor cazuri recente de spălare a banilor care implică instituțiile de credit din UE [COM (2019) 373 final (24.7.2019)], Raport de evaluare a cadrului de cooperare dintre unitățile de informații financiare [COM (2019) 371 final, (24.7.2019)].

[25] JOIN(2017) 450 final (13.9.2017).

[26] Cadrul de politici pentru apărarea cibernetică al UE (actualizare 2018), astfel cum a fost adoptat de Consiliu la 19 noiembrie 2018 (14413/18).

[27] Regulamentul (UE) 2019/881 (17.4.2019).

[28] COM(2018) 630 final (12.9.2018).

cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare. Propunerea urmărește să consolideze capacitatea de securitate cibernetică a Uniunii prin stimularea ecosistemului tehnologic și industrial european al securității cibernetice, precum și prin coordonarea și punerea în comun a resurselor aferente. Comisia îi invită pe ambii colegiuitori să reia și să încheie rapid negocierile interinstituționale cu privire la această inițiativă prioritară de consolidare a securității cibernetice.

Eforturile de îmbunătățire a securității cibernetice includ sprijinul atât pentru nivelul național, cât și pentru nivelul regional[29].

Dincolo de amenințările cibernetice la adresa sistemelor și a datelor, UE continuă să răspundă provocărilor complexe și multidimensionale generate de **amenințările hibride**. În cadrul Consiliului, a fost creat un grup de lucru orizontal privind contracararea amenințărilor hibride pentru a îmbunătăți reziliența UE și a statelor sale membre împotriva amenințărilor hibride și pentru a sprijini acțiunile de consolidare a rezilienței la criză a societăților. Comisia și Serviciul European de Acțiune Externă sprijină aceste eforturi în temeiul Cadrului comun privind contracararea amenințărilor hibride din 2016[30] și al Comunicării comune din 2018[31] privind sporirea rezilienței și consolidarea capacităților de abordare a amenințărilor hibride. În plus, Centrul Comun de Cercetare elaborează un cadru de tip „model conceptual” pentru a caracteriza amenințările hibride, cu scopul de a sprijini statele membre și autoritățile lor competente să identifice tipul de atac hibrid cu care s-ar putea confrunta. Modelul analizează modul în care un actor (statal sau nestatal) utilizează o serie de instrumente (de la dezinformare la spionaj sau operațiuni fizice) în diferite domenii (economic, militar, social, politic) pentru a afecta o țintă în vederea realizării unei serii de obiective.

Pentru a întări securitatea cibernetică, Comisia invită Parlamentul European și Consiliul:
• să ajungă rapid la un acord asupra propunerii legislative privind **Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare**.

III. ÎNTĂRIREA SECURITĂȚII INFRASTRUCTURILOR DIGITALE

Rețelele de a cincea generație (5G) vor constitui viitoarea coloană vertebrală a economiilor și societăților din ce în ce mai digitalizate. Sunt vizate miliarde de obiecte și de sisteme conectate, inclusiv în sectoare vitale, cum ar fi energia, transporturile, serviciile bancare și sănătatea, precum și sistemele de control industrial care transmit informații sensibile și sprijină sistemele de siguranță. Asigurarea securității cibernetice și a rezilienței rețelelor 5G este, prin urmare, esențială.

Ca parte a unei abordări coordonate, statele membre au publicat, la 9 octombrie 2019, un raport privind **evaluarea coordonată a riscurilor în materie de securitate cibernetică în rețelele 5G la nivelul UE**, cu sprijinul Comisiei și al Agenției Europene pentru Securitate

[29] De exemplu, Comisia sprijină un parteneriat de inovare inter-regională cu privire la securitatea cibernetică, care implică Bretania, Castilia-Leon, Renania de Nord-Westfalia, Finlanda Centrală și Estonia, pentru a dezvolta un lanț valoric al securității cibernetice în Europa cu accent pe comercializare și extindere.

[30] JOIN(2016) 18 final (6.4.2016).

[31] JOIN(2018) 16 final (13.6.2018).

Cibernetică.[32] Acest pas important face parte din punerea în aplicare a recomandării Comisiei din martie 2019 de asigurare a unui nivel ridicat de securitate cibernetică a rețelelor 5G în întreaga UE.[33] Raportul se bazează pe rezultatele evaluărilor naționale ale riscurilor în materie de securitate cibernetică efectuate de toate statele membre ale UE. Acesta identifică principalele amenințări și principalii factori de amenințare, activele cele mai sensibile, principalele vulnerabilități (atât cele tehnice, cât și alte tipuri de vulnerabilități) și o serie de riscuri strategice. Această evaluare oferă baza necesară pentru a identifica măsurile de reducere a riscurilor care pot fi aplicate la nivel național și european.

Raportul identifică o serie de **provocări** importante **în materie de securitate cibernetică** care sunt susceptibile să apară sau să devină mai proeminente în rețelele 5G. Aceste provocări în materie de securitate sunt legate în principal de *inovațiile* esențiale din tehnologia 5G, în special de importanța programelor informatice și de gama largă de servicii și aplicații permise de 5G, precum și de rolul *furnizorilor* în crearea și operarea rețelelor 5G și de gradul de dependență de furnizori individuali. Aceasta înseamnă că produsele, serviciile și operațiunile furnizorilor devin din ce în ce mai mult parte a „suprafeței de atac” a rețelelor 5G. În plus, profilul de risc al furnizorilor individuali va deveni deosebit de important, inclusiv probabilitatea ca furnizorul să facă obiectul unei intervenții din partea unei țări care nu este membră a UE.

În conformitate cu procesul stabilit în recomandarea Comisiei din martie 2019, statele membre ar trebui să convină, până la 31 decembrie 2019, asupra unui **set de măsuri de atenuare** care să abordeze riscurile de securitate cibernetică identificate la nivel național și la nivelul Uniunii. Comisia și Serviciul European de Acțiune Externă vor continua, de asemenea, să facă schimb cu parteneri care împărtășesc aceeași viziune cu privire la securitatea cibernetică și reziliența rețelelor 5G.

[32] Evaluarea coordonată a riscurilor în materie de securitate cibernetică în rețelele 5G la nivelul UE a fost finalizată de către grupul de cooperare al autorităților competente, astfel cum este instituit în temeiul Directivei privind securitatea rețelelor și a sistemelor informatice [Directiva (UE) 2016/1148) (6.7.2016)], cu ajutorul Comisiei și al Agenției Europene pentru Securitate Cibernetică: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019)2355 final (26.3.2019).

IV. COMBATEREA DEZINFORMĂRII ȘI PROTEJAREA ALEGERILOR ÎMPOTRIVA ALTOR AMENINȚĂRI CIBERNETICE

UE a stabilit un **cadru de acțiune coordonată împotriva dezinformării,** cu respectarea deplină a valorilor europene și a drepturilor fundamentale.[34] În cadrul Planului de acțiune împotriva dezinformării[35], se desfășoară în continuare activități pentru reducerea posibilităților de dezinformare, inclusiv în vederea protejării integrității alegerilor.

Elementul central în acest sens îl reprezintă colaborarea cu industria prin intermediul unui **Cod de bune practici privind dezinformarea** bazat de autoreglementare, care vizează platformele online și sectorul publicității și care a devenit aplicabil în octombrie 2018.[36] Comisia a evaluat eficacitatea codului în urma primului an de operațiuni, pe baza rapoartelor anuale de autoevaluare transmise de platformele online și de ceilalți semnatari ai codului și publicate la 29 octombrie 2019, împreună cu o declarație a Comisiei.[37] În linii mari, rapoartele demonstrează eforturile considerabile depuse de semnatari în vederea punerii în aplicare a angajamentelor asumate.

Acțiunile întreprinse de semnatarii platformelor variază în ceea ce privește viteza și domeniul de aplicare în cadrul celor cinci piloni ai angajamentelor stabiliți în cod. În general, progresele sunt mai avansate în ceea ce privește angajamentele legate de alegerile europene din 2019, și anume cu privire la perturbarea stimulentelor pentru promovarea și monetizarea dezinformării (pilonul 1), asigurarea transparenței publicității politice și tematice (pilonul 2) și asigurarea integrității serviciilor raportat la conturile și comportamentele neautentice (pilonul 3). În schimb, sunt mai puțin avansate sau lipsesc progresele în ceea ce privește angajamentele referitoare la întărirea poziției consumatorilor (pilonul 4) și la întărirea poziției comunității de cercetare, inclusiv prin furnizarea de către platforme a unui acces relevant și care să respecte confidențialitatea la seturi de date în scopuri de cercetare (pilonul 5). Există, de asemenea, diferențe în ceea ce privește domeniul de aplicare a acțiunilor întreprinse de fiecare platformă pentru a asigura punerea în aplicare a angajamentelor acestora, precum și diferențe în rândul statelor membre în ceea ce privește implementarea politicilor individuale. Comisia continuă să colaboreze cu semnatarii codului și cu alte părți interesate pentru a intensifica acțiunile întreprinse împotriva dezinformării.

În cadrul Planului de acțiune împotriva dezinformării, Comisia și Înaltul Reprezentant, în cooperare cu statele membre, au instituit un **sistem de alertă rapidă** pentru abordarea campaniilor de dezinformare. Sistemul de alertă rapidă a permis instituțiilor UE și statelor membre să facă schimb de informații și analize înainte de alegerile din 2019 pentru Parlamentul European și să-și coordoneze răspunsurile. Această activitate s-a intensificat și

---

34 A se vedea Planul de acțiune împotriva dezinformării [JOIN (2018) 36 final (5.12.2018)].

35 COM(2019) 12 final (14.6.2019).

36 În temeiul codului, platformele online Google, Facebook, Twitter și Microsoft s-au angajat să prevină utilizarea în scopuri de manipulare a serviciilor lor de către factori negativi, să asigure transparența și divulgarea publică a publicității politice și să ia alte măsuri pentru a îmbunătăți transparența, responsabilitatea și credibilitatea ecosistemului online. Asociațiile profesionale din sectorul publicității s-au angajat, de asemenea, să coopereze cu platformele pentru a îmbunătăți controlul plasării anunțurilor publicitare și pentru a dezvolta instrumente de siguranță a mărcilor menite să limiteze plasarea de anunțuri publicitare pe site-uri web care promovează dezinformarea.

37 https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. Pe lângă Google, Facebook, Twitter și Microsoft, printre ceilalți semnatari ai codului se numără Mozilla, șapte asociații la nivel european sau la nivel național care reprezintă sectorul publicității, și EDiMA, o asociație europeană care reprezintă platformele și alte întreprinderi tehnologice active în sectorul online.

mai mult după alegeri, schimburile la nivel de lucru având loc zilnic și fiind organizate trei reuniuni ale punctelor de contact ale sistemelor de alertă rapidă de către diferite state membre.

Un alt pas practic pentru identificarea dezinformării l-a constituit activitatea **echipei de comunicare strategică** („StratComms"), în special a grupului său operativ East Stratcom, care a derulat proiectul „EUvsDisinfo" pentru a monitoriza, a analiza și a răspunde la dezinformarea pro-Kremlin.[38] De la începutul anului 2019, primul buget dedicat de 3 milioane EUR a făcut posibilă intensificarea și extinderea acestei activități pentru a include monitorizarea și analiza dezinformării pro-Kremlin pe internet, în emisiunile televizate și pe platformele de comunicare socială în 19 limbi, de la engleză la sârbă și arabă. Volumul activităților de dezinformare expuse a crescut de mai mult de două ori ca urmare a îmbunătățirii capacității de monitorizare, fiind înregistrate aproximativ 2000 de cazuri de dezinformare până în prezent în 2019, comparativ cu 765 de cazuri în aceeași perioadă din 2018. Grupul operativ East Stratcom a jucat un rol vital în monitorizarea și expunerea dezinformării pro-Kremlin vizând alegerile din 2019 pentru Parlamentul European. Cercetarea a fost asociată cu o campanie de sensibilizare cu privire la tentativele de ingerință în procesele electorale din întreaga lume. Activitatea sa de informare, desfășurată în strânsă cooperare cu Parlamentul European și cu Comisia, a avut drept rezultat peste 20 de interviuri în mass-media, în timp ce campania a implicat peste 300 de jurnaliști.

Comisia a luat, de asemenea, măsuri pentru **a reduce răspândirea dezinformării și a miturilor legate de instituțiile și politicile UE**. Aceasta a instituit o rețea de experți în comunicare cu un portal online care furnizează materiale informative interactive cu privire la politicile UE și la provocarea reprezentată de dezinformare și impactul acesteia asupra societății. De asemenea, Comisia a lansat o serie de campanii pe platformele de comunicare socială axate pe combaterea dezinformării[39], în colaborare cu Parlamentul European și cu Serviciul European de Acțiune Externă.

V. PUNEREA ÎN APLICARE A ALTOR DOSARE PRIORITARE ÎN MATERIE DE SECURITATE

1. Punerea în aplicare a măsurilor legislative legate de Uniunea securității

Măsurile convenite în Uniunea securității vor aduce beneficii depline numai în cazul în care toate statele membre asigură punerea în aplicare rapidă și completă a acestora. În acest scop, Comisia sprijină în mod activ statele membre în ceea ce privește punerea în aplicare a legislației UE, inclusiv prin finanțare și prin facilitarea schimbului de cele mai bune practici. Comisia recurge la toate mijloacele de care dispune în temeiul tratatelor pentru asigurarea respectării legislației UE, inclusiv măsurile de constatare a neîndeplinirii obligațiilor, după caz.

Termenul pentru transpunerea **Directivei privind registrul UE cu numele pasagerilor**[40] a expirat la 25 mai 2018. Până în prezent, 25 de state membre au notificat transpunerea integrală[41], ceea ce reprezintă un progres semnificativ din iulie 2018, când Comisia a lansat

[38] www.euvsdisinfo.eu

[39] https://europa.eu/euprotects/

[40] Directiva (UE) 2016/681 (27.4.2016). Danemarca nu a participat la adoptarea acestei directive, nu are obligații în temeiul acesteia și nu face obiectul aplicării sale.

[41] Trimiterile la notificarea transpunerii integrale țin seama de declarațiile statelor membre și nu aduc atingere verificării transpunerii de către serviciile Comisiei (situație verificată la 17.10.2019).

proceduri de constatare a neîndeplinirii obligațiilor împotriva a 14 state membre.[42] Două state membre nu au notificat încă transpunerea integrală, în pofida procedurilor de constatare a neîndeplinirii obligațiilor aflate în curs de desfășurare, lansate la 19 iulie 2018.[43] În paralel, Comisia continuă să sprijine toate statele membre în eforturile lor de a finaliza dezvoltarea propriilor lor sisteme tip registru cu numele pasagerilor, inclusiv prin facilitarea schimbului de informații și de cele mai bune practici.

Termenul de transpunere a **Directivei privind combaterea terorismului**[44] a expirat la 8 septembrie 2018. Până în prezent, 22 de state membre au notificat transpunerea integrală, ceea ce reprezintă un progres semnificativ din noiembrie 2018, când Comisia a lansat proceduri de constatare a neîndeplinirii obligațiilor împotriva a 16 state membre.[45] Trei state membre nu au notificat încă transpunerea integrală, în pofida procedurilor de constatare a neîndeplinirii obligațiilor aflate în curs de desfășurare.[46] La 25 iulie 2019, Comisia a trimis avize motivate către două state membre pentru neîndeplinirea obligației de notificare a transpunerii integrale a directivei[47]. Ca răspuns, ambele state membre au anunțat că lucrările legislative vor fi finalizate până la sfârșitul acestui an.

Termenul pentru transpunerea **Directivei privind controlul achiziționării și deținerii de arme**[48] a expirat la 14 septembrie 2018. Până în prezent, 13 state membre au notificat transpunerea integrală. Un număr de 15 state membre nu au notificat încă transpunerea integrală, în pofida procedurilor de constatare a neîndeplinirii obligațiilor aflate în curs de desfășurare, lansate la 22 noiembrie 2018.[49] La 25 iulie 2019, Comisia a trimis avize motivate către 20 de state membre pentru neîndeplinirea obligației de notificare a transpunerii integrale a directivei. Ca răspuns, cinci state membre au notificat transpunerea integrală a directivei.[50]

Termenul pentru transpunerea **Directivei privind asigurarea respectării legislației din domeniul protecției datelor**[51] a expirat la 6 mai 2018. Până în prezent, 25 de state membre au notificat transpunerea integrală, ceea ce reprezintă un progres semnificativ din iulie 2018, când Comisia a lansat proceduri de constatare a neîndeplinirii obligațiilor împotriva a 19 state membre.[52] Trei state membre nu au notificat încă transpunerea integrală, în pofida procedurilor de constatare a neîndeplinirii obligațiilor aflate în curs de desfășurare.[53] La

---

42 A se vedea cel de Al șaisprezecelea raport privind progresele înregistrate către o Uniune a securității efectivă și reală [COM (2018) 690 final (10.10.2018)].

43 Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea (situație verificată la 17.10.2019).

44 Directiva (UE) 2017/541 (15.3.2017). Directiva nu se aplică în Regatul Unit, Irlanda și Danemarca.

45 A se vedea cel de Al șaptesprezecelea raport privind progresele înregistrate către o Uniune a securității efectivă și reală [COM (2018) 845 final (11.12.2018)].

46 Grecia și Luxemburg nu au notificat măsurile naționale de punere în aplicare. Polonia a notificat măsuri naționale care constituie transpunere parțială (situație verificată la 17.10.2019).

47 Grecia și Luxemburg.

48 Directiva (UE) 2017/853 (17.10.2019).

49 Belgia, Cehia, Estonia, Polonia, Suedia, Slovacia, Regatul Unit au notificat măsuri de transpunere pentru o parte dintre noile dispoziții. Cipru, Germania, Grecia, Spania, Luxemburg, Ungaria, România, Slovenia nu au notificat încă nicio măsură de transpunere (situație verificată la 17.10.2019).

50 Finlanda, Irlanda, Lituania, Țările de Jos, Portugalia (situație verificată la 17.10.2019).

51 Directiva (UE) 2016/680 (27.4.2016).

52 A se vedea cel de Al șaisprezecelea raport privind progresele înregistrate către o Uniune a securității efectivă și reală [COM (2018) 690 final (10.10.2018)].

53 Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea. Deși Germania a notificat transpunerea integrală, Comisia consideră că transpunerea respectivă nu este integrală (situație verificată la 17.10.2019).

25 iulie 2019, Comisia a decis să trimită două state membre[54] în fața Curții de Justiție a Uniunii Europene pentru netranspunerea directivei și a trimis o scrisoare de punere în întârziere unui stat membru[55] pentru netranspunerea integrală a directivei.[56]

Comisia evaluează transpunerea celei de **A patra directive privind combaterea spălării banilor**[57] și, în același timp, verifică dacă normele respective sunt puse în aplicare de către statele membre. Acestea trebuiau să transpună directiva în legislația națională până la 26 iunie 2018. Comisia menține procedurile de constatare a neîndeplinirii obligațiilor împotriva a 21 de state membre deoarece a considerat că statele membre au transmis comunicări care nu reprezintă o transpunere integrală a directivei.[58]

Comisia a evaluat conformitatea transpunerii **directivelor privind criminalitatea informatică**. Aceasta a lansat în iulie și octombrie 2019 proceduri de constatare a neîndeplinirii obligațiilor împotriva a 23 de state membre[59] deoarece a considerat că legislația națională de punere în aplicare notificată de statele membre respective nu reprezintă o transpunere corectă a **Directivei privind combaterea abuzului sexual asupra copiilor**[60]. De asemenea, Comisia a lansat în iulie și octombrie 2019 proceduri de constatare a neîndeplinirii obligațiilor împotriva a patru state membre[61] deoarece a considerat că legislația națională de punere în aplicare notificată de statele membre respective nu reprezintă o transpunere corectă a **Directivei privind atacurile împotriva sistemelor informatice**[62].

Comisia invită statele membre să ia de urgență măsurile necesare pentru transpunerea integrală a următoarelor directive în legislația națională și comunicarea acestora către Comisie:

- **Directiva privind registrul UE cu numele pasagerilor** - 1 stat membru nu a notificat încă transpunerea în legislația națională, iar 1 stat membru nu a finalizat încă notificarea transpunerii;[63]
- **Directiva privind combaterea terorismului** - 2 state membre nu au notificat încă transpunerea în legislația națională, iar 1 stat membru nu a finalizat încă notificarea transpunerii;[64]
- **Directiva privind controlul achiziționării și deținerii de arme** - 8 state membre nu au notificat încă transpunerea în legislația națională, iar 7 state membre nu au finalizat încă notificarea transpuneri;[65]

54 Grecia și Spania.
55 Germania.
56 Grecia a notificat transpunerea integrală pe care o evaluează Comisia.
57 Directiva (UE) 2015/849 (20.5.2015).
58 Belgia, Bulgaria, Cehia, Danemarca, Germania, Estonia, Irlanda, Franța, Italia, Cipru, Letonia, Lituania, Ungaria, Țările de Jos, Austria, Polonia, România, Slovacia, Finlanda, Suedia și Regatul Unit (situație verificată la 17.10.2019.). Anterior, au fost închise 7 proceduri de constatare a neîndeplinirii obligațiilor legate de directivă.
59 Belgia, Bulgaria, Cehia, Germania, Estonia, Grecia, Spania, Franța, Croația, Italia, Letonia, Lituania, Luxemburg, Ungaria, Malta, Austria, Polonia, Portugalia, România, Slovenia, Slovacia, Finlanda și Suedia.
60 Directiva 2011/93/UE (13.12.2011).
61 Bulgaria, Italia, Portugalia și Slovenia.
62 Directiva 2013/40/UE (12.08.2013).
63 Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea (situație verificată la 17.10.2019).
64 Grecia și Luxemburg nu au notificat transpunerea. Polonia a notificat transpunerea parțială (situație verificată la 17.10.2019).

- **Directiva privind asigurarea respectării legislației din domeniul protecției datelor** – 1 stat membru nu a notificat încă transpunerea în legislația națională, iar 2 state membre nu au finalizat încă notificarea transpunerii;[66]
- **A 4-a directivă privind combaterea spălării banilor** - 21 de state membre nu au finalizat încă notificarea transpunerii;[67]
- **Directiva privind combaterea abuzului sexual asupra copiilor,** în cazul căreia au fost lansate împotriva a 23 de state membre[68] proceduri de constatare a neîndeplinirii obligațiilor, ca urmare a transpunerii incorecte;
- **Directiva privind atacurile împotriva sistemelor informatice**, în cazul căreia au fost lansate împotriva a 4 state membre[69] proceduri de constatare a neîndeplinirii obligațiilor, ca urmare a transpunerii incorecte.

2. Gradul de pregătire și de protecție

Consolidarea rezilienței împotriva amenințărilor la adresa securității reprezintă o parte esențială a eforturilor depuse pentru realizarea unei uniuni a securității efective și autentice. Comisia sprijină statele membre și autoritățile locale în ceea ce privește consolidarea protecției spațiilor publice, prin punerea în aplicare a planului de acțiune din octombrie 2017 și a Parteneriatului din ianuarie 2019 privind securitatea în spațiile publice în cadrul Agendei urbane a UE. Această activitate implică orașele care s-au adresat Comisiei și au solicitat sprijin pentru abordarea provocărilor cu care s-au confruntat în protejarea spațiilor publice.

Schimbul de cele mai bune practici între autoritățile locale și cu operatorii privați este esențial pentru consolidarea securității spațiilor publice. Acest aspect s-a aflat în centrul **Săptămânii europene a securității** de la Nisa, Franța, în perioada 14-18 octombrie 2019, organizată prin proiectul finanțat de UE „Protejarea orașelor aliate împotriva terorismului în domeniul securității zonelor urbane". Reunind 500 de participanți din orașe din întreaga Europă, autorități naționale și instituții de cercetare, evenimentul a evidențiat importanța unei cooperări strânse între toate părțile interesate implicate, atât publice, cât și private, precum și rolul noilor tehnologii pentru o mai bună protecție a orașelor. Protecția spațiilor publice a fost abordată, de asemenea, în **Săptămâna europeană a regiunilor și orașelor** din Bruxelles, în perioada 7-10 octombrie 2019, printr-un atelier privind Agenda urbană pentru Parteneriatul UE pentru securitatea în spațiile publice. Acesta s-a axat pe rolul autorităților locale în domeniul politicii de securitate, pe reglementarea și finanțarea UE pentru a face față principalelor provocări în materie de securitate în spațiile publice urbane și pe teme-cheie precum inovarea prin soluții și tehnologii inteligente, inclusiv conceptul de securitate din momentul proiectării, prevenire și incluziune socială. Comisia contribuie, de asemenea, la stimularea inovării orașelor în aceste domenii prin intermediul ultimei sale cereri de propuneri

---

65 Belgia, Cehia, Estonia, Polonia, Suedia, Slovacia, Regatul Unit au notificat măsuri de transpunere pentru o parte dintre noile dispoziții. Cipru, Germania, Grecia, Spania, Luxemburg, Ungaria, România, Slovenia nu au notificat încă nicio măsură de transpunere (situație verificată la 17.10.2019).

66 Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea. Deși Germania a notificat transpunerea completă, Comisia consideră că această transpunere nu este completă (situație verificată la 17.10.2019).

67 Belgia, Bulgaria, Cehia, Danemarca, Germania, Estonia, Irlanda, Franța, Italia, Cipru, Letonia, Lituania, Ungaria, Țările de Jos, Austria, Polonia, România, Slovacia, Finlanda, Suedia și Regatul Unit (situație verificată la 17.10.2019).

68 Belgia, Bulgaria, Cehia, Germania, Estonia, Grecia, Spania, Franța, Croația, Italia, Letonia, Lituania, Luxemburg, Ungaria, Malta, Austria, Polonia, Portugalia, România, Slovenia, Slovacia, Finlanda și Suedia.

69 Bulgaria, Italia, Portugalia și Slovenia.

pentru acțiuni urbane inovatoare, ale cărei rezultate au fost anunțate în august 2019. Printre proiectele selectate, trei orașe (Pireu în Grecia, Tampere în Finlanda și Torino în Italia) vor testa soluții noi în materie de securitate urbană.[70]

Pentru a **proteja mai bine locurile de cult** și a explora nevoile diferitelor grupuri religioase, Comisia a organizat o reuniune la 7 octombrie 2019 cu reprezentanții comunităților evreiești, musulmane, creștine și budiste. Parte a punerii în aplicare a Planului de acțiune al UE din 2017 pentru sprijinirea protecției spațiilor publice, reuniunea a arătat că nivelul de conștientizare și de pregătire în materie de securitate variază în mod semnificativ între diferitele comunități religioase, subliniind importanța continuării schimbului de bune practici. Reuniunea a evidențiat, de asemenea, că introducerea unor măsuri de securitate de bază și o mai bună conștientizare a aspectelor legate de securitate nu sunt incompatibile cu menținerea caracterului deschis și accesibil al locurilor de cult. Comisia va colecta bune practici și materiale de sensibilizare pe platforma sa electronică a experților și va aduce această situație în atenția autorităților de securitate din statele membre în cadrul Forumului public-privat pentru protecția spațiilor publice.

Un domeniu specific care necesită o atenție sporită este creșterea amenințării la adresa securității infrastructurii critice și a spațiilor publice reprezentată de **drone**. Venind în completarea legislației recente a UE[71] cu privire la operarea în siguranță a dronelor în sisteme aeronautice fără pilot la bord și fără a submina oportunitățile de utilizare benefică a dronelor, Comisia sprijină statele membre în ceea ce privește urmărirea tendințelor de utilizare răuvoitoare a dronelor, finanțarea cercetării relevante și facilitarea testării de contramăsuri. Schimbul de experiență și de cele mai bune practici este esențial, astfel cum s-a arătat în cadrul Conferinței internaționale la nivel înalt privind combaterea amenințărilor reprezentate de sistemele de aeronave fără pilot la bord de la Bruxelles, din 17 octombrie 2019. Organizat de Comisie, acest eveniment a reunit 250 de participanți din statele membre, organizații internaționale, parteneri din țări terțe, reprezentanți ai industriei, ai mediului academic și ai societății civile pentru a discuta provocările în materie de securitate generate de drone și modalitățile de abordare a acestora. Reuniunea a arătat necesitatea unor evaluări periodice ale riscurilor legate de drone, precum și a unei cooperări strânse între autoritățile aeronautice și autoritățile de aplicare a legii în vederea dezvoltării în continuare a legislației europene privind operarea în siguranță a dronelor. De asemenea, este necesară testarea suplimentară a contramăsurilor împotriva dronelor prin intermediul unei abordări europene coordonate. În plus, s-a convenit că, pentru ca dronele să fie sigure, securizate, fiabile din punct de vedere operațional și dificil de utilizat în scopuri răuvoitoare, este esențial să existe o strânsă colaborare între autorități și industrie.

3. Dimensiunea externă

Întrucât majoritatea riscurilor de securitate cu care se confruntă Uniunea depășesc frontierele UE și reprezintă amenințări la nivel mondial, cooperarea cu țările partenere, organizațiile și părțile interesate relevante joacă un rol vital în construirea unei uniuni a securității efective și autentice.

---

[70] „Acțiunile urbane inovatoare” sunt un instrument cofinanțat prin Fondul european de dezvoltare regională. Pentru informații suplimentare, a se vedea: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

[71] Regulamentul de punere în aplicare (UE) 2019/947 al Comisiei din 24 mai 2019 privind normele și procedurile de operare a sistemelor de aeronave fără pilot la bord.

Schimbul de informații este esențial pentru această cooperare. Împreună cu acest raport, Comisia a adoptat o recomandare adresată Consiliului de autorizare a inițierii negocierilor pentru un **acord între UE și Noua Zeelandă cu privire la schimbul de date cu caracter personal pentru combaterea formelor grave de criminalitate și a terorismului** între Europol și autoritățile competente din Noua Zeelandă. Un astfel de acord va consolida și mai mult capacitățile Europol de a se implica alături de Noua Zeelandă în scopul prevenirii și combaterii criminalității care se încadrează în sfera de cuprindere a obiectivelor Europol. În timp ce acordul de lucru din aprilie 2019 dintre Europol și poliția din Noua Zeelandă oferă un cadru pentru o cooperare structurată la nivel strategic, acesta nu oferă un temei juridic pentru schimbul de date cu caracter personal. Schimbul de date cu caracter personal cu respectarea deplină a dreptului UE și a drepturilor fundamentale este esențial pentru o cooperare operațională eficace în domeniul polițienesc. Anterior, Comisia a identificat opt țări prioritare din regiunea Orientul Mijlociu/Africa de Nord pe baza amenințării teroriste, a provocărilor legate de migrație și a nevoilor operaționale ale Europol de a începe negocierile.[72] Ținând seama de nevoile operaționale ale autorităților de aplicare a legii din întreaga UE, precum și de beneficiile potențiale ale unei cooperări mai strânse în acest domeniu, astfel cum s-a demonstrat, de asemenea, prin acțiunile ulterioare atacului din martie 2019 de la Christchurch, Comisia consideră că este necesar să adauge Noua Zeelandă ca țară prioritară pentru începerea negocierilor pe termen scurt.

O altă piatră de temelie a cooperării în materie de securitate dintre Uniune și țările terțe partenere este reprezentată de transferul de **date din registrul cu numele pasagerilor**. La 27 septembrie 2019, Comisia a adoptat o recomandare către Consiliu de autorizare a deschiderii negocierilor pentru un acord **UE-Japonia** privind transferul de date din registrul cu numele pasagerilor în vederea prevenirii și combaterii terorismului și a infracțiunilor transnaționale grave, cu respectarea deplină a garanțiilor în materie de protecție a datelor și a drepturilor fundamentale.[73] Recomandarea este în curs de examinare la nivelul grupului de lucru al Consiliului, iar Comisia invită Consiliul să adopte rapid un mandat pentru negocierile cu Japonia. Existența unor măsuri în timp util pentru Jocurile olimpice din 2020 ar aduce beneficii reale în materie de securitate.

La nivel global, Comisia sprijină activitatea desfășurată de **Organizația Aviației Civile Internaționale** în vederea stabilirii unui standard pentru prelucrarea datelor din registrul cu numele pasagerilor. Aceasta răspunde unei solicitări din cadrul Rezoluției nr. 2396 a Consiliului de Securitate al Organizației Națiunilor Unite care îndeamnă toate statele membre ale Organizației Națiunilor Unite să dezvolte capacitatea de a colecta, a prelucra și a analiza datele din registrul de nume al pasagerilor. La 13 septembrie 2019, Comisia a prezentat o propunere[74] de decizie a Consiliului privind poziția care urmează să fie adoptată în numele UE în cadrul Organizației Aviației Civile Internaționale în ceea ce privește standardele și practicile recomandate referitoare la datele din registrul cu numele pasagerilor. Propunerea este în curs de examinare la nivelul grupului de lucru al Consiliului, iar Comisia solicită adoptarea rapidă a deciziei Consiliului. Poziția Uniunii și a statelor sale membre a fost prezentată, de asemenea, în documentul informativ privind „Standardele și principiile referitoare la colectarea, utilizarea, prelucrarea și protecția datelor din registrul cu numele

[72] A se vedea Al unsprezecelea raport privind progresele înregistrate către o Uniune a securității efectivă și reală [COM (2017) 608 final (18.10.2017)]. Țările prioritare sunt Algeria, Egipt, Israel, Iordania, Liban, Maroc, Tunisia și Turcia.

[73] COM(2019) 420 final (27.9.2019).

[74] COM(2019) 416 final (13.9.2019).

pasagerilor", care a fost transmis celei de a 40-a sesiuni a Adunării Organizației Aviației Civile Internaționale.

În ceea ce privește lucrările în vederea unui nou acord privind registrul cu numele pasagerilor cu **Canada**, Comisia urmărește finalizarea rapidă a acordului. Între timp, revizuirea comună combinată și evaluarea comună a acordului privind registrul cu numele pasagerilor cu **Australia**, precum și evaluarea comună a acordului privind registrul cu numele pasagerilor cu **Statele Unite** au fost lansate în această vară, începând cu vizite la Canberra și Washington în august și, respectiv, septembrie 2019. Comisia a informat Comisia pentru libertăți civile, justiție și afaceri interne a Parlamentului European în cadrul unei sesiuni închise, din 14 octombrie 2019, cu privire la situația actuală a colaborării cu Japonia, Australia și Canada în ceea ce privește datele din registrul cu numele pasagerilor.

De asemenea, s-au înregistrat progrese în ceea ce privește cooperarea în materie de securitate cu partenerii din **Balcanii de Vest**, prin punerea în aplicare a Planului comun de acțiune privind combaterea terorismului pentru Balcanii de Vest din octombrie 2018. La 9 octombrie, Comisia a semnat două acorduri bilaterale de combatere a terorismului, fără caracter obligatoriu, cu Albania și cu Republica Macedonia de Nord.[75] Aceste acorduri stabilesc acțiuni prioritare adaptate care trebuie întreprinse de către autoritățile din țara parteneră respectivă, acoperind cele cinci obiective ale Planului de acțiune comun[76] și indicând sprijinul pe care Comisia intenționează să îl acorde. Se așteaptă ca în următoarele săptămâni să fie încheiate acorduri similare cu ceilalți parteneri din Balcanii de Vest. În plus, la 7 octombrie 2019, Comisia a semnat cu Muntenegru un acord privind cooperarea în materie de gestionare a frontierelor între Muntenegru și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă (EBCGA). Acordul permite agenției să acorde asistență statului Muntenegru în ceea ce privește gestionarea frontierelor cu scopul de a combate migrația neregulamentară și criminalitatea transfrontalieră, consolidând astfel securitatea la frontierele externe ale UE.

Pentru a întări cooperarea cu țările partenere în vederea combaterii amenințărilor comune la adresa securității, Comisia invită Consiliul:

- să adopte autorizația de lansare a negocierilor pentru un acord între UE și **Noua Zeelandă** privind schimbul de date cu caracter personal pentru combaterea formelor grave de criminalitate și a terorismului;
- să adopte autorizația de lansare a negocierilor pentru un acord între UE și **Japonia** privind transferul de date din Registrul cu numele pasagerilor;
- să adopte Propunerea de **Decizie a Consiliului privind poziția care urmează să fie adoptată în numele UE în cadrul Organizației Aviației Civile Internaționale** în ceea ce privește standardele și practicile recomandate referitoare la datele din Registrul cu numele pasagerilor.

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

[76] Planul de acțiune comun prevede acțiuni circumscrise următoarelor cinci obiective: un cadru solid pentru combaterea terorismului; prevenirea și combaterea eficace a extremismului violent; schimbul eficace de informații și cooperarea operațională; consolidarea capacităților de combatere a spălării banilor și de combatere a finanțării terorismului; consolidarea protecției cetățenilor și a infrastructurii.

VI. CONCLUZII

Prezentul raport prezintă gama largă de măsuri luate de UE pentru a răspunde amenințărilor comune din Europa și pentru a întări securitatea noastră colectivă. Ca urmare a viziunii comune potrivit căreia provocările actuale în materie de securitate sunt abordate cel mai bine lucrând împreună și colaborând cu țările terțe, progresele înregistrate către o Uniune a securității efectivă și autentică sunt rezultatul unei cooperări strânse între o gamă largă de actori care au inspirat încredere, și-au partajat resursele și au făcut față amenințărilor împreună: de la toate nivelurile de guvernare, de la orașe și alți actori locali, regiuni și autorități naționale până la nivelul UE, împreună cu Parlamentul European și cu Consiliul; implicând autorități publice, agenții ale UE, actori privați și societatea civilă; și utilizând competențe, instrumente și resurse din mai multe domenii de politică, precum politica în domeniul transporturilor, piața unică digitală sau politica de coeziune. Astfel, activitatea Uniunii securității este integrată în protecția drepturilor fundamentale, asigurând și promovând valorile noastre.

Eforturile în direcția unei Uniuni a securității efective și autentice trebuie să continue. Este nevoie de un acord rapid cu privire la inițiativele importante aflate în curs, în special cu privire la: (1) propunerea legislativă privind eliminarea conținutului online cu caracter terorist, (2) propunerea legislativă de îmbunătățire a accesului autorităților de aplicare a legii la probele electronice, (3) propunerea legislativă de instituire a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare și (4) propunerile legislative în curs referitoare la sisteme de informații mai puternice și mai inteligente pentru asigurarea securității și gestionarea frontierelor și a migrației. Măsurile și instrumentele convenite trebuie transformate într-o realitate operațională pe teren, cu punerea în aplicare pe deplin și în timp util a legislației UE de către toate statele membre, pentru a beneficia de toate avantajele acesteia în materie de securitate. În special, este esențial ca toate statele membre să pună în aplicare legislația recent convenită privind interoperabilitatea sistemelor de informații ale UE pentru asigurarea securității și gestionarea frontierelor și a migrației, în vederea atingerii obiectivului ambițios de realizare a interoperabilității depline până în 2020. În sfârșit, Europa trebuie să rămână vigilentă la amenințările emergente și în schimbare și să conlucreze în continuare pentru a întări securitatea tuturor cetățenilor.