

**I. INTRODUCERE**

Prezentul document este cel de Al nouăsprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și autentică. Raportul prezintă evoluțiile care au avut loc în cadrul a doi piloni principali: pe de o parte, combaterea terorismului și a criminalității organizate, precum și a mijloacelor care le susțin și, pe de altă parte, consolidarea mijloacelor noastre de apărare și a rezilienței împotriva acestor amenințări.

Europenii se așteaptă, în mod legitim, ca Uniunea să le asigure securitatea. Securitatea a fost o prioritate absolută pentru Comisia Juncker încă din prima zi a mandatului său. În documentul Consiliului European „O nouă agendă strategică 2019-2024”, obiectivul „protecției cetățenilor și a libertăților cetățenești” este prima dintre cele patru priorități principale ale Uniunii[[1]](#footnote-2). Consiliul European a anunțat, de asemenea, că va valorifica și va consolida eforturile Uniunii în lupta împotriva terorismului și a criminalității transfrontaliere, inclusiv prin îmbunătățirea cooperării și a schimbului de informații și prin dezvoltarea în continuare a unor instrumente comune.

Datorită cooperării strânse dintre Parlamentul European, Consiliu și Comisie, UE a făcut progrese importante în cadrul eforturilor comune în direcția unei uniuni a securității efective și autentice, prezentând o serie de inițiative legislative prioritare și punând în aplicare o gamă largă de măsuri nelegislative menite să sprijine statele membre și să sporească securitatea tuturor cetățenilor[[2]](#footnote-3). Uniunea a luat măsuri decisive pentru ca activitatea teroriștilor și a membrilor rețelelor infracționale să fie îngreunată, privându-i pe teroriști de mijloacele de care ar avea nevoie pentru a declanșa atacuri prin interzicerea achiziționării și a utilizării anumitor arme de foc și a anumitor explozivi și limitând accesul lor la finanțare. UE a consolidat, de asemenea, schimbul de informații dintre statele membre și a eliminat lacunele în materie de informații și așa-numitele „unghiuri moarte”, combătând, în același timp, radicalizarea, protejându-i pe europeni în mediul online, contracarând amenințările cibernetice și cele facilitate de tehnologiile informatice, consolidând gestionarea frontierelor externe ale Uniunii și cooperarea internațională în domeniul securității.

În același timp, există încă o serie de inițiative prioritare legate de uniunea securității care așteaptă să fie adoptate de colegiuitori. În urma constituirii celei de a 9-a legislaturi a Parlamentului European la 2 iulie 2019, prezentul raport:

* stabilește cazurile în care sunt necesare acțiuni din partea colegiuitorilor pentru a răspunde amenințărilor imediate. Trebuie luate în mod imperativ măsuri pentru a **combate propaganda teroristă și radicalizarea în mediul online**;
* stabilește inițiativele prioritare în curs legate de uniunea securității care necesită acțiuni suplimentare din partea colegiuitorilor în vederea consolidării **securității cibernetice** și a facilitării accesului la **probele electronice**, precum și a finalizării activității legate de dezvoltarea unor sisteme de informații mai puternice și mai inteligente pentru asigurarea securității și gestionarea frontierelor și a migrației;
* actualizează acțiunile comune și urgente lansate în martie 2019 pentru evaluarea și consolidarea **securității rețelelor 5G**, pornind de la evaluările naționale ale riscurilor prezentate de statele membre până la 15 iulie 2019;
* răspunde unui pachet de patru rapoarte referitoare la **combaterea spălării banilor**, adoptat de Comisie la 24 iulie 2019, care analizează riscurile și vulnerabilitățile actuale legate de spălarea banilor și evaluează modul în care cadrul de reglementare relevant al UE este aplicat în prezent în sectorul privat și public;
* oferă informații actualizate cu privire la progresele înregistrate din martie 2019[[3]](#footnote-4) până în prezent în ceea ce privește punerea în aplicare a măsurilor legislative legate de uniunea securității, interoperabilitatea sistemelor de informații fiind una dintre principalele priorități care trebuie puse în aplicare rapid și integral de către statele membre;
* face un bilanț al acțiunilor în curs în vederea combaterii dezinformării și a protejării alegerilor în fața amenințărilor facilitate de tehnologiile informatice, al eforturilor de îmbunătățire a gradului de pregătire și a protecției în fața amenințărilor la adresa securității, precum și al cooperării cu partenerii internaționali cu privire la aspectele legate de securitate.

**II. PROGRESELE ÎNREGISTRATE ÎN CEEA CE PRIVEȘTE PRIORITĂȚILE LEGISLATIVE**

*1. Prevenirea radicalizării online și în cadrul comunităților*

Prevenirea radicalizării, atât în mediul online, cât și în sânul comunităților noastre, este o axă centrală a răspunsului UE la terorism.

Atacul oribil care a avut loc la 15 martie 2019 la Christchurch, în Noua Zeelandă, a fost un avertisment teribil cu privire la modul în care internetul poate fi exploatat în scopuri teroriste, indiferent de ideologia extremistă, fie ea jihadism, extremă dreaptă sau alte ideologii extremiste, care motivează astfel de acțiuni. Viteza și amploarea cu care înregistrarea video a atacului de la Christchurch transmisă în live streaming prin internet a fost circulată pe platformele online au subliniat cât este de important ca platformele de internet să ia măsuri corespunzătoare pentru a împiedica propagarea rapidă a unui astfel de conținut.

Ca reacție la această situație, șefii de stat sau de guvern ai unor state membre și țări terțe, președintele Juncker și platformele online au sprijinit, la 15 mai 2019, „**Apelul la acțiune în urma atentatului de la Christchurch**[[4]](#footnote-5)”, care stabilește acțiunile colective menite să elimine conținutul online cu caracter terorist și extremist violent. Noi angajamente în acest sens au fost asumate de către G7[[5]](#footnote-6) și G20[[6]](#footnote-7).

Comisia a abordat deja pericolul clar și prezent pe care îl reprezintă conținutul online cu caracter terorist în cadrul **propunerii legislative** pe care președintele Juncker a anunțat-o în discursul său privind starea Uniunii din 2018, care propunea un cadru juridic clar și armonizat, menit să prevină utilizarea necorespunzătoare a serviciilor oferite de furnizorii de servicii de găzduire pentru diseminarea de conținut online cu caracter terorist[[7]](#footnote-8). Măsurile propuse ar obliga platformele de internet să elimine conținutul cu caracter terorist în termen de o oră atunci când primesc un ordin de eliminare a unui astfel de conținut din partea autorităților competente dintr-un stat membru. În plus, în cazul în care o platformă este utilizată pentru diseminarea de conținut cu caracter terorist, aceasta ar avea obligația de a lua măsuri proactive pentru a detecta acest conținut și a împiedica reapariția sa – prevăzând norme și garanții clare în acest sens. Autoritățile din statele membre ar trebui să pună la dispoziția autorităților de asigurare a respectării legii competente în materie resursele necesare pentru a detecta în mod eficace conținutul cu caracter terorist și a emite ordine de eliminare a acestuia.

Acest lucru va permite instituirea la nivelul Uniunii a unui sistem rapid și eficace și va prevedea garanții solide în acest sens, inclusiv mecanisme eficace de tratare a plângerilor și căi de atac judiciare.   
Măsurile propuse vor contribui la garantarea bunei funcționări a pieței unice digitale, sporind în același timp securitatea și încrederea în mediul online și consolidând garanțiile pentru libertatea de exprimare și de informare.

În cadrul Consiliului, miniștrii justiției și ai afacerilor interne au convenit în decembrie 2018 asupra unei abordări generale cu privire la această propunere. În aprilie 2019, Parlamentul European a adoptat poziția sa în prima lectură. **Comisia îi invită pe ambii colegiuitori să înceapă negocierile interinstituționale cu privire la această inițiativă prioritară de eliminare a conținutului cu caracter terorist online cât mai curând posibil**, astfel încât să se ajungă rapid la un acord cu privire la un cadru de reglementare al UE care să prevadă norme și garanții clare în materie.

În paralel, Comisia continuă cooperarea cu platformele online în cadrul **Forumului UE pentru internet[[8]](#footnote-9)**. Așa cum anunța președintele Juncker în cadrul reuniunii de la Paris din 15 mai 2019 cu privire la „Apelul la acțiune în urma atentatului de la Christchurch”, Comisia, împreună cu Europol, a început să lucreze la elaborarea unui **protocol UE pentru situații de criză** pentru a permite guvernelor și platformelor de internet să răspundă rapid și într-o manieră coordonată la diseminarea de conținut online cu caracter terorist, de exemplu în perioada imediat următoare unui atac terorist. Această inițiativă se înscrie în contextul eforturilor depuse la nivel internațional pentru punerea în aplicare a „Apelului la acțiune în urma atentatului de la Christchurch”. Pe lângă discuțiile ulterioare inițiate cu statele membre și cu reprezentanții sectorului și exercițiul de simulare planificat pentru luna septembrie 2019 în cadrul căruia ar urma să fie simulată o situație de urgență, Comisia va convoca la 7 octombrie 2019 o reuniune ministerială a Forumului UE pentru internet în vederea aprobării protocolului UE pentru situații de criză.

În plus, Comisia își continuă eforturile de **sprijinire a statelor membre și a actorilor locali în eforturile de prevenire și combatere a radicalizării** pe teren, în sânul comunităților locale din întreaga Europă. Acest lucru necesită eforturi susținute pe termen lung care să îi implice pe toți actorii relevanți de la nivel local, național și de la nivelul UE. **Comitetul director pentru acțiunile Uniunii din domeniul prevenirii și combaterii radicalizării** înființat în luna august 2018 pentru a oferi consultanță Comisiei cu privire la modul în care poate fi consolidată strategia UE în acest domeniu, a organizat cea de a doua reuniune a sa la 17 iunie 2019 pentru a analiza noi acțiuni care ar putea fi întreprinse în domenii prioritare precum radicalizarea în închisori și combaterea ideologiilor extremiste. Având în vedere că practicienii din prima linie și cei de pe teren sunt cei mai în măsură să identifice semnalele timpurii de alarmă în privința radicalizării și modalitățile de contracarare a acestora, **Rețeaua pentru sensibilizarea publicului cu privire la radicalizare**[[9]](#footnote-10), finanțată de UE, continuă să sprijine personalul care intervine în prima linie, punând în legătură aproximativ 5 000 de practicieni din societatea civilă, din școli și din poliție, precum și coordonatori naționali și factori de decizie.

Colaborarea recentă dintre practicienii din prima linie în cadrul rețelei a condus la o înțelegere mai profundă a provocărilor reprezentate de extremismul de dreapta. Anul acesta, Rețeaua pentru sensibilizarea publicului cu privire la radicalizare va publica fișe informative pentru a-i ajuta pe factorii de decizie și pe practicieni să identifice principalele forme și manifestări ale extremismului de dreapta și ale extremismului islamist, cum ar fi tipurile de discurs, limbajul, formele, simbolurile, tipologiile și strategiile cele mai reprezentative ale acestora. În cele din urmă, întrucât actorii locali și **orașele** se află în prima linie în ceea ce privește prevenirea și combaterea radicalizării, Comisia sprijină inițiativele conduse de orașe în materie de combatere a radicalizării. În urma unei conferințe privind „Orașele UE în lupta împotriva radicalizării”, care a avut loc la 26 februarie 2019, un grup-pilot de aproximativ 20 de orașe a organizat la 8 iulie 2019 o primă reuniune, găzduită de primarul orașului Strasbourg, menită să intensifice schimbul de bune practici și să sporească eforturile orașelor în acest domeniu.

În paralel, sunt în curs de desfășurare activități de sprijinire a țărilor partenere în combaterea radicalizării care poate duce la terorism, inclusiv în penitenciare.

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

|  |
| --- |
| * să inițieze negocieri cu privire la propunerea legislativă de prevenire a diseminării **conținutului online cu caracter terorist**, astfel încât să se ajungă la un acord rapid cu privire la un cadru de reglementare al UE care să includă norme și garanții clare. |

*2.      Consolidarea securității cibernetice*

Securitatea cibernetică rămâne o provocare majoră pentru securitate. UE a înregistrat progrese importante[[10]](#footnote-11) în ceea ce privește combaterea amenințărilor cibernetice „clasice” la adresa sistemelor și a datelor, punând în aplicare acțiunile prevăzute în Comunicarea comună din septembrie 2017[[11]](#footnote-12) intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE”. Printre aceste acțiuni se numără și Legea privind securitatea cibernetică a UE[[12]](#footnote-13), care conferă Agenției Uniunii Europene pentru Securitate Cibernetică un mandat permanent, consolidând rolul acesteia și instituind un cadru al UE de certificare de securitate cibernetică. Comisia a răspuns, de asemenea, cerințelor specifice ale sectorului, de exemplu prin intermediul Recomandării sale privind securitatea cibernetică în sectorul energetic, adoptată la 3 aprilie 2019[[13]](#footnote-14). Însă faptul că există o activitate tot mai susținută a unor actori răuvoitori și un evantai larg de ținte și victime ale acestora înseamnă că eforturile de combatere a criminalității cibernetice și de consolidare a securității cibernetice rămân o prioritate a acțiunilor UE.

Parlamentul European și Consiliul nu au ajuns încă la un acord cu privire la inițiativa prioritară a Comisiei privind **Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare**[[14]](#footnote-15). Propunerea urmărește să sprijine capacitățile tehnologice și industriale din domeniul securității cibernetice și să sporească competitivitatea industriei securității cibernetice a Uniunii. Ambii colegiuitori și-au adoptat mandatele de negociere în martie 2019. Întrucât nu a fost posibil să se încheie negocierile interinstituționale înainte de sfârșitul mandatului anterior al Parlamentului European, acesta a adoptat în mod oficial poziția sa în primă lectură. Între timp, continuă discuțiile dintre statele membre în cadrul Consiliului, cu un accent deosebit pe interacțiunea dintre Propunerea de regulament de instituire a Centrului de competențe în materie de securitate cibernetică și a rețelei aferente, pe de o parte, și programele Orizont Europa și Europa digitală, pe de altă parte. **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.**

Între timp, Comisia continuă să **sprijine cercetarea și inovarea** în domeniul securității cibernetice, punând la dispoziție 135 de milioane EUR în cadrul financiar multianual actual pentru proiecte în domenii precum securitatea cibernetică în infrastructurile critice, gestionarea inteligentă a securității și a vieții private și instrumentele elaborate în mod specific pentru cetățeni și pentru întreprinderile mici și mijlocii[[15]](#footnote-16). În iulie 2019, Comisia a lansat o nouă cerere de propuneri în cadrul programului Mecanismul pentru interconectarea Europei, punând la dispoziție fonduri UE în valoare de 10 milioane EUR pentru actorii-cheie identificați de Directiva privind securitatea rețelelor și a sistemelor informatice (Directiva NIS)[[16]](#footnote-17), cum ar fi echipele europene de intervenție în caz de incidente de securitate informatică, operatorii de servicii esențiale (de exemplu, bănci, spitale, furnizori de utilități, companii feroviare, companii aeriene, furnizori de nume de domeniu) și diversele autorități publice. Pentru prima dată, autoritățile europene de certificare de securitate cibernetică sunt, de asemenea, eligibile să își manifeste interesul pentru acest program, ceea ce le va permite să pună în aplicare Legea UE privind securitatea cibernetică.

La 17 mai 2019, Consiliul a instituit un **regim de sancțiuni** care permite UE să impună măsuri restrictive specifice pentru a descuraja atacurile cibernetice care constituie o amenințare externă la adresa UE și a statelor sale membre și pentru a răspunde unor astfel de atacuri. Noul regim de sancțiuni face parte din **Setul de instrumente ale UE pentru diplomația cibernetică**[[17]](#footnote-18), un cadru pentru un răspuns diplomatic comun al UE la activitățile cibernetice răuvoitoare[[18]](#footnote-19) care permite UE să valorizeze pe deplin gama de măsuri disponibile în cadrul politicii externe și de securitate comune pentru descurajarea și combaterea activităților cibernetice răuvoitoare.

Dincolo de amenințările cibernetice la adresa sistemelor și a datelor, UE ia, de asemenea, măsuri pentru a răspunde provocărilor complexe și multidimensionale generate de **amenințările hibride**[[19]](#footnote-20). Consiliul European, în concluziile sale din 21 iunie 2019[[20]](#footnote-21), a subliniat faptul că *„UE trebuie să asigure un răspuns coordonat la amenințările hibride și la amenințările cibernetice și să își consolideze cooperarea cu actorii internaționali relevanți”*. Comisia salută faptul că acțiunile de contracarare a amenințărilor hibride sunt o prioritate și pentru președinția finlandeză a Consiliului și că, în cadrul reuniunii informale a miniștrilor justiției și afacerilor interne de la Helsinki, care a avut loc în perioada 18-19 iulie 2019, s-a purtat o discuție strategică bazată pe scenarii referitoare la amenințările hibride. Discuții similare bazate pe scenarii referitoare la amenințările hibride au avut loc între directorii UE în materie de politici de apărare în perioada 7-8 iulie 2019 și între directorii politici ai UE în perioada 9-10 iulie 2019, al căror rezultat va fi raportat miniștrilor afacerilor externe și apărării în cadrul unei sesiuni informale comune desfășurate în perioada 29-30 august 2019.

**Pentru a consolida securitatea cibernetică, Comisia îndeamnă Parlamentul European și Consiliul:**

|  |
| --- |
| * să ajungă rapid la un acord cu privire la propunerea legislativă privind **Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și Rețeaua de centre naționale de coordonare**. |

*3.*      *Îmbunătățirea accesului autorităților de asigurare a respectării legii la probele electronice*

UE a luat măsuri suplimentare pentru a-i împiedica pe teroriști și pe infractori să acționeze, îngreunându-le accesul la precursorii de explozivi[[21]](#footnote-22) și la sursele prin care își finanțează activitățile[[22]](#footnote-23) și împiedicând, de asemenea, deplasarea acestora fără a fi detectați[[23]](#footnote-24).

Negocierile cu privire la propunerile Comisiei din aprilie 2018 de îmbunătățire a **accesului autorităților de asigurare a respectării legii la probele electronice** ar trebui finalizate cât mai curând posibil – mai mult de jumătate dintre toate anchetele penale presupun în prezent o cerere transfrontalieră de acces la probe electronice[[24]](#footnote-25). Consiliul a adoptat poziția sa de negociere cu privire la Propunerea de regulament[[25]](#footnote-26) privind îmbunătățirea accesului transfrontalier la probele electronice în cadrul anchetelor penale și cu privire la Propunerea de directivă[[26]](#footnote-27) de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul obținerii de probe în cadrul procedurilor penale. Având în vedere importanța crucială a accesului eficient la probe electronice pentru anchetarea și urmărirea penală a infracțiunilor transfrontaliere, cum ar fi terorismul sau criminalitatea informatică, Comisia îndeamnă Parlamentul European să facă progrese în privința acestei propuneri astfel încât colegiuitorii să o poată adopta rapid.

În paralel, Comisia lucrează la îmbunătățirea și asigurarea garanțiilor necesare în cadrul **schimbului internațional de probe electronice** în contextul negocierilor în curs privind un al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică, precum și cu Statele Unite, în conformitate cu mandatele de negociere acordate de Consiliu în cadrul reuniunii Consiliului Justiție și Afaceri Interne din 6­7 iunie 2019[[27]](#footnote-28). Comisia a participat la ultima rundă de negocieri privind un al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică din 9-11 iulie 2019. Comisia și autoritățile Statelor Unite se pregătesc în prezent la nivel tehnic pentru lansarea oficială a negocierilor pentru un acord UE­SUA privind accesul transfrontalier la probele electronice.

**Pentru a îmbunătăți accesul autorităților de asigurare a respectării legii la probele electronice, Comisia invită Parlamentul European:**

|  |
| --- |
| * să își adopte mandatul de negociere cu privire la propunerile legislative privind **probele electronice** pentru a începe rapid discuțiile în cadrul trilogului cu Consiliul. *(prioritate stabilită în Declarația comună)* |

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

În urma adoptării de norme privind **interoperabilitatea sistemelor de informații**[[28]](#footnote-29) care vor elimina lacunele în materie de informații și „unghiurile moarte” prin faptul că vor permite detectarea identităților multiple și combaterea fraudei de identitate, Comisia a lansat rapid o serie de inițiative menite să sprijine statele membre în procesul de punere în aplicare, inclusiv prin finanțare acolo unde este necesar, precum și prin ateliere de lucru care să faciliteze schimbul de expertiză și de cele mai bune practici. 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.

Pentru ca acest obiectiv să fie atins, este, de asemenea, nevoie să se pună în aplicare cu rapiditate și integral legislația recent adoptată de instituire a unor noi sisteme de informații – sistemul de intrare/ieșire al UE[[29]](#footnote-30) și Sistemul european de informații și de autorizare privind călătoriile[[30]](#footnote-31) –, precum și să se consolideze Sistemul de informații Schengen[[31]](#footnote-32) și să se extindă Sistemul european de informații cu privire la cazierele judiciare[[32]](#footnote-33) pentru a-i include pe resortisanții țărilor terțe. Noua arhitectură pentru sisteme de informații mai puternice și mai inteligente în materie de asigurare a securității și de gestionare a frontierelor și a migrației va da rezultate pe teren numai dacă toate componentele sunt puse în aplicare integral la nivelul Uniunii și de către fiecare stat membru, în conformitate cu calendarul convenit.

În același timp, colegiuitorii trebuie să ia măsuri suplimentare pentru a finaliza activitatea începută legată de dezvoltarea unor sisteme de informații mai puternice și mai inteligente pentru asigurarea securității și gestionarea frontierelor și a migrației.   
Ca parte a punerii în aplicare din punct de vedere tehnic a **Sistemului european de informații și de autorizare privind călătoriile**, Comisia a prezentat, la 7 ianuarie 2019, două propuneri care prevăd o serie de modificări tehnice la regulamentul în materie[[33]](#footnote-34) ce sunt necesare pentru ca sistemul să fie pe deplin operațional. Comisia îi invită pe colegiuitori să își intensifice activitatea cu privire la modificările tehnice pentru a ajunge la un acord cât mai curând posibil, permițând astfel punerea în aplicare rapidă și în timp util a Sistemului european de informații și de autorizare privind călătoriile, astfel încât acesta să devină operațional la începutul anului 2021.

În mai 2018, Comisia a prezentat o propunere de **consolidare a actualului Sistem de informații privind vizele**[[34]](#footnote-35) care prevede verificări mai amănunțite ale antecedentelor solicitanților de viză și eliminarea lacunelor în materie de informații prin îmbunătățirea schimbului de informații între statele membre.   
La 19 decembrie 2018, Consiliul și-a adoptat mandatul de negociere, iar, la 13 martie 2019, plenul Parlamentului European a votat raportul referitor la această propunere, încheind astfel prima sa lectură. Comisia solicită începerea rapidă a negocierilor dintre colegiuitori în cadrul nou-constituitei legislaturi a Parlamentului European.

În mai 2016, Comisia a propus extinderea sferei de acțiune a **Eurodac**[[35]](#footnote-36) pentru a include identificarea nu numai a solicitanților de azil, ci și a resortisanților țărilor terțe aflați în situație de ședere ilegală și a celor care intră în UE în mod neregulamentar. În conformitate cu concluziile Consiliului European din decembrie 2018[[36]](#footnote-37) și cu Comunicarea Comisiei din 6 martie 2019 privind progresele înregistrate în punerea în aplicare a Agendei europene privind migrația[[37]](#footnote-38), Comisia invită colegiuitorii să adopte propunerea. Este necesar să se adopte această propunere legislativă pentru a permite Eurodac să devină parte a viitoarei arhitecturi a sistemelor de informații interoperabile la nivelul UE, în care sunt astfel integrate datele esențiale ale resortisanților țărilor terțe aflați în situație de ședere ilegală și ale celor care au intrat în UE în mod neregulamentar.

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

|  |
| --- |
| * să adopte propunerea legislativă privind **Eurodac** *(prioritate stabilită în Declarația comună)*; * să își intensifice activitatea în vederea ajungerii la un acord rapid cu privire la modificările tehnice propuse care sunt necesare pentru instituirea **Sistemului european de informații și de autorizare privind călătoriile**. |

**III. CONSOLIDAREA SECURITĂȚII INFRASTRUCTURILOR DIGITALE**

Reziliența infrastructurii noastre digitale este esențială pentru guverne, pentru întreprinderi, pentru securitatea datelor noastre cu caracter personal și pentru funcționarea instituțiilor noastre democratice. **Rețelele de a cincea generație (5G)** care vor fi instalate în următorii ani vor constitui coloana vertebrală digitală a societăților și a economiilor noastre, conectând miliarde de cetățeni, obiecte și sisteme, inclusiv în sectoare critice, cum ar fi energia, transporturile, sectorul bancar și medical, precum și sistemele de control industrial care transmit informații sensibile și sprijină sistemele de siguranță.

Cu un nivel al veniturilor generate la nivel mondial estimat la 225 de miliarde EUR în 2025, tehnologia 5G reprezintă un atu esențial pentru asigurarea competitivității Europei pe piața mondială, iar **securitatea rețelelor 5G este crucială pentru asigurarea autonomiei strategice a Uniunii**. Asigurarea unui nivel ridicat de securitate cibernetică necesită luarea de măsuri concertate atât la nivel național, cât și la nivel european, întrucât orice vulnerabilitate a rețelelor 5G dintr-un stat membru ar afecta întreaga Uniune.

Având în vedere sprijinul exprimat de șefii de stat sau de guvern cu ocazia Consiliului European din luna martie 2019[[38]](#footnote-39), Comisia a prezentat la 26 martie 2019 o **Recomandare privind securitatea cibernetică a rețelelor 5G**[[39]](#footnote-40), care stabilește acțiunile prin care să se evalueze riscurile la adresa securității cibernetice asociate rețelelor 5G și să se consolideze măsurile preventive. Recomandările se bazează pe măsuri coordonate la nivelul UE de evaluare și gestionare a riscurilor, pe un cadru eficace de cooperare și schimb de informații și pe o conștientizare comună a situației în UE a rețelelor de comunicații critice.

Ca **primă etapă** a procesului inițiat de recomandare, toate statele membre și-au finalizat, până la 15 iulie 2019, **evaluarea națională a riscurilor** și au prezentat Comisiei și Agenției UE pentru Securitate Cibernetică constatările lor sau au anunțat că vor face acest lucru în scurt timp. Evaluările naționale ale riscurilor au fost elaborate pe baza unui set de orientări și a unui model comun de raportare a constatărilor care au fost convenite de statele membre și de Comisie cu scopul de a se promova coerența și a se facilita schimbul de informații cu privire la rezultatele naționale la nivelul UE. Parametrii evaluați în toate statele membre au inclus:

* principalele amenințări și principalii factori de amenințare care au un impact asupra rețelelor 5G;
* gradul de sensibilitate a componentelor și a funcțiilor rețelei 5G, precum și a altor active și
* diferitele tipuri de vulnerabilități, inclusiv cele tehnice, cum ar fi cele care ar putea rezulta din lanțul de aprovizionare 5G.

În plus, la realizarea evaluărilor naționale ale riscurilor au participat diferite organisme competente din statele membre, inclusiv, în funcție de responsabilitățile naționale, autorități din domeniul securității cibernetice, al telecomunicațiilor, al serviciilor de securitate și de informații, ceea ce a consolidat cooperarea și coordonarea între aceștia. În paralel și având în vedere calendarele naționale pentru implementarea tehnologiei 5G, o serie de state membre au luat deja măsuri pentru a consolida cerințele de securitate aplicabile în acest domeniu, în timp ce alte câteva state membre și-au exprimat intenția de a avea în vedere adoptarea unor măsuri noi în viitorul apropiat.

Pe baza rezultatelor evaluărilor naționale ale riscurilor, autoritățile competente în materie de securitate cibernetică din statele membre care participă la Grupul de cooperare în materie de securitate a rețelelor și a sistemelor informatice[[40]](#footnote-41) vor pregăti, până la 1 octombrie 2019, o **evaluare comună a riscurilor la nivelul UE**, care va reprezenta cea de a doua etapă a procesului inițiat în baza recomandării. Pe baza rezultatului acesteia și ca o a treia etapă, grupul de cooperare va pregăti, până la 31 decembrie 2019, un **instrumentar comun al Uniunii cu măsuri de atenuare** menite să abordeze riscurile identificate. Comisia și Agenția UE pentru Securitate Cibernetică vor continua să sprijine punerea în aplicare a recomandării.

Activitatea din cadrul Grupului de cooperare în materie de securitate a rețelelor și a sistemelor informatice este sprijinită de alte câteva foruri. Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice pregătește un sondaj cu privire la toate măsurile de securitate aplicate în prezent care pot fi relevante pentru 5G. Un nou grup specializat de experți în domeniul securității cibernetice din cadrul Agenției UE pentru Securitate Cibernetică a lansat o serie de activități care să cartografieze amenințările pe care le prezintă rețelele 5G. În plus, în urma intrării în vigoare, la 27 iunie 2019, a Legii privind securitatea cibernetică Comisia și Agenția UE pentru Securitate Cibernetică vor lua toate măsurile necesare pentru a institui cadrul de certificare la nivelul UE. De asemenea, statele membre s-au reunit în cadrul Comitetului pentru standarde în iunie 2019 pentru a discuta despre securitatea cibernetică și standardizare ca răspuns la recomandarea de a explora viitoarele provocări la adresa standardizării în domeniul securității cibernetice, inclusiv în rețelele 5G, și despre inițiativele politice potrivite la nivelul UE.

În ultimă instanță, securitatea rețelelor 5G are o importanță strategică pentru Uniune. Investițiile străine în sectoare strategice, achiziționarea de active, tehnologii și infrastructuri critice în Uniune și furnizarea de echipamente critice pot, de asemenea, reprezenta riscuri la adresa securității Uniunii.

Noul **cadru al UE pentru examinarea investițiilor străine directe**[[41]](#footnote-42) a intrat în vigoare la 10 aprilie 2019. În următoarele 18 luni, Comisia și statele membre vor face demersurile necesare pentru a se asigura că UE poate aplica pe deplin Regulamentul pentru examinarea investițiilor începând cu 11 octombrie 2020.

**IV. COMBATEREA SPĂLĂRII BANILOR**

Capacitatea membrilor rețelelor infracționale și a teroriștilor de a transfera fonduri dintr-un cont bancar în altul în numai câteva ore le permite acestora să își pregătească mai ușor actele teroriste sau să spele în mod ilegal produsele provenite din săvârșirea de infracțiuni în diferite state membre. Pentru a aborda această problemă, Uniunea a elaborat un **cadru de reglementare solid pentru combaterea spălării banilor și a finanțării terorismului**, în conformitate cu standardele internaționale adoptate de Grupul de Acțiune Financiară Internațională.

Având în vedere necesitatea de a ține pasul cu evoluția tendințelor, cu evoluțiile tehnologice și cu ingeniozitatea infractorilor în a exploata eventualele lacune sau probleme din sistem, Comisia a adoptat, la 24 iulie 2019, **un pachet de patru rapoarte** în care sunt analizate riscurile și vulnerabilitățile actuale legate de spălarea banilor și este evaluat modul în care este aplicat cadrul în vigoare de către actorii relevanți din sectorul privat și din cel public[[42]](#footnote-43).

Pachetul include o **evaluare a potențialului de interconectare a registrelor naționale centralizate de conturi bancare** **și a sistemelor de extragere a datelor** în UE. Astfel de sisteme naționale centralizate permit identificarea oricărei persoane fizice sau juridice care deține sau controlează conturi de plăți, conturi bancare și casete de valori – informații adesea esențiale pentru autoritățile competente în lupta împotriva spălării banilor și a finanțării terorismului. Cea de a cincea Directivă privind combaterea spălării banilor[[43]](#footnote-44) impune statelor membre obligația de a institui astfel de sisteme naționale centralizate și de a oferi unităților lor naționale de informații financiare accesul direct la sistemele respective. Normele recent adoptate de facilitare a utilizării informațiilor financiare pentru combaterea formelor grave de criminalitate[[44]](#footnote-45) furnizează autorităților de asigurare a respectării legii și birourilor de recuperare a activelor desemnate accesul direct la registrele lor naționale centralizate de conturi bancare. Pe baza celor de mai sus și în conformitate cu cerințele prevăzute în Directiva privind combaterea spălării banilor, raportul evaluează diferitele soluții IT la nivelul UE care fie sunt deja operaționale, fie sunt în curs de a fi dezvoltate și care pot servi drept model pentru o posibilă interconectare a sistemelor naționale centralizate. Având în vedere că o viitoare interconectare la nivelul UE a mecanismelor centralizate ar accelera accesul la informațiile financiare și ar facilita cooperarea transfrontalieră a autorităților competente, Comisia intenționează să se consulte în continuare cu părțile interesate relevante, cu guvernele, precum și cu unitățile de informații financiare, cu autoritățile de asigurare a respectării legii și cu birourile de recuperare a activelor, ca potențiali „utilizatori finali” ai unui eventual sistem interconectat.

Ca parte a procesului de reflecție al Comisiei cu privire la activitatea unităților de informații financiare, un raport de evaluare a **cooperării dintre unitățile de informații financiare** analizează atât cooperarea în cadrul Uniunii, cât și cooperarea cu țările terțe[[45]](#footnote-46). Acesta identifică anumite deficiențe care ar putea continua să existe până când sarcinile și obligațiile de cooperare transfrontalieră ale unităților de informații financiare vor fi precizate mai clar în cadrul juridic al UE privind combaterea spălării banilor și a finanțării terorismului. Evaluarea evidențiază, de asemenea, necesitatea unui mecanism mai solid de coordonare și sprijinire a cooperării și analizei transfrontaliere.

Dincolo de activitatea curentă de combatere a spălării banilor și a finanțării terorismului și ca răspuns la îndemnul lansat în acest sens de Parlamentul European[[46]](#footnote-47), Comisia va continua să evalueze necesitatea, fezabilitatea tehnică și proporționalitatea adoptării unor măsuri suplimentare de urmărire a finanțărilor în scopuri teroriste în UE[[47]](#footnote-48).

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

*1.      Punerea în aplicare a măsurilor legislative legate de uniunea securității*

Ajungerea la un acord cu privire la măsurile legate de uniunea securității nu este punctul final al procesului, ceea ce este esențial este să se asigure ulterior punerea în aplicare rapidă și integrală a măsurilor respective de către statele membre, astfel încât să putem beneficia pe deplin de avantajele acestei uniuni. În acest scop, Comisia sprijină în mod activ statele membre, inclusiv prin finanțare și prin facilitarea schimbului de bune practici.   
Dacă este necesar, Comisia este însă pregătită și să recurgă la toate mijloacele de care dispune în temeiul tratatelor pentru a asigura respectarea legislației UE, inclusiv la proceduri de constatare a neîndeplinirii obligațiilor, atunci când este cazul.

Termenul pentru punerea în aplicare a **Directivei privind registrul UE cu numele pasagerilor**[[48]](#footnote-49) a expirat la 25 mai 2018. Până în prezent, 25 de state membre au notificat Comisiei transpunerea integrală a directivei[[49]](#footnote-50). Aceasta nu a fost transpusă integral în două state membre, în ciuda procedurilor de constatare a neîndeplinirii obligațiilor lansate la 19 iulie 2018[[50]](#footnote-51). 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 bune practici.

Termenul de transpunere a **Directivei privind combaterea terorismului**[[51]](#footnote-52) a expirat la 8 septembrie 2018. Până în prezent, 22 de state membre au notificat Comisiei transpunerea integrală a directivei. Trei state membre nu au comunicat încă adoptarea legislației naționale care transpune integral directiva, în ciuda procedurilor de constatare a neîndeplinirii obligațiilor lansate la 22 noiembrie 2018[[52]](#footnote-53).

Termenul pentru transpunerea **Directivei privind controlul achiziționării și deținerii de arme**[[53]](#footnote-54) a expirat la 14 septembrie 2018. Până în prezent, 8 state membre au notificat Comisiei transpunerea integrală a directivei. 20 de state membre nu au comunicat încă adoptarea legislației naționale care transpune integral directiva, în ciuda procedurilor de constatare a neîndeplinirii obligațiilor lansate la 22 noiembrie 2018[[54]](#footnote-55).

În ceea ce privește transpunerea în legislația națională a **Directivei privind protecția datelor în materie de asigurare a respectării legii**[[55]](#footnote-56), termenul de transpunere a expirat la 6 mai 2018. Până în prezent, 20 de state membre au notificat Comisiei transpunerea integrală a directivei[[56]](#footnote-57). 7 state membre nu au comunicat încă adoptarea legislației naționale care transpune integral directiva, în ciuda procedurilor de constatare a neîndeplinirii obligațiilor lansate de Comisie la 19 iulie 2018[[57]](#footnote-58).

Statele membre au avut obligația de a transpune **Directiva privind securitatea rețelelor și a sistemelor informatice[[58]](#footnote-59)** în legislația lor națională până la 9 mai 2018. Până în prezent, 26 de state membre au notificat Comisiei transpunerea integrală, iar 2 state membre au transpus parțial directiva[[59]](#footnote-60). În plus, până la 9 noiembrie 2018, statelor membre li s-a solicitat să identifice operatorii de servicii esențiale în conformitate cu directiva. Până la 9 mai 2019, Comisia trebuia să prezinte Parlamentului European și Consiliului un raport de evaluare a coerenței abordării în ceea ce privește identificarea operatorilor de servicii esențiale repertoriați pe teritoriul lor. Însă, întrucât mai multe state membre nu au prezentat încă informații complete privind procesul de identificare, Comisia a trebuit să își amâne raportul.

Comisia evaluează transpunerea celei de **A patra directive privind combaterea spălării banilor**[[60]](#footnote-61) și, în același timp, verifică dacă normele respective sunt puse în aplicare de către statele membre. Comisia a inițiat proceduri de constatare a neîndeplinirii obligațiilor împotriva a 24 de state membre, deoarece a considerat că statele membre au transmis comunicări care nu reprezintă o transpunere integrală a directivei[[61]](#footnote-62).

**Comisia invită statele membre să ia de urgență măsurile necesare pentru transpunerea integrală a următoarelor directive în legislația națională și să le comunice Comisiei:**

|  |
| --- |
| * **Directiva privind registrul UE cu numele pasagerilor**, în cazul căreia 1 stat membru nu a notificat încă transpunerea în legislația națională, iar 1 stat membru nu a finalizat notificarea transpunerii[[62]](#footnote-63); * **Directiva privind combaterea terorismului**, în cazul căreia 2 state membre nu au notificat încă transpunerea în legislația națională, iar 1 stat membru nu a finalizat notificarea transpunerii[[63]](#footnote-64); * **Directiva privind controlul achiziționării și deținerii de arme**, în cazul căreia 12 state membre nu au notificat încă transpunerea în legislația națională, iar 8 state membre nu au finalizat notificarea transpunerii[[64]](#footnote-65); * **Directiva privind protecția datelor în materie de asigurare a respectării legii**, în cazul căreia 2 state membre nu au notificat încă transpunerea în legislația națională, iar 5 state membre nu au finalizat notificarea transpunerii[[65]](#footnote-66); * **Directiva privind securitatea rețelelor și a sistemelor informatice**, în cazul căreia 2 state membre nu au finalizat încă notificarea transpunerii[[66]](#footnote-67); și * Cea de **A 4-a directivă privind combaterea spălării banilor**, în cazul căreia 24 de state membre nu au finalizat încă notificarea transpunerii[[67]](#footnote-68). |

*2. Combaterea dezinformării și protejarea alegerilor în fața altor amenințări facilitate de tehnologiile informatice*

Protejarea proceselor și a instituțiilor democratice împotriva dezinformării și a ingerințelor conexe reprezintă o provocare majoră pentru societățile din întreaga lume. Pentru a aborda acest aspect, UE a instituit un **cadru solid de acțiune coordonată împotriva dezinformării**, cu respectarea deplină a valorilor europene și a drepturilor fundamentale[[68]](#footnote-69). După cum se prevede în Comunicarea comună din 14 iunie 2019 privind punerea în aplicare a Planului de acțiune împotriva dezinformării[[69]](#footnote-70), eforturile derulate pe mai multe linii de acțiune complementare au contribuit la reducerea dezinformării și la apărarea integrității alegerilor pentru Parlamentul European.

În concluziile sale din 21 iunie 2019[[70]](#footnote-71), Consiliul European a salutat intenția Comisiei de a realiza o evaluare aprofundată a punerii în aplicare a angajamentelor asumate de către platformele online și alți semnatari în temeiul **Codului de bune practici privind dezinformarea**[[71]](#footnote-72) și a invitat Comisia și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate să evalueze în permanență și să răspundă în mod corespunzător *„*caracterului evolutiv al amenințărilor și riscului tot mai mare de ingerințe răuvoitoare și manipulare online asociate cu dezvoltarea inteligenței artificiale și a tehnicilor de culegere de date”.

Comisia și Înaltul Reprezentant își vor intensifica activitatea în acest domeniu, în conformitate cu concluziile Consiliului European. În luna martie 2019, Comisia și Înaltul Reprezentant au instituit un **sistem de alertă rapidă** între instituțiile UE și statele membre pentru a facilita schimbul de informații privind campaniile de dezinformare și pentru a coordona răspunsurile. Prima reuniune a punctelor de contact ale statelor membre în urma alegerilor pentru Parlamentul European a avut loc la Tallinn în perioada 3-4 iunie 2019. Pentru a consolida în continuare sistemul de alertă rapidă, Înaltul Reprezentant și Comisia, în strânsă cooperare cu statele membre, vor revizui funcționarea sistemului de alertă rapidă în toamna anului 2019. De asemenea, cele două părți vor elabora o metodologie comună pentru analizarea și demascarea campaniilor de dezinformare și vor dezvolta parteneriate mai strânse cu partenerii internaționali, cum ar fi G7 și NATO.

Continuă totodată activitatea în cadrul **Rețelei europene de cooperare privind alegerile**[[72]](#footnote-73), a cărei primă reuniune a avut loc la 7 iunie 2019 pentru a face un bilanț al alegerilor pentru Parlamentul European. Aceste reflecții și contribuțiile suplimentare venite din partea autorităților naționale relevante, a partidelor politice și a platformelor online vor contribui la raportul cuprinzător al Comisiei privind alegerile pentru Parlamentul European, care urmează să fie adoptat în octombrie 2019. Statele membre au utilizat rețeaua pentru alte alegeri decât cele pentru Parlamentul European, ceea ce evidențiază utilitatea sa mai largă în ceea ce privește asigurarea integrității democrației în UE.

De asemenea, Comisia va continua să monitorizeze și să promoveze punerea în aplicare a angajamentelor asumate de către platforme în cadrul **Codului de bune practici privind dezinformarea**.   
Rapoartele furnizate de Google, Twitter și Facebook în temeiul Codului de bune practici arată că toate platformele au luat măsuri înainte de alegerile pentru Parlamentul European prin etichetarea anunțurilor politice și prin punerea acestora la dispoziția publicului prin intermediul bibliotecilor de anunțuri cu funcții de căutare. Mai pot fi aduse însă îmbunătățiri acestui proces, astfel cum a sugerat Grupul autorităților europene de reglementare pentru serviciile mass-media audiovizuale[[73]](#footnote-74). În special, nu s-a dat încă acces la datele brute detaliate necesare pentru o monitorizare cuprinzătoare. În fine, platformele ar trebui să ofere comunității de cercetare un acces util la date, în conformitate cu normele de protecție a datelor cu caracter personal. Mai târziu în cursul acestui an, Comisia va efectua o evaluare cuprinzătoare a punerii în aplicare a tuturor angajamentelor asumate în temeiul Codului de bune practici pe parcursul perioadei inițiale de 12 luni. Pe această bază, Comisia poate avea în vedere întreprinderea unor acțiuni suplimentare, inclusiv de natură normativă, pentru a îmbunătăți răspunsul UE pe termen lung la dezinformare.

*3.    Gradul de pregătire și protecție*

Consolidarea mijloacelor de apărare și a rezilienței împotriva amenințărilor la adresa securității reprezintă un aspect important al eforturilor către o uniune a securității efectivă și autentică. Printre măsurile în acest sens se înscrie și sprijinul oferit de Comisie statelor membre și autorităților lor locale în vederea consolidării **protecției spațiilor publice**[[74]](#footnote-75), precum și sprijinul acordat statelor membre pentru a îmbunătăți pregătirea acestora în fața **riscurilor în materie de siguranță chimică, biologică, radiologică și nucleară**[[75]](#footnote-76), punerea în aplicare a celor două planuri de acțiune în acest domeniu, precum și analizarea nevoilor de capacități de răspuns în domeniu care să fie dezvoltate în cadrul rescEU[[76]](#footnote-77). În ceea ce privește evoluția amenințărilor la adresa siguranței chimice[[77]](#footnote-78), în cooperare cu statele membre și în consultare cu partenerii internaționali, Comisia a elaborat o listă de substanțe chimice care suscită cea mai mare preocupare din perspectiva posibilității utilizării lor în scopuri teroriste. Lista UE servește drept bază pentru continuarea eforturilor de reducere a accesibilității acestor substanțe chimice și pentru colaborarea cu producătorii în vederea îmbunătățirii capacităților de detectare a acestor substanțe.

Tehnologiile pentru aeronavele fără pilot la bord permit o gamă largă de operațiuni posibile. Cu o expansiune rapidă în ultimii ani pe piața sistemelor de aeronave fără pilot la bord pentru scopuri militare, comerciale civile și recreative, dronele reprezintă o oportunitate, dar și o amenințare din ce în ce mai mare la adresa securității infrastructurilor critice (inclusiv a aviației), a spațiilor publice și a evenimentelor, a siturilor sensibile și a persoanelor. În Europa, dronele au fost utilizate pentru a perturba operațiuni aviatice și de asigurare a respectării legii, pentru a supraveghea infrastructura critică și pentru a face contrabandă în închisori și la nivel transfrontalier.

Comisia sprijină statele membre în combaterea amenințării tot mai mari pe care o reprezintă dronele pentru cetățeni și funcțiile societale critice, fără a elimina utilizarea lor benefică, de exemplu în cadrul operațiunilor de răspuns în situații de urgență. Comisia a adoptat recent **norme comune la nivelul UE privind operarea în siguranță a dronelor**[[78]](#footnote-79) pentru a atenua riscul utilizării lor în scopuri răuvoitoare, norme care includ dispoziții ce impun înregistrarea operatorilor și permit identificarea de la distanță. În plus, Comisia sprijină statele membre prin monitorizarea tendințelor de evoluție a amenințării reprezentate de drone, prin finanțarea unor proiecte de cercetare relevante și a unor măsuri de consolidare a capacităților, precum și prin facilitarea schimburilor între statele membre și alte părți interesate. Pentru a-și intensifica sprijinul în acest sens, Comisia va organiza la 17 octombrie 2019 o conferință internațională la nivel înalt menită să contracareze riscurile reprezentate de drone.

Ca răspuns la necesitatea de a avea o perspectivă largă asupra politicii UE privind **protejarea infrastructurilor critice**[[79]](#footnote-80), Comisia a prezentat, la 23 iulie 2019, o evaluare a Directivei privind infrastructurile critice europene[[80]](#footnote-81) care reprezintă cadrul juridic pentru identificarea și desemnarea infrastructurilor critice europene și pentru evaluarea necesității de a îmbunătăți protecția acestora. Evaluarea a constatat, pe de o parte, o evoluție semnificativă a contextului în care funcționează infrastructurile critice din Europa față de momentul intrării în vigoare a directivei, inclusiv în lumina evoluțiilor legislative din sectoarele vizate în mod specific de directivă[[81]](#footnote-82), cum ar fi sectorul energetic, și, pe de altă parte, faptul că, dată fiind această evoluție, dispozițiile directivei sunt în prezent doar parțial relevante. În același timp, există un sprijin susținut din partea statelor membre pentru politica UE în domeniul protecției infrastructurilor critice, care respectă principiul subsidiarității și aduce valoare adăugată.

*4.      Dimensiunea externă*

Având în vedere caracterul transfrontalier și anvergura mondială a majorității amenințărilor la adresa securității cu care se confruntă Uniunea noastră, cooperarea cu organizațiile internaționale și cu țările partenere din afara UE este parte integrantă a eforturilor în direcția unei uniuni a securității efective și autentice.

Valorificarea beneficiilor cooperării multilaterale este o parte integrantă a acestui efort și include cooperarea dintre UE și ONU, astfel cum a fost consolidată recent prin semnarea, la 24 aprilie 2019, la New York, a **cadrului UE-ONU privind combaterea terorismului**, cu ocazia celui de al doilea dialog politic la nivel înalt ONU-UE privind combaterea terorismului[[82]](#footnote-83). Cadrul promovează cooperarea în materie de consolidare a capacităților de combatere a terorismului și de prevenire și combatere a extremismului violent în Africa, Orientul Mijlociu și Asia. Cadrul identifică domeniile de cooperare și prioritățile ONU-UE până în 2020.

**Cooperarea în materie de securitate cu Balcanii de Vest** reprezintă o prioritate regională deosebită, care transpune în realitate o serie de acțiuni prioritare în domeniul securității identificate în Strategia comună privind Balcanii de Vest din 2018[[83]](#footnote-84). În acest scop, la 4 aprilie 2019, Comisia a organizat prima reuniune a Grupului operativ inter-agenții pentru Balcanii de Vest, în cadrul căruia reprezentanții a șapte agenții ale UE și-au împărtășit experiența și au consolidat cooperarea operațională cu partenerii din regiune, inclusiv în lupta împotriva criminalității organizate, a terorismului, a armelor de foc, a traficului de droguri, a introducerii ilegale de migranți și a traficului de persoane. Au fost lansate sondaje privind riscurile hibride cu toate cele șase țări din Balcanii de Vest. Un alt exemplu concret de cooperare cu regiunea îl constituie Acordul privind statutul poliției de frontieră și gărzii de coastă la nivel european încheiat între UE și Albania, care a intrat în vigoare la 1 mai 2019, urmat rapid de trimiterea pe teren a echipelor Agenției Europene pentru Poliția de Frontieră și Garda de Coastă la frontiera cu Grecia. Acesta este primul acord de acest tip încheiat cu o țară terță. Acorduri similare ar trebui semnate în curând cu alte țări din regiune.

În plus, un ofițer de legătură Europol a fost trimis în Albania în iulie 2019 pentru a sprijini în continuare autoritățile albaneze în eforturile lor de prevenire și combatere a criminalității organizate. Pentru a intensifica lupta împotriva traficului cu arme de foc, Comisia a prezentat la 27 iunie 2019 o evaluare a Planului de acțiune 2015-2019 privind **combaterea traficului de arme de foc** între UE și regiunea Europei de Sud-Est[[84]](#footnote-85). Evaluarea demonstrează valoarea adăugată a cooperării, dar subliniază că sunt necesare eforturi suplimentare, de exemplu prin instituirea unor centre naționale de coordonare eficiente privind armele de foc sau prin armonizarea colectării de informații și raportarea cu privire la confiscările de arme de foc.

UE acordă o prioritate egală dezvoltării **cooperării în domeniul securității cu țările din Orientul Mijlociu și din Africa de Nord**. UE a lansat un dialog în materie de securitate cu Tunisia și Algeria. UE și Tunisia au organizat cel de Al treilea dialog în domeniul securității și al combaterii terorismului la 12 iunie la Tunis, în timp ce Al doilea dialog UE-Algeria privind securitatea și combaterea terorismului a avut loc la 12 noiembrie 2018 la Alger. Sunt în curs discuții privind lansarea unui dialog structurat în materie de securitate cu Marocul, în urma recentului Consiliu de asociere din 27 iunie, în cadrul căruia UE și Marocul au recunoscut importanța aprofundării cooperării în materie de securitate pentru a face față provocărilor comune. În paralel, sunt în curs discuții privind dezvoltarea unui dialog structurat în materie de securitate cu Egiptul, astfel cum a fost confirmat, de asemenea, cu ocazia ultimei reuniuni oficiale a înalților funcționari UE-Egipt, care a avut loc la 10 iulie la Cairo.

Pe baza mandatului acordat de Consiliu, Comisia a demarat discuții informale cu majoritatea țărilor din **Orientul Mijlociu și Africa de Nord** în vederea lansării unor negocieri formale pentru un acord internațional privind schimbul de date cu caracter personal între Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (**Europol**) și autoritățile competente relevante din țările din **Orientul Mijlociu și Africa de Nord** în vederea combaterii infracțiunilor grave și a terorismului. În acest context, Comisia promovează, de asemenea, încheierea unor acorduri de lucru direct între Europol și autoritățile partenere din țările din **Orientul Mijlociu și Africa de Nord**, pentru a oferi un cadru formal pentru o cooperare regulată la nivel strategic.

UE și **Statele Unite** sunt parteneri apropiați și strategici în ceea ce privește abordarea amenințărilor comune și consolidarea securității. În cadrul reuniunii miniștrilor justiției și afacerilor interne din 19 iunie 2019, UE și Statele Unite au reafirmat faptul că lupta împotriva terorismului se numără printre principalele lor priorități. În ceea ce privește Acordul UE-SUA privind registrul cu numele pasagerilor[[85]](#footnote-86), ambele părți au reiterat importanța acordului și s-au angajat să înceapă o evaluare comună în septembrie 2019 pentru a evalua punerea sa în aplicare, în conformitate cu dispozițiile acordului. Ambele părți s-au angajat, de asemenea, să își intensifice eforturile comune de combatere a terorismului, inclusiv prin extinderea schimbului de informații colectate în zonele de luptă pentru a fi utilizate în cadrul anchetelor și al urmăririlor penale.

Pentru a intensifica această cooperare, Comisia a găzduit, la 10 iulie 2019, la Bruxelles, împreună cu coordonatorul UE pentru lupta împotriva terorismului, un atelier la nivel înalt privind informațiile din teatrele de luptă. Acesta a reunit înalți funcționari din ministerele apărării, afacerilor interne și justiției din statele membre, Statele Unite, dar și din partea Europol, a Eurojust și reprezentanți ai organizațiilor internaționale pentru a face schimb de opinii cu privire la utilizarea informațiilor din teatrele de luptă și a reflecta împreună asupra provocărilor procedurale, juridice și operaționale cu care se confruntă în prezent, în încercarea de a-i identifica pe teroriști și de a-i aduce în fața justiției. UE și Statele Unite au organizat la Bruxelles, în perioada 14–15 mai 2019, și un Dialog privind consolidarea capacităților în domeniul chimic, biologic, radiologic și nuclear pentru a coordona eforturile în vederea reducerii amenințărilor reprezentate de armele de distrugere în masă și a consolidării securității CBRN în lume.

**Acordul privind Programul de urmărire a finanțărilor în scopuri teroriste încheiat între UE și Statele Unite**[[86]](#footnote-87) este în vigoare din 2010 și reglementează transferul și prelucrarea datelor în scopul identificării, detectării și urmăririi penale a teroriștilor și a rețelelor acestora. Acordul conține garanții care asigură protecția datelor cetățenilor UE și prevede o revizuire periodică a „dispozițiilor privind garanțiile, controalele și reciprocitatea”. Într-un raport periodic de evaluare[[87]](#footnote-88) publicat la 22 iulie 2019, Comisia s-a declarat mulțumită de faptul că acordul, inclusiv garanțiile și controalele sale esențiale, este pus în aplicare în mod corespunzător. UE salută transparența constantă demonstrată de autoritățile americane în ceea ce privește schimbul de informații, ceea de ilustrează valoarea Programului de urmărire a finanțărilor în scopuri teroriste în contextul eforturilor noastre comune de combatere a terorismului. Informațiile furnizate în temeiul acordului au avut un rol esențial în realizarea unor anchete specifice referitoare la atacuri teroriste pe teritoriul european, inclusiv în contextul atacurilor de la Stockholm, Barcelona și Turku din 2017. Statele membre și Europol au apelat într-o măsură mai mare la acest mecanism, iar datele din Programul de urmărire a finanțărilor în scopuri teroriste au generat de șapte ori mai multe piste de anchetă decât în perioada de raportare precedentă. Următoarea revizuire comună a acordului este prevăzută pentru 2021.

În ceea ce privește cooperarea internațională în domeniul schimbului de date din **registrele cu numele pasagerilor în scopul combaterii terorismului și a criminalității grave**, în cadrul celei de a 17-a reuniuni la nivel înalt UE-Canada de la Montreal din 17-18 iulie 2019, UE și Canada au salutat faptul că au încheiat negocierile pentru un nou acord privind registrul cu numele pasagerilor. Canada a luat act de obligația inclusă în acesta referitoare la revizuirea juridică, iar părțile se angajează, sub rezerva acestei revizuiri, să finalizeze acordul cât mai curând posibil, recunoscând rolul esențial al respectivului acord în consolidarea securității și în garantarea respectării vieții private și a protecției datelor cu caracter personal. În ceea ce privește actualul Acord UE-Australia privind registrele cu numele pasagerilor[[88]](#footnote-89), în august 2019 va avea loc la Canberra o vizită a unei echipe a UE în contextul revizuirii comune și al evaluării comune a acordului.

Comisia colaborează, de asemenea, cu statele membre din cadrul Consiliului pe marginea poziției pe care ar urma să o adopte UE în cadrul celei de a 40-a sesiuni a Adunării **Organizației Aviației Civile Internaționale,** care va avea loc în perioada 24 septembrie–4 octombrie 2019. Adunarea va stabili direcția politică și va oferi instrucțiuni Consiliului Organizației Aviației Civile Internaționale cu privire la lucrările tehnice referitoare la standardele Organizației Aviației Civile Internaționale în ceea ce privește prelucrarea datelor din registrul cu numele pasagerilor. Consiliul a aprobat un document de informare elaborat de Comisie care descrie poziția Uniunii cu privire la principiile fundamentale care ar trebui să stea la baza oricărui standard viitor privind registrul mondial cu numele pasagerilor. Documentul de informare va fi prezentat organismului cu referire la membrii săi, alții decât statele membre ale UE.

**VI. CONCLUZII**

Datorită cooperării strânse dintre Parlamentul European, Consiliu, statele membre și Comisie, UE a făcut progrese considerabile în ultimii ani în eforturile comune în direcția unei uniuni a securității efective și autentice, convenind asupra unei serii de inițiative legislative prioritare. Statele membre, cu sprijinul Comisiei, pun, de asemenea, în aplicare o gamă largă de măsuri operaționale nelegislative menite să sporească securitatea pentru toți cetățenii. În același timp, există încă o serie de inițiative prioritare aflate în curs legate de uniunea securității care necesită acțiuni suplimentare din partea colegiuitorilor astfel încât să poată fi abordate amenințările imediate. Comisia invită Parlamentul European și Consiliul să ia măsurile necesare pentru a ajunge rapid la un acord cu privire la propunerile legislative de combatere a propagandei teroriste și a radicalizării online, de îmbunătățire a securității cibernetice, de facilitare a accesului la probele electronice și de finalizare a activității legate de dezvoltarea unor sisteme de informații mai puternice și mai inteligente pentru asigurarea securității și gestionarea frontierelor și a migrației.

Comisia invită statele membre să pună în aplicare rapid și integral toate actele legislative adoptate legate de uniunea securității astfel încât să putem beneficia pe deplin de avantajele acesteia. În plus, Comisia invită statele membre să își continue și să își intensifice activitatea crucială legată de măsurile practice vizând sporirea securității infrastructurilor digitale, combaterea dezinformării și a altor amenințări facilitate de tehnologiile informatice, îmbunătățirea gradului de pregătire și de protecție și consolidarea cooperării cu partenerii din afara Uniunii împotriva amenințărilor comune. Luate împreună, aceste măsuri consolidează în mod colectiv securitatea tuturor cetățenilor.

1. <https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf> [↑](#footnote-ref-2)
2. Pentru o imagine de ansamblu, a se vedea fișa informativă privind „Uniunea securității: o Europă care protejează” (<https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf> ) și Cel de al optsprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și autentică [COM(2019) 145 final, 20.3.2019]. [↑](#footnote-ref-3)
3. A se vedea Cel de al optsprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și autentică [COM(2019) 145 final (20.3.2019)]. [↑](#footnote-ref-4)
4. <https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en>. Președintele Franței, dl Emmanuel Macron, și prim-ministrul Noii Zeelande, dna Jacinda Ardern, au invitat liderii și platformele online la Paris, la 15 mai 2019, pentru a lansa această inițiativă. [↑](#footnote-ref-5)
5. <https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes> [↑](#footnote-ref-6)
6. În cadrul reuniunii G20 de la Osaka din perioada 28-29 iunie 2019, liderii și-au reafirmat angajamentul de a acționa pentru a-și proteja cetățenii împotriva terorismului și a extremismului violent care permit exploatarea internetului în scopuri teroriste ( <https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf>). [↑](#footnote-ref-7)
7. COM(2018) 640 final (12.9.2018). [↑](#footnote-ref-8)
8. Lansat în 2015, **Forumul UE pentru internet** îi reunește în cadrul său pe miniștrii afacerilor interne din UE, pe reprezentanții sectorului internetului și alte părți interesate care colaborează în cadrul unui parteneriat voluntar menit să abordeze problema utilizării internetului de către grupurile teroriste și să îi protejeze pe cetățeni. [↑](#footnote-ref-9)
9. În 2011, Comisia a înființat **Rețeaua pentru sensibilizarea publicului cu privire la radicalizare**, menită să îi reunească pe practicienii din prima linie și pe cei de pe teren. În 2015, Comisia a consolidat rețeaua prin înființarea Centrului de excelență al Rețelei pentru sensibilizarea publicului cu privire la radicalizare, menit să dezvolte servicii de orientare, sprijin și consiliere mai bine adaptate nevoilor părților interesate din statele membre și să sporească gradul de expertiză și competențele diferiților actori. Pentru mai multe informații privind activitățile Rețelei pentru sensibilizarea publicului cu privire la radicalizare, a se vedea: <https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en>. [↑](#footnote-ref-10)
10. Pentru mai multe informații, a se vedea broșura „Construirea unei securități cibernetice puternice în Uniunea Europeană: reziliență, prevenire, apărare”: <https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence>. [↑](#footnote-ref-11)
11. JOIN(2017) 450 final (13.9.2017). [↑](#footnote-ref-12)
12. Legea privind securitatea cibernetică a UE [Regulamentul (UE) 2019/881 din 17.4.2019] introduce, pentru prima dată, norme la nivelul UE pentru certificarea de securitate cibernetică a produselor, proceselor și serviciilor. Mai mult, Legea privind securitatea cibernetică prevede un nou mandat permanent pentru Agenția UE pentru Securitate Cibernetică și îi alocă acesteia mai multe resurse pentru a-i permite să își îndeplinească obiectivele. Pentru mai multe informații privind cererea de propuneri, a se vedea: <https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross>. [↑](#footnote-ref-13)
13. C(2019) 2400 final (3.4.2019) și SWD(2019) 1240 final (3.4.2019). [↑](#footnote-ref-14)
14. COM(2018) 630 final (12.9.2018). [↑](#footnote-ref-15)
15. <https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas> [↑](#footnote-ref-16)
16. Directiva (UE) 2016/1148 (6.7.2016). [↑](#footnote-ref-17)
17. <http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/ro/pdf> [↑](#footnote-ref-18)
18. Acestea includ atacurile cibernetice, precum și tentativele de atacuri cibernetice cu un efect potențial semnificativ, care implică, de exemplu, accesul la sistemele de informații sau interceptarea de date prin intermediul infrastructurii digitale, cum ar fi rețelele 5G (a se vedea, de asemenea, secțiunea III privind consolidarea securității infrastructurilor digitale). [↑](#footnote-ref-19)
19. A se vedea Raportul privind punerea în aplicare a Cadrului comun din 2016 privind contracararea amenințărilor hibride și Comunicarea comună din 2018 privind creșterea rezilienței și consolidarea capacităților necesare pentru a aborda amenințările hibride [SWD(2019) 200 final, 28.5.2019]. A se vedea, de asemenea, Propunerea legislativă din septembrie 2016 de regulament de instituire a unui regim al Uniunii pentru controlul exporturilor, transferului, serviciilor de intermediere, asistenței tehnice și tranzitului în ceea ce privește produsele cu dublă utilizare (reformare) [COM (2016) 616 final, 28.9.2016]. [↑](#footnote-ref-20)
20. <https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf> [↑](#footnote-ref-21)
21. Regulamentul (UE) 2019/1148 (20.6.2019) privind comercializarea și utilizarea precursorilor de explozivi. [↑](#footnote-ref-22)
22. 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. [↑](#footnote-ref-23)
23. 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. [↑](#footnote-ref-24)
24. Probele electronice sunt necesare în aproximativ 85 % din anchetele penale, iar în două treimi dintre ele trebuie solicitate dovezi din partea furnizorilor de servicii online aflați într-o altă jurisdicție. A se vedea evaluarea impactului care însoțește propunerea legislativă [SWD(2018) 118 final (17.4.2018)]. [↑](#footnote-ref-25)
25. COM(2018) 225 final (17.4.2018). Consiliul și-a adoptat mandatul de negociere cu privire la propunerea de regulament în cadrul Consiliului Justiție și Afaceri Interne din 7 decembrie 2018. [↑](#footnote-ref-26)
26. COM(2018) 226 final (17.4.2018). Consiliul și-a adoptat poziția de negociere cu privire la propunerea de directivă în cadrul Consiliului Justiție și Afaceri Interne din 8 martie 2019. [↑](#footnote-ref-27)
27. <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/> [↑](#footnote-ref-28)
28. Regulamentul (UE) 2019/817 (20.5.2019) și Regulamentul (UE) 2019/818 (20.5.2019). [↑](#footnote-ref-29)
29. Regulamentul (UE) 2017/2226 (30.11.2017). [↑](#footnote-ref-30)
30. Regulamentul (UE) 2018/1240 (12.9.2018) și Regulamentul (UE) 2018/1241 (12.9.2018). [↑](#footnote-ref-31)
31. Regulamentul (UE) 2018/1860 (28.11.2018), Regulamentul (UE) 2018/1861 (28.11.2018), Regulamentul (UE) 2018/1862 (28.11.2018). [↑](#footnote-ref-32)
32. Regulamentul (UE) 2019/816 (17.4.2019). [↑](#footnote-ref-33)
33. COM(2019) 3 final și COM(2019) 4 final (7.1.2019). [↑](#footnote-ref-34)
34. COM(2018) 302 final (16.5.2018). [↑](#footnote-ref-35)
35. COM(2016) 272 final (4.5.2016). [↑](#footnote-ref-36)
36. <https://www.consilium.europa.eu/ro/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/> [↑](#footnote-ref-37)
37. COM(2019) 126 final (6.3.2019). [↑](#footnote-ref-38)
38. <https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/ro/pdf> [↑](#footnote-ref-39)
39. COM(2019) 2335 final (26.3.2019). [↑](#footnote-ref-40)
40. Grupul de cooperare în materie de securitate a rețelelor și a informațiilor este instituit în temeiul Directivei (UE) 2016/1148 (6.7.2016) privind securitatea rețelelor și a sistemelor informatice. Astfel cum se prevede în recomandare, a fost stabilit un flux de lucru specific în cadrul Grupului de cooperare în materie de securitate a rețelelor și a sistemelor informatice, condus de mai multe state membre. Grupul s-a reunit deja de trei ori – în lunile aprilie, mai și iulie 2019 – pentru a face schimb de informații cu privire la abordările naționale și pentru a discuta modalitățile de facilitare a pregătirii evaluării coordonate a riscurilor la nivelul UE. [↑](#footnote-ref-41)
41. Regulamentul (UE) 2019/452 (19.3.2019) de stabilire a unui cadru pentru examinarea investițiilor străine directe în Uniune. Noul cadru creează un mecanism de cooperare prin care statele membre și Comisia vor putea face schimb de informații și își vor putea exprima preocupările legate de anumite investiții specifice. Acesta va permite, de asemenea, Comisiei să emită avize atunci când o investiție amenință securitatea sau ordinea publică a mai multor state membre sau atunci când o investiție ar putea submina un proiect sau un program de interes pentru întreaga UE. Statul membru în care are loc investiția are ultimul cuvânt cu privire la modul în care va fi tratată investiția. [↑](#footnote-ref-42)
42. Raportul 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 final din 24.7.2019], Raportul 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 din 24.7.2019], Raportul privind evaluarea presupuselor cazuri recente de spălare a banilor care implică instituțiile de credit din UE [COM(2019) 373 final din 24.7.2019], Raportul de evaluare a cadrului de cooperare dintre unitățile de informații financiare [COM(2019) 371 final din 24.7.2019]. [↑](#footnote-ref-43)
43. Directiva (UE) 2015/849 (20.5.2015). [↑](#footnote-ref-44)
44. Directiva (UE) 2019/1153 (20.6.2019). [↑](#footnote-ref-45)
45. Această evaluare este impusă de articolul 65 alineatul (2) din cea de a cincea Directivă a (UE) 2018/843 privind combaterea spălării banilor (30.5.2018). [↑](#footnote-ref-46)
46. În raportul său final adoptat în decembrie 2018, Comisia specială pentru combaterea terorismului din cadrul Parlamentului European a solicitat instituirea unui sistem de urmărire a finanțărilor în scopuri teroriste la nivelul Uniunii Europene care să vizeze tranzacțiile efectuate de persoane care au legături cu terorismul și finanțarea acestora în cadrul zonei unice de plăți în euro. [↑](#footnote-ref-47)
47. A se vedea cel de Al optsprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și autentică [COM(2019) 145 final (20.3.2019)]. [↑](#footnote-ref-48)
48. Directiva (UE) 2016/681 (27.4.2016). [↑](#footnote-ref-49)
49. Trimiterile la notificarea transpunerii complete țin seama de declarațiile statelor membre și nu aduc atingere verificării transpunerii efectuată de către serviciile Comisiei. [↑](#footnote-ref-50)
50. Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-51)
51. Directiva (UE) 2017/541 (15.3.2017). [↑](#footnote-ref-52)
52. Polonia a notificat transpunerea parțială. Grecia și Luxemburg nu au notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-53)
53. Directiva (UE) 2017/853 (17.5.2017). [↑](#footnote-ref-54)
54. Belgia, Cehia, Estonia, Lituania, Polonia, Portugalia, Suedia și Regatul Unit au notificat transpunerea parțială. Germania, Irlanda, Grecia, Spania, Cipru, Luxemburg, Ungaria, Țările de Jos, România, Slovenia, Slovacia și Finlanda nu au notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-55)
55. Directiva (UE) 2016/680 (27.4.2016). [↑](#footnote-ref-56)
56. 20 de state membre au finalizat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-57)
57. Letonia, Portugalia, Slovenia și Finlanda au notificat transpunerea parțială. Grecia și Spania nu au notificat transpunerea. Deși Germania a notificat transpunerea integrală, Comisia consideră că această transpunere nu este integrală (situație verificată la 24 iulie 2019). [↑](#footnote-ref-58)
58. Directiva (UE) 2016/1148 (27.4.2016). [↑](#footnote-ref-59)
59. Belgia și Ungaria au transpus parțial directiva (situație verificată la 24 iulie 2019). [↑](#footnote-ref-60)
60. Directiva (UE) 2015/849 (20.5.2015). [↑](#footnote-ref-61)
61. Belgia, Bulgaria, Cehia, Danemarca, Germania, Estonia, Irlanda, Spania, Franța, Italia, Cipru, Letonia, Lituania, Ungaria, Țările de Jos, Austria, Polonia, Portugalia, România, Slovenia, Slovacia, Finlanda, Suedia și Regatul Unit (situație verificată la 24 iulie 2019). [↑](#footnote-ref-62)
62. Slovenia a notificat transpunerea parțială. Spania nu a notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-63)
63. Polonia a notificat transpunerea parțială. Grecia și Luxemburg nu au notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-64)
64. Belgia, Cehia, Estonia, Lituania, Polonia, Portugalia, Suedia și Regatul Unit au notificat transpunerea parțială. Germania, Irlanda, Grecia, Spania, Cipru, Luxemburg, Ungaria, Țările de Jos, România, Slovenia, Slovacia și Finlanda nu au notificat transpunerea (situație verificată la 24 iulie 2019). [↑](#footnote-ref-65)
65. Letonia, Portugalia, Slovenia și Finlanda au notificat transpunerea parțială. Grecia și Spania nu au notificat transpunerea. Deși Germania a notificat transpunerea integrală, Comisia consideră că această transpunere nu este integrală (situație verificată la 24 iulie 2019). [↑](#footnote-ref-66)
66. Belgia și Ungaria au transpus parțial directiva (situație verificată la 24 iulie 2019). [↑](#footnote-ref-67)
67. Belgia, Bulgaria, Cehia, Danemarca, Germania, Estonia, Irlanda, Spania, Franța, Italia, Cipru, Letonia, Lituania, Ungaria, Țările de Jos, Austria, Polonia, Portugalia, România, Slovenia, Slovacia, Finlanda, Suedia și Regatul Unit (situație verificată la 24 iulie 2019). [↑](#footnote-ref-68)
68. A se vedea Planul de acțiune împotriva dezinformării [JOIN(2018) 36 final din 5.12.2018]. [↑](#footnote-ref-69)
69. COM(2019) 12 final (14.6.2019). [↑](#footnote-ref-70)
70. [https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf](https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-ro.pdf) Îndemnul Consiliului European se bazează pe contribuțiile președinției române a Consiliului, precum și ale Comisiei și ale Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate cu privire la lecțiile învățate în ceea ce privește dezinformarea și asigurarea unor alegeri libere și corecte, inclusiv pe Comunicarea comună privind punerea în aplicare a Planului de acțiune împotriva dezinformării. [↑](#footnote-ref-71)
71. Codul de bune practici a fost semnat de platformele online Facebook, Google și Twitter, Mozilla, precum și de către societățile de publicitate și sectorul publicitar în octombrie 2018 și stabilește standarde de autoreglementare pentru combaterea dezinformării. Codul urmărește atingerea obiectivelor stabilite în Comunicarea Comisiei din aprilie 2018 privind combaterea dezinformării online (COM/2018/236 final din 26.4.2018) prin stabilirea unei game largi de angajamente care includ transparența în publicitatea politică, închiderea conturilor false și demonetizarea vectorilor dezinformării. [↑](#footnote-ref-72)
72. Rețeaua europeană de cooperare privind alegerile reunește punctele de contact ale rețelelor naționale de cooperare în materie electorală ale autorităților cu competențe în materie electorală și ale autorităților responsabile cu monitorizarea și asigurarea respectării normelor referitoare la activitățile online relevante în context electoral. Scopul Rețelei europene de cooperare privind alegerile este de a transmite alerte privind amenințările, de a face schimb de bune practici între rețelele naționale, de a discuta soluțiile comune la provocările identificate și de a încuraja proiectele și exercițiile comune între rețelele naționale. [↑](#footnote-ref-73)
73. Grupul autorităților europene de reglementare pentru serviciile mass-media audiovizuale reunește șefii sau reprezentanții la nivel înalt ai organismelor naționale de reglementare independente în domeniul serviciilor audiovizuale cu scopul de a oferi consultanță Comisiei cu privire la punerea în aplicare a Directivei UE privind serviciile mass-media audiovizuale (Directiva 2010/13/UE din 10.3.2010). În cadrul celei mai recente reuniuni a sale din 20-21 iunie 2019, care a avut loc la Bratislava, Grupul a prezentat rezultatele activității pe care a desfășurat-o până în prezent în materie de dezinformare, punând accentul pe alegerile pentru Parlamentul European din 2019 și pe domeniile conexe ale publicității politice și tematice. [↑](#footnote-ref-74)
74. A se vedea „Bune practici pentru autoritățile publice și operatorii privați în vederea consolidării securității spațiilor publice”, astfel cum sunt descrise în cel de Al optsprezecelea raport privind progresele înregistrate către o uniune a securității efectivă și autentică [COM (2019) 145 final din 20.3.2019]. Aceasta se bazează pe Planul de acțiune din octombrie 2017 de sprijinire a protecției spațiilor publice [COM(2017) 612 final din 18.10.2017]. La 5 iunie 2019 a avut loc cea de a treia reuniune a Forumului operatorilor din cadrul Forumului UE privind protecția spațiilor publice. Acesta a reunit reprezentanți ai statelor membre ale UE și operatori privați de spații publice, reprezentați de 14 asociații europene din sectoare precum sectorul hotelier, al spectacolelor live, al muzicii și divertismentului, al parcurilor de distracție și de atracții, al aviației, al transportului feroviar, al centrelor comerciale, al telecomunicațiilor, precum și al serviciilor de securitate private și al producătorilor de echipamente de securitate. [↑](#footnote-ref-75)
75. În special prin punerea în aplicare a Planului de acțiune din octombrie 2017 privind îmbunătățirea nivelului de pregătire împotriva riscurilor de siguranță chimică, biologică, radiologică și nucleară [COM(2017) 610 final din 18.10.2017]. [↑](#footnote-ref-76)
76. A se vedea articolul 12 alineatul (2) din Decizia 1313/2013/UE privind mecanismul de protecție civilă al Uniunii (17.12.2013), astfel cum a fost modificată prin Decizia (UE) 2019/420 (13.3.2019). [↑](#footnote-ref-77)
77. A se vedea acțiunile consolidate împotriva amenințărilor chimice, astfel cum figurează în Al cincisprezecelea raport privind progresele înregistrate în direcția realizării unei uniuni a securității efective și reale [COM(2018) 470 final din 13.6.2018]. [↑](#footnote-ref-78)
78. JO L 152, 11.6.2019 – Regulamentul de punere în aplicare (UE) 2019/947 al Comisiei din 24 mai 2019 privind normele și procedurile de operare a aeronavelor fără pilot la bord. [↑](#footnote-ref-79)
79. Evaluarea cuprinzătoare din 2017 a politicii de securitate a UE [SWD(2017) 278 final, 26.7.2017] a evidențiat necesitatea adoptării unei viziuni largi asupra politicii UE privind protecția infrastructurilor critice. [↑](#footnote-ref-80)
80. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora urmărește să îmbunătățească protecția infrastructurilor critice din Uniunea Europeană. [↑](#footnote-ref-81)
81. În special Regulamentul (UE) 2017/1938 (25.10.2017) privind măsurile de garantare a siguranței furnizării de gaze și Regulamentul (UE) 2019/941 (5.6.2019) privind pregătirea pentru riscuri în sectorul energiei electrice. [↑](#footnote-ref-82)
82. <https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf> [↑](#footnote-ref-83)
83. COM(2018) 65 final (6.2.2018). [↑](#footnote-ref-84)
84. <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_ro.pdf> [↑](#footnote-ref-85)
85. JO L 215, 11.8.2012, p. 5. [↑](#footnote-ref-86)
86. JO L 195, 27.7. 2010, p. 5. [↑](#footnote-ref-87)
87. COM(2019) 342 final (22.7.2019). [↑](#footnote-ref-88)
88. JO L 186, 14.7.2012, p. 4. [↑](#footnote-ref-89)