

Bruxelles, 25.1.2017
COM(2017) 41 final

**COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN,
CONSILIUL EUROPEAN ȘI CONSILIU**

**Al patrulea raport privind progresele înregistrate către o uniune a securității efectivă și
autentică**

Al patrulea raport privind progresele înregistrate către o uniune a securității efectivă și autentică

I. INTRODUCERE

Acesta este cel de al patrulea raport lunar referitor la progresele înregistrate către o uniune a securității efectivă și autentică. Raportul prezintă evoluția situației în cadrul a doi piloni principali: *pe de o parte, combaterea terorismului și a criminalității organizate, precum și a mijloacelor de care dispun acestea și, pe de altă parte, consolidarea mijloacelor noastre de apărare și dezvoltarea rezilienței împotriva acestor amenințări*. Prezentul raport se axează pe patru domenii-cheie: sistemele de informații și interoperabilitatea, protecția țărilor vulnerabile, amenințările cibernetice și protecția datelor în contextul cercetărilor penale.

Atacul care a avut loc la Berlin, în luna decembrie, cu ocazia târgului de Crăciun, a evidențiat încă o dată faptul că există deficiențe grave în ceea ce privește sistemele noastre de informații care trebuie soluționate de urgență, în special la nivelul UE, pentru a ajuta autoritățile naționale de frontieră și autoritățile responsabile de asigurarea respectării legii să își îndeplinească într-un mod mai eficace pe teren sarcinile lor de serviciu solicitante. Faptul că diferitele sisteme de informații nu sunt interconectate, permițându-le astfel atacatorilor să folosească identități multiple pentru a se deplasa fără a fi detectați, inclusiv la trecerea frontierelor, și că informațiile respective nu sunt introduse în mod sistematic de statele membre în bazele de date relevante ale UE reprezintă deficiențe în ceea ce privește punerea în aplicare concretă ce trebuie remediate neîntârziat. Mai mult, este, de asemenea, necesar să se depună eforturi suplimentare¹ în ceea ce privește măsurile de asigurare a respectării legii la frontiere și returnarea persoanelor ale căror cereri de azil au fost respinse.

În ceea ce privește protecția țărilor vulnerabile, Comisia își va intensifica eforturile pentru a reuni experți din statele membre care să facă schimb de bune practici și să convină asupra unor orientări standard.

Amenințarea cu care se confruntă UE în domeniul cibernetic este un subiect foarte mediatizat, iar prezentul raport trece în revistă diferitele filiere de activitate din acest domeniu care sunt deja în derulare. Aceste filiere acoperă atât prevenirea – care presupune, pe de o parte, colaborarea cu întreprinderile din sector pentru a promova securitatea de la stadiul conceperii și, pe de altă parte, punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor – cât și încurajarea cooperării între statele membre și cu organizații și parteneri internaționali pentru a face față atacurilor cibernetice în timp ce se produc. În lunile următoare, Comisia și Înalțul Reprezentant al Uniunii pentru afaceri externe și politica de securitate vor identifica acțiunile necesare pentru a da un răspuns eficace la nivelul UE în privința acestor amenințări, pe baza Strategiei de securitate cibernetică a UE din 2013.

Protecția vieții private și a datelor cu caracter personal ale cetățenilor reprezintă un drept fundamental și, deci, piatra de temelie pentru orice acțiune desfășurată în direcția unei

¹ În săptămânile care urmează, Comisia va prezenta un plan de acțiune revizuit privind returnările; a se vedea Raportul Comisiei către Parlamentul European, Consiliul European și Consiliu privind operaționalizarea Poliției de frontieră și gărzii de coastă la nivel european, COM(2017) 42.

reale uniuni a securității. Directiva privind protecția datelor în domeniul polițienesc și al justiției penale, adoptată în aprilie 2016, asigură un standard comun ridicat de protecție a datelor și, prin urmare, va facilita schimbul de informații relevante între autoritățile responsabile de asigurarea respectării legii din statele membre. Comisia a lansat, de asemenea, un proces de revizuire a Directivei asupra confidențialității și comunicațiilor electronice în cadrul pachetului său referitor la date în vederea extinderii domeniului de aplicare al directivei pentru a-i include pe toți furnizorii de servicii de comunicații electronice și în vederea alinierii dispozițiilor sale la Regulamentul general privind protecția datelor. Propunerea este concepută astfel încât să asigure confidențialitatea comunicațiilor electronice și să definească rațiunile pentru care pot fi avute în vedere restrângeri ale domeniului de aplicare al Regulamentului privind confidențialitatea în mediul electronic, inclusiv motive aferente securității naționale sau cercetărilor penale.

II. CONSOLIDAREA SISTEMELOR DE INFORMAȚII ȘI A INTEROPERABILITĂȚII

Discursul președintelui Juncker privind starea Uniunii din septembrie 2016 și concluziile Consiliului European din decembrie 2016 fac referire la importanța eliminării deficiențelor actuale în domeniul gestionării informațiilor și a îmbunătățirii **interoperabilității și a interconectării dintre sistemele de informații existente**. Evenimentele recente au subliniat încă o dată nevoia urgentă de a interconecta bazele de date existente ale UE, nu în ultimul rând pentru a le oferi, pe teren, autorităților de frontieră și celor responsabile de asigurarea respectării legii instrumentele necesare pentru detectarea fraudei de identitate. De exemplu, autorul atacurilor teroriste de la Berlin din decembrie 2016 a utilizat cel puțin 14 identități diferite și a reușit să treacă dintr-un stat membru în altul fără a fi detectat. Există o nevoie de netăgăduit ca sistemele de informații existente și viitoare ale UE să poată fi consultate simultan cu ajutorul unor elemente biometrice de identificare pentru a-i împiedica pe teroriști și pe infractori să aibă acces la ele.

În acest sens, Comisia a demarat lucrările în aprilie 2016, prezentându-și propunerile referitoare la „sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”². Acestea au identificat deficiențe în ceea ce privește funcționalitățile sistemelor de informații existente, lacune în arhitectura UE privind gestionarea datelor, probleme legate de peisajul complex al sistemelor de informații reglementate în mod diferit și o fragmentare majoră din cauza faptului că sistemele actuale au fost concepute pentru a funcționa separat, mai degrabă decât împreună. În cadrul acestui proces, Comisia a lansat **Grupul de experți la nivel înalt privind sistemele de informații și interoperabilitatea**, împreună cu agențiile UE, cu statele membre și cu părțile interesate relevante. La 21 decembrie 2016³, un raport al președintelui grupului a prezentat **concluziile intermediare** ale grupului, cuprinzând opțiunea prioritară referitoare la crearea unui portal unic de căutare menit să le permită autorităților naționale de asigurare a respectării legii și autorităților de frontieră să efectueze, simultan, căutări în bazele de date și în sistemele de informații existente ale UE. Raportul intermediar evidențiază, de asemenea, importanța calității datelor – având

² Comunicarea intitulată „Sisteme de informații mai puternice și mai inteligente în materie de frontiere și securitate”, COM(2016) 205 final.

³ <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1>

în vedere că eficacitatea sistemelor de informații depinde de calitatea și de formatul datelor conținute în acestea – și formulează recomandări pentru îmbunătățirea calității datelor în sistemele UE prin intermediul unor controale automatizate ale calității datelor.

Comisia va da curs rapid opțiunii de a crea un portal unic de căutare și, împreună cu Agenția UE pentru gestionarea operațională a sistemelor IT la scară largă, eu-LISA, își va începe lucrările pentru instituirea unui portal care va permite efectuarea unor căutări, în paralel, în toate sistemele existente ale UE. Un studiu conex ar trebui să fie întocmit până în luna iunie; acesta va servi drept bază pentru conceperea și testarea unui prototip al portalului înainte de sfârșitul anului. Comisia consideră că, în paralel, Europol ar trebui să își continue lucrările în vederea elaborării unei interfețe de sistem care le va permite ofițerilor din prima linie ai statelor membre, atunci când își consultă propriile sisteme naționale, să consulte în același timp, automat, și bazele de date ale Europol.

Lucrările în vederea interoperabilității sistemelor de informații vizează remedierea fragmentării actuale la nivelul UE a arhitecturii aferente gestionării datelor aplicată controalelor la frontieră și securității, precum și reducerea „unghiurilor moarte” pe care le creează această fragmentare. Atunci când bazele de date utilizează un registru comun de date de identitate – astfel cum se prevede în propunerile referitoare la sistemul de intrare/ieșire al UE și la sistemul UE de informații și de autorizare privind călătoriile (ETIAS) –, o persoană nu poate fi înregistrată decât cu o singură identitate în diferitele baze de date, ceea ce împiedică utilizarea mai multor identități false. Ca un prim pas, astfel cum s-a sugerat în concluziile intermediare ale Grupului de experți la nivel înalt, Comisia a solicitat Agenției eu-LISA să analizeze aspectele tehnice și operaționale ale punerii în aplicare a unui serviciu comun de comparare a datelor biometrice. Un astfel de serviciu ar permite efectuarea unor căutări în diferite baze de date cu ajutorul unor date biometrice, ceea ce ar putea revela identitățile false utilizate de persoana în cauză într-un alt sistem. În afară de aceasta, Grupul de experți la nivel înalt ar trebui să evalueze în prezent dacă este necesar, realizabil din punct de vedere tehnic și proporțional ca **registru comun de date de identitate** care a fost conceput pentru sistemul de intrare/ieșire și pentru ETIAS să fie extins la alte sisteme. În plus față de datele biometrice stocate în serviciul de comparare a datelor biometrice, un astfel de registru comun ar include, de asemenea, date de identitate alfanumerice. Grupul ar trebui să își prezinte concluziile în acest sens în raportul său final până la sfârșitul lunii aprilie 2017.

Evenimentele recente care au periclitat securitatea evidențiază necesitatea de a reexamina chestiunea **schimbului de informații obligatoriu** între statele membre. Propunerea Comisiei din decembrie 2016 vizând consolidarea **Sistemului de Informații Schengen** prevede, pentru prima dată, obligația pentru statele membre de a introduce semnalări privind persoanele care au legătură cu infracțiuni de terorism. Este important ca, în prezent, colegiitorii să depună eforturi în direcția adoptării rapide a măsurilor propuse. Comisia este pregătită să examineze dacă este oportun să se introducă o condiție obligatorie privind schimbul de informații pentru alte baze de date ale UE.

III. PROTECȚIA ȚINTELOR NOASTRE VULNERABILE ÎMPOTRIVA ATACURILOR TERORISTE

Atacul de la Berlin a fost evenimentul cel mai recent care a avut loc în UE, îndreptat împotriva așa-numitelor ținte vulnerabile; acestea sunt, de obicei, zone civile în care oamenii se reunesc în număr mare (de exemplu, spații publice, spitale, școli, centre sportive și culturale, cafenele și restaurante, centre comerciale și noduri de transport).

Prin natura lor, aceste locuri sunt vulnerabile și dificil de apărat, având, de asemenea, caracteristica de a putea cauza un număr considerabil de victime în cazul unui atac. Pentru toate aceste motive, locurile acestea sunt privilegiate de teroriști. Amenințarea unor atacuri viitoare împotriva unor ținte vulnerabile, inclusiv împotriva sectorului transporturilor, rămâne ridicată, astfel cum se confirmă în analizele disponibile, printre altele în raportul Europol privind evoluția modului de operare al Daesh⁴.

Agenda europeană privind securitatea din 2015 și Comunicarea din 2016 referitoare la o uniune a securității au evidențiat necesitatea de a intensifica acțiunile de îmbunătățire a securității și de a utiliza instrumente și tehnologii de detecție inovatoare în domeniul protecției țăintelor vulnerabile. Comisia a depus eforturi pentru a sprijini și a încuraja schimbul de bune practici între statele membre în ceea ce privește elaborarea unor instrumente mai eficiente pentru a preveni atacurile îndreptate împotriva țăintelor vulnerabile și pentru a le contracara. Grație acestui demers, Comisia a fost în măsură să elaboreze manuale operaționale și materiale de orientare. În prezent, Comisia întocmește, în strânsă cooperare cu experți din statele membre, un manual cuprinzător privind procedurile de securitate și modelele aplicabile diferitelor ținte vulnerabile (de exemplu, centre comerciale, spitale, evenimente sportive și culturale). Scopul avut în vedere este acela de a publica, la începutul anului 2017, orientări privind protecția țăintelor vulnerabile, adresate statelor membre, pe baza celor mai bune practici aplicate în statele membre.

În paralel, Comisia va organiza, în februarie, primul atelier cu autoritățile naționale referitor la protecția țăintelor vulnerabile, cu scopul de a face schimb de informații și de a dezvolta cele mai bune practici privind chestiunea complexă pe care o reprezintă protecția țăintelor vulnerabile și siguranța și securitatea publice. Comisia finanțează, de asemenea, în temeiul Fondului pentru securitate internă, un proiect-pilot inițiat de Belgia, Țările de Jos și Luxemburg pentru a înființa un centru de excelență regional pentru intervențiile speciale ale forțelor de ordine, care va oferi cursuri de formare pentru polițiști, aceștia fiind, adesea, responsabili de prima intervenție în cazul unui atac terorist.

Contracararea atacurilor îndreptate asupra unor ținte vulnerabile este o componentă esențială a activității Comisiei în materie de protecție civilă. În decembrie, Comisia a anunțat acțiunile pe care intenționează să le întreprindă împreună cu statele membre pentru a proteja cetățenii UE și pentru a reduce vulnerabilitățile în perioada imediat următoare atacurilor teroriste. Aceste acțiuni vor consolida coordonarea între toți actorii implicați în gestionarea consecințelor unui atac, iar Comisia s-a angajat să susțină eforturile statelor membre facilitând organizarea de cursuri de formare și de exerciții comune și asigurând un dialog susținut prin intermediul punctelor de contact și al grupurilor de experți existente. De asemenea, Comisia va sprijini dezvoltarea de module specializate pentru a răspunde atacurilor teroriste în cadrul mecanismului de protecție civilă al Uniunii și al unor inițiative menite să stimuleze schimbul de învățăminte desprinse și să sensibilizeze publicul larg.

De asemenea, Comisia va analiza, alături de statele membre, tipul de instrumente pe care UE le-ar putea mobiliza pentru a contribui la consolidarea rezilienței și a securității în

⁴ Raportul Europol intitulat „*Changes in modus operandi of Islamic State terrorist attacks (IS) revisited*” („Evoluția modului de operare al Statului Islamic (IS) - raport revizuit”), noiembrie 2016 – publicație a Europol, disponibilă la următoarea adresă: <https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited>

jurul unor potențiale ținte vulnerabile. Statele membre ar putea, de asemenea, să solicite finanțare din partea Băncii Europene de Investiții (BEI), inclusiv din partea Fondului european pentru investiții strategice, în conformitate cu politicile UE și ale Grupului BEI. Orice proiect ar urma să facă obiectul procedurilor decizionale obișnuite prevăzute în legislație.

În ceea ce privește țintele vulnerabile specifice legate de spații publice din sectorul transporturilor, cum ar fi părțile publice ale aeroporturilor sau ale gărilor, atelierul specializat pe care Comisia l-a consacrat acestei chestiuni în noiembrie 2016 a reunit o gamă largă de părți interesate și a subliniat necesitatea de a menține un echilibru între nevoile în materie de securitate, confortul pasagerilor și operațiunile de transport. Concluziile acestui atelier evidențiază importanța edificării unei culturi a securității, care să cuprindă nu numai personalul, ci și pasagerii, importanța evaluărilor riscurilor la nivel local ca bază pentru definirea contramăsurilor adecvate, precum și necesitatea de a îmbunătăți comunicarea între toate părțile implicate.

IV. CONFRUNTAREA CU PROVOCAREA REPREZENTATĂ DE AMENINȚĂRILE CIBERNETICE

Criminalitatea cibernetică și atacurile cibernetice reprezintă provocări majore cu care se confruntă Uniunea și un domeniu în care o acțiune la nivel european poate contribui la consolidarea rezilienței noastre colective. În fiecare zi, incidente legate de securitatea cibernetică afectează grav viețile oamenilor și produc pagube economice considerabile pentru economia și întreprinderile europene. Atacurile cibernetice reprezintă un element esențial al amenințărilor hibride; corelate în mod expres cu amenințări fizice, de exemplu în legătură cu terorismul, ele pot avea un impact devastator. De asemenea, ele pot contribui la destabilizarea unei țări sau la contestarea autorității instituțiilor sale politice și a proceselor sale democratice fundamentale. Pe măsură ce dependența noastră de tehnologiile online crește, infrastructurile noastre critice (de la spitale la centrale nucleare) vor deveni din ce în ce mai vulnerabile.

Strategia de securitate cibernetică a UE din 2013 face parte din chintesența măsurilor de politică luate pentru a răspunde provocărilor în materie de securitate cibernetică. Componenta principală este Directiva privind securitatea rețelelor și a informațiilor⁵, adoptată în luna iulie a anului trecut. Aceasta pune bazele pentru îmbunătățirea cooperării și a rezilienței cibernetice la nivelul UE, prin sprijinirea cooperării și a schimbului de informații între statele membre și prin încurajarea cooperării operaționale cu ocazia anumitor incidente specifice legate de securitatea cibernetică, precum și prin schimbul de informații cu privire la riscuri. Pentru a asigura transpunerea coerentă la nivelul diferitelor sectoare și la nivel transfrontalier, Comisia va organiza, în luna februarie, prima reuniune a Grupului de cooperare privind securitatea rețelelor și a informațiilor cu statele membre.

În aprilie 2016, Comisia și Înaltul Reprezentant au adoptat un cadru comun privind contracararea amenințărilor hibride⁶, care a propus 22 de acțiuni operaționale vizând

⁵ Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

⁶ JOIN (2016) 18.

sensibilizarea opiniei publice, consolidarea rezilienței, un răspuns mai eficient la crize și intensificarea cooperării dintre UE și NATO. Astfel cum s-a solicitat de către Consiliu, până în iulie 2017, Comisia și Înalțul Reprezentant vor prezenta un raport de evaluare a progreselor înregistrate.

Comisia promovează și sprijină, de asemenea, inovarea tehnologică, inclusiv prin valorificarea fondurilor pentru cercetare ale UE pentru a stimula găsirea de noi soluții și crearea de noi tehnologii care pot contribui la consolidarea rezilienței noastre împotriva atacurilor cibernetice (de exemplu, proiecte legate de „securitatea de la stadiul conceperii”). În vara anului trecut am lansat un parteneriat public-privat în valoare de 1,8 miliarde EUR în domeniul securității cibernetice cu întreprinderile din acest sector⁷.

În sectorul transporturilor, digitalizarea devine un factor major al transformării atât de necesare a sistemului actual de transport. Ritmul rapid al digitalizării oferă numeroase avantaje, dar face, de asemenea, ca sectorul transporturilor să devină mai vulnerabil la riscurile legate de securitatea sau de siguranța cibernetică. Numeroase acțiuni sunt întreprinse pentru a reduce amenințarea la diferite niveluri, în special în sectorul aviației, dar și în sectoarele maritim, fluvial, feroviar și rutier⁸. Provocarea care persistă încă se referă la clarificarea, armonizarea și completarea în continuare a activităților diferitelor părți interesate implicate în îmbunătățirea diverselor aspecte ale rezilienței cibernetice.

Pe scară mai largă și ținând seama de natura amenințării, care evoluează rapid, Comisia și Înalțul Reprezentant vor identifica, în următoarele luni, acțiunile necesare pentru a da un răspuns eficient la nivelul UE la aceste amenințări, întemeindu-se pe Strategia de securitate cibernetică a UE din 2013.

V. PROTEJAREA DATELOR CU CARACTER PERSONAL, SPRIJININD TOTODATĂ DESFĂȘURAREA UNOR ANCHETE PENALE EFICIENTE

Directiva privind protecția datelor în domeniul poliției și al justiției penale⁹ este un element crucial în lupta împotriva terorismului și a infracțiunilor grave. Pe baza unui standard comun de protecție a datelor prevăzut în directivă, autoritățile responsabile de asigurarea respectării legii din statele membre vor putea face cu ușurință schimb de date relevante, în timp ce datele privind victimele, martorii și persoanele suspectate de a fi săvârșit infracțiuni vor fi protejate în mod corespunzător.

⁷ Anunțat în Comunicarea din 2016 privind reziliența cibernetică, COM(2016) 410 final.

⁸ De exemplu, orientări internaționale, cum sunt cele elaborate de Organizația Maritimă Internațională sau prin intermediul unei rezoluții a OACI, adoptată recent, la inițiativa comună a UE și a SUA; raportarea incidentelor în cadrul căreia Agenția Europeană de Siguranță a Aviației elaborează în prezent o modalitate de a reacționa mai prompt, precum și securitatea cibernetică de la stadiul conceperii, aplicabilă sistemelor noi, în curs de elaborare, cum ar fi Planul general de management al traficului aerian conceput de întreprinderea comună SESAR.

⁹ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului. Directiva, care a intrat în vigoare la 5 mai 2016, trebuie să fie transpusă de statele membre până la 6 mai 2018. Comisia a instituit un grup de experți împreună cu statele membre pentru a face schimb de opinii cu privire la transpunerea directivei menționate anterior.

În plus, pentru a asigura un grad ridicat de confidențialitate a comunicațiilor atât pentru cetățeni, cât și pentru întreprinderi, precum și condiții de concurență echitabile pentru toți actorii de pe piață, astfel cum se prevede în Strategia privind piața unică digitală din aprilie 2015, Comisia a adoptat, la 11 ianuarie, propunerea de **Regulament privind viața privată și comunicațiile electronice** (care înlocuiește Directiva 2002/58/CE)¹⁰. La fel ca în actuala directivă, Regulamentul revizuit privind viața privată și comunicațiile electronice detaliază Regulamentul general privind protecția datelor¹¹ și stabilește cadrul care reglementează protecția confidențialității și a datelor personale în sectorul comunicațiilor electronice.

Ca urmare a acestei revizui, se consideră că toate datele transmise în cadrul comunicațiilor electronice, chiar și atunci când comunicarea este auxiliară, sunt confidențiale/restricționate – indiferent dacă acestea sunt transmise prin servicii de telecomunicații tradiționale sau prin alte așa-numite servicii de comunicații *over-the-top* (OTT) care sunt echivalente din punct de vedere funcțional (de exemplu, Skype și WhatsApp) și care au devenit adesea, pentru mulți utilizatori, interschimbabile cu operatorii de telecomunicații obișnuiți¹². Printre obligațiile impuse furnizorilor de servicii – în plus față de obligația de a respecta alegerile referitoare la viața privată a clienților lor privind utilizarea, stocarea și prelucrarea datelor lor – se numără, de asemenea, obligația furnizorilor de servicii cu sediul în afara UE de a numi un reprezentant pe teritoriul unui stat membru. Acest lucru le va oferi totodată statelor membre posibilitatea de a facilita cooperarea autorităților responsabile de asigurarea respectării legii și a celor judiciare cu furnizorii de servicii pentru a avea acces la probe electronice (a se vedea mai jos).

În conformitate cu actualele norme privind viața privată și comunicațiile electronice, accesul autorităților responsabile de asigurarea respectării legii și al autorităților judiciare la informații electronice pertinente, necesare pentru investigarea infracțiunilor, va fi reglementat prin excepția prevăzută la articolul 11 din propunerea de Regulament privind viața privată și comunicațiile electronice¹³. Această dispoziție oferă posibilitatea ca în dreptul UE sau în dreptul național să se limiteze confidențialitatea comunicațiilor, dacă acest lucru este necesar și proporțional, pentru a proteja securitatea națională, apărarea, siguranța publică, precum și pentru a asigura prevenirea, investigarea, identificarea și urmărirea penală a infracțiunilor sau executarea sancțiunilor penale. Această dispoziție este deosebit de relevantă pentru normele naționale în materie de **păstrare a datelor**, și anume pentru a-i obliga pe furnizorii de servicii de telecomunicații să păstreze datele transmise în cadrul comunicațiilor pentru o perioadă determinată în vederea unui posibil acces în scopul asigurării respectării legii, ca urmare a anulării, în 2014, de către Curtea

¹⁰ Regulamentul privind viața privată și comunicațiile electronice, COM(2017) 10.

¹¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - RGPD), care va începe să se aplice de la 25 mai 2018.

¹² Aceasta urmează abordarea adoptată în propunerea de Directivă de instituire a Codului european al comunicațiilor electronice, prezentată de Comisie la 14 septembrie 2016 (pachetul privind telecomunicațiile), COM(2016) 590 final.

¹³ A se vedea articolul 11 alineatul (1) („clauza privind păstrarea datelor”), care este identic cu articolul 15 din Directiva asupra confidențialității și comunicațiilor electronice și conform cu cerințele prevăzute în RGPD. O asemenea restricție trebuie să respecte conținutul esențial al drepturilor fundamentale și să fie necesară, adecvată și proporțională.

Europeană de Justiție (CEJ) a Directivei privind păstrarea datelor¹⁴. De atunci, nu a mai existat niciun instrument al UE privind păstrarea datelor și unele state membre și-au adoptat propriile legi naționale în materie de păstrare a datelor. Legislația suedeză și cea britanică în materie de păstrare a datelor au fost contestate în fața CEJ, care a pronunțat, la 21 decembrie 2016, hotărârea Tele2¹⁵. CEJ a constatat incompatibilitatea cu dreptul Uniunii a unei legislații naționale care prevede, în vederea combaterii criminalității, păstrarea generalizată și nediferențiată a tuturor datelor legate de trafic și de localizare ale abonaților și ale utilizatorilor referitoare la toate mijloacele de comunicare electronică. Implicațiile hotărârii sunt analizate în prezent, iar Comisia va elabora orientări cu privire la modul în care legislațiile naționale în materie de păstrare a datelor pot fi redactate în conformitate cu hotărârea respectivă.

Criminalitatea lasă urme digitale care pot servi drept probe în cadrul procedurilor judiciare; comunicațiile electronice între persoane suspectate sunt adesea singurele indicii pe care le pot colecta autoritățile responsabile de asigurarea respectării legii și procurorii. Cu toate acestea, obținerea accesului la **probe electronice**, în special în cazul în care acestea sunt stocate în străinătate sau într-un sistem de tip *cloud*, poate fi un demers complex atât din punct de vedere tehnic, cât și din punct de vedere juridic și poate să presupună adesea o procedură împovăritoare, ceea ce periclitează capacitatea anchetatorilor de a acționa rapid. Pentru a aborda aceste provocări, Comisia examinează în prezent soluții menite să le permită anchetatorilor să obțină probe electronice la nivel transfrontalier, inclusiv prin eficientizarea asistenței juridice reciproce, prin identificarea unor mijloace de cooperare directă cu furnizorii de servicii de internet, precum și să propună criterii pentru stabilirea și asigurarea respectării competenței de executare în spațiul cibernetic, în deplină conformitate cu normele aplicabile în materie de protecție a datelor¹⁶. La 9 decembrie 2016, Comisia a prezentat Consiliului Justiție și Afaceri Interne un raport referitor la progresele înregistrate¹⁷.

Un proces cuprinzător de consultare a experților (încă în curs) a permis Comisiei să definească diversele probleme, adesea complexe, pe care le presupune accesul la probe electronice, să înțeleagă mai bine normele și practicile actuale aplicate în statele membre și să identifice posibile opțiuni de politică. Raportul privind progresele înregistrate oferă o imagine de ansamblu a ideilor care au apărut până în prezent în cursul colectării informațiilor și al procesului de consultare a experților, pe care Comisia, pe baza consultărilor cu părțile interesate, le va analiza în mod detaliat în lunile următoare. După cum a anunțat în programul său de lucru, Comisia va prezenta o inițiativă în 2017.

¹⁴ Hotărârea CEJ din 8 aprilie 2014, Digital Rights Ireland, în cauzele conexate C-293/12 și C-594/12.

¹⁵ Hotărârea CEJ din 21 decembrie 2016, Tele2, în cauzele conexate C-203/15 și C-698/15.

¹⁶ Conform angajamentului asumat în cadrul Agendei europene privind securitatea, COM(2015) 185 final, și al Comunicării Comisiei intitulată „Punerea în aplicare a Agendei europene privind securitatea pentru a combate terorismul și a deschide calea către o uniune a securității efectivă și autentică”, COM(2016) 230 final.

¹⁷ În concluziile sale privind îmbunătățirea justiției penale în spațiul cibernetic din 9 iunie 2016, Consiliul a invitat Comisia să ia măsuri concrete, să elaboreze o abordare europeană comună și să prezinte, cel mai târziu în luna iunie 2017, rezultate în acest sens.

VI. CONCLUZII

Următorul raport, care ar trebui să fie publicat la 1 martie, va oferi ocazia de a trece în revistă progresele înregistrate în ceea ce privește punerea în aplicare a acestor direcții de activitate și a altor acțiuni cruciale.