Orientări

Avizul 23/2018 privind propunerile Comisiei referitoare la ordinele europene de divulgare și de păstrare a probelor electronice în materie penală [articolul 70 alineatul 1 litera (b)]

Adoptat la 26 septembrie 2018

Cuprins

Comitetul European pentru Protecția Datelor,

având în vedere articolul 70 alineatul (1) litera (b) din 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,

ADOPTĂ URMĂTORUL AVIZ:

Introducere

În aprilie 2018, Comisia a prezentat o propunere de regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală și o propunere de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul obținerii de probe în cadrul procedurilor penale. Cele două propuneri, COM(2018) 225 final și COM(2018) 226 final, sunt complementare. Obiectivul general urmărit de Comisie este de a îmbunătăți cooperarea dintre autoritățile statelor membre și furnizorii de servicii, inclusiv cei care își au sediul în afara UE, și de a propune soluții pentru problema reprezentată de stabilirea și asigurarea respectării jurisdicției în spațiul cibernetic.

În timp ce proiectul de regulament prevede norme și proceduri aplicabile în materie de emitere, notificare și executare a ordinelor de divulgare și de păstrare a probelor electronice pentru furnizorii de servicii de comunicații electronice, proiectul de directivă prevede norme minime privind numirea unui reprezentant legal pentru furnizorii de servicii care nu au sediul în UE.

În noiembrie 2017[1], înainte de prezentarea proiectului de propunere de către Comisie, Grupul de Lucru „Articolul 29” (GL29) a reamintit necesitatea de a asigura că orice propunere legislativă respectă pe deplin acquis-ul UE în materie de protecție a datelor în special, precum și legislația și jurisprudența UE în general.

În special, GL29 a avertizat cu privire la limitarea drepturilor la protecția datelor și la viața privată în ceea ce privește datele prelucrate de furnizorii de telecomunicații și de societățile informaționale, în special atunci când acestea sunt prelucrate ulterior de autoritățile de aplicare a legii, a reamintit necesitatea de a asigura coerența oricărui instrument al UE cu Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică și cu Directiva UE privind ordinul european de anchetă (OEA) și a recomandat să se clarifice normele procedurale respective care reglementează accesul la probe electronice la nivel național și la nivelul UE pentru a se asigura că noul instrument nu ar conferi autorităților noi competențe pe care acestea nu le-ar avea la nivel intern. Pe lângă aceste observații generale, GL29 a formulat observații cu privire la opțiunile legislative luate în considerare de Comisie la momentul respectiv cu privire la categoriile de date în cauză și la garanțiile corespunzătoare pentru accesarea acestora, la posibilitatea de a aborda aspectele legate de ordinele/cererile de divulgare pentru a obliga furnizorii de servicii să furnizeze datele localizate în

[1] A se vedea declarația GL29 (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801).

afara UE, precum și la garanțiile necesare legate de condițiile de fond și de procedură necesare pentru a asigura accesul direct la date.

Împreună cu propunerile concrete privind probele electronice disponibile în prezent, CEPD dorește să furnizeze o analiză mai detaliată a instrumentelor juridice propuse din punct de vedere al protecției datelor.

1. Temeiul juridic al propunerii de regulament (articolul 82 din TFUE)

Temeiul juridic propus pentru proiectul de regulament privind probele electronice îl constituie articolul 82 alineatul (1) din TFUE, privind cooperarea judiciară în materie penală, care prevede:

> „1. Cooperarea judiciară în materie penală în cadrul Uniunii se întemeiază pe principiul recunoașterii reciproce a hotărârilor judecătorești și a deciziilor judiciare și include apropierea actelor cu putere de lege și a normelor administrative ale statelor membre în domeniile prevăzute la alineatul (2) și la articolul 83.
>
> Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară, adoptă măsurile privind:
>
> (a) instituirea unor norme și proceduri care să asigure recunoașterea, în întreaga Uniune, a tuturor categoriilor de hotărâri judecătorești și decizii judiciare;
>
> (b) prevenirea și soluționarea conflictelor de competență între statele membre;
>
> (c) sprijinirea formării profesionale a magistraților și a personalului din justiție;
>
> (d) facilitarea cooperării dintre autoritățile judiciare sau echivalente ale statelor membre în materie de urmărire penală și executare a deciziilor."

Așa cum a subliniat Comisia în evaluarea impactului care însoțește propunerile, „articolul 82 alineatul (1) precizează că cooperarea judiciară în materie penală se întemeiază pe principiul recunoașterii reciproce. Acest temei juridic ar acoperi o posibilă legislație privind cooperarea directă cu furnizorii de servicii, în care autoritatea din statul membru emitent ar urma să se adreseze direct unei entități (furnizorul de servicii) din statul de executare și chiar să impună obligații acesteia. Acesta ar introduce o nouă dimensiune în recunoașterea reciprocă, dincolo de cooperarea judiciară tradițională în cadrul Uniunii, întemeiată până în prezent pe procedurile care implică două autorități judiciare, una din statul emitent și cealaltă din statul de executare" (subliniere adăugată).

Având în vedere noutatea utilizării acestui temei juridic în contextul cererilor directe între autoritățile publice și părțile private, CEPD regretă faptul că nu este furnizată nicio analiză sau evaluare suplimentară de către Comisie.

Într-adevăr, astfel cum a subliniat deja Grupul de Lucru în declarația sa anterioară, CEPD continuă să își exprime îndoielile cu privire la caracterul adecvat al acestui temei juridic, acestea fiind sprijinite de analiza CJUE și a avocatului său general în Avizul 1/15. Printre progresele înregistrate în ceea ce privește validitatea articolului 82 ca temei juridic pentru proiectul de acord privind PNR dintre UE și Canada, Curtea a subliniat că autoritatea competentă din Canada „*nu constituie nici o autoritate judiciară, nici o autoritate echivalentă*"[2]. În contextul propunerilor privind probele electronice, unul

[2] A se vedea punctul 103 din Avizul 1/15 și punctul 108 din concluziile avocatului general în acest caz.

dintre principalele obiective urmărite, astfel cum au fost stabilite de Comisie, pare să fie evitarea cooperării judiciare „prea greoaie”. Prin urmare, propunerea se întemeiază pe principiul conform căruia cooperarea ar trebui să aibă loc mai degrabă între o autoritate și un furnizor de servicii decât între două autorități. Procedura prevăzută plasează, în primul rând, entitățile private în poziția de a fi parte destinatară și de a răspunde cererilor din partea autorităților judiciare.

CEPD constată că procesul de executare a ordinelor de divulgare și de păstrare ar putea presupune implicarea unei autorități care primește datele în situația în care furnizorul de servicii care primește date nu își îndeplinește obligațiile și, prin urmare, va declanșa necesitatea de a solicita o executare ex post a ordinului. Cu toate acestea, întrucât obiectivul principal al procedurii instituite este tocmai de a nu implica o autoritate care primește datele, CEPD și-a exprimat îndoielile cu privire la faptul că această procedură auxiliară ar putea justifica utilizarea articolului 82 ca unic temei juridic pentru acest instrument.

Prin urmare, CEPD este de opinie că, pentru ca articolul 82 să fie utilizat drept temei juridic, principalele etape procedurale ale cooperării trebuie să aibă loc între două autorități judiciare și că ar trebui să se utilizeze un alt temei juridic pentru acest tip de cooperare.

2. Necesitatea unor probe electronice în raport cu tratatele de asistență judiciară reciprocă și cu ordinul european de anchetă

CEPD ia act de angajamentul Comisiei de a revizui obstacolele din calea anchetei penale, în special în ceea ce privește chestiunea accesului la probele electronice. În expunerea sa de motive, Comisia prezintă contextul propunerii și subliniază caracterul volatil al probelor electronice, dimensiunea lor internațională, precum și necesitatea de a adapta mecanismul de cooperare la era digitală. Propunerile de regulament și de directivă privind transferul și accesarea probelor electronice nu urmăresc să înlocuiască instrumentele de cooperare în materie penală anterioare, cum ar fi Convenția de la Budapesta, Tratatul de asistență judiciară reciprocă și ordinul european de anchetă (Directiva privind ordinul european de anchetă). Potrivit Comisiei, propunerile privind probele electronice vizează îmbunătățirea cooperării judiciare în materie penală între autoritățile și furnizorii de servicii din Uniunea Europeană, precum și cu țările terțe, în special cu Statele Unite ale Americii.

Întrucât aceste noi instrumente suplimentare vor fi dedicate în mod specific accesului la probe electronice și transferului acestora, CEPD va evalua valoarea adăugată a instrumentelor în ceea ce privește Directiva privind ordinul european de anchetă și Tratatul de asistență judiciară reciprocă.

a) Necesitatea unor probe electronice în raport cu garanțiile oferite de ordinul european de anchetă și tratatele de asistență judiciară reciprocă

Principalul argument invocat de Comisie în favoarea propunerilor privind probele electronice constă în accelerarea procesului de obținere și colectare a probelor electronice care sunt stocate și/sau deținute de furnizorii de servicii stabiliți în altă jurisdicție.

Cu toate acestea, CEPD regretă faptul că necesitatea de a dispune de un nou instrument pentru a organiza accesul la probele electronice nu a fost demonstrată în evaluarea impactului. Într-adevăr, propunerile nu demonstrează că nu ar fi putut fi utilizat un alt mijloc mai puțin intruziv pentru a

realiza obiectivul propunerii privind probele electronice, deși ar fi putut fi avute în vedere soluții alternative. De exemplu, posibilitatea de a modifica și a îmbunătăți Directiva privind ordinul european de anchetă ar fi putut fi examinată și ar fi răspuns, de asemenea, cerinței specifice, în temeiul Directivei privind ordinul european de anchetă, de a evalua necesitatea de a modifica textul până la 21 mai 2019[3]. O altă opțiune ar fi fost de a prevedea utilizarea unor ordine de păstrare a probelor electronice pentru a îngheța datele, atât timp cât a fost emisă o cerere formală bazată pe un tratat de asistență reciprocă. Aceste opțiuni ar fi permis menținerea garanțiilor prevăzute în cadrul acestor instrumente, asigurându-se în același timp că datele cu caracter personal solicitate nu sunt șterse.

CEPD ia notă de faptul că termenele stabilite în Directiva privind ordinul european de anchetă sunt mai lungi decât cele prevăzute în propunerea privind probele electronice. Într-adevăr, autoritatea de executare are la dispoziție 30 de zile pentru a lua o decizie cu privire la recunoașterea cererii[4], iar ulterior va executa ordinul în termen de 90 de zile[5]. CEPD consideră că acordarea unui termen de 30 de zile de reflecție pentru autoritățile de executare în cazul ordinului european de anchetă este o garanție esențială care le permite acestora să evalueze dacă cererea de executare este întemeiată și respectă toate condițiile pentru emiterea și transmiterea unui ordin european de anchetă[6].

CEPD este preocupat de faptul că termenul de 10 zile prezentat în propunerile privind probele electronice pentru emiterea certificatului de ordin european de divulgare a probelor electronice (EPOC), fără nicio perioadă de reflecție, împiedică o evaluare corespunzătoare a măsurii în care certificatul de ordin european de divulgare a probelor electronice întrunește toate criteriile și este completat în mod corect.

Prin urmare, CEPD recomandă ca destinatarul certificatului de ordin european de divulgare a probelor electronice să dispună de mai mult timp pentru a stabili dacă ordinul ar trebui sau nu să fie executat.

CEPD menționează că, în cazul unui certificat de ordin european de păstrare a probelor electronice (EPOC-PR), nu există nicio garanție că păstrarea datelor se va limita la ceea ce este necesar pentru divulgarea datelor. Într-adevăr, durata de păstrare a datelor poate depăși 60 de zile, întrucât nu este prevăzut un termen în care autoritatea emitentă informează destinatarul să nu emită sau să retragă un ordin de divulgare. Prin urmare, CEPD recomandă cel puțin stabilirea unui termen pentru ca autoritatea emitentă să nu emită sau să retragă ordinul de divulgare, pentru a respecta principiul minimizării datelor stabilit în RGPD[7].

În cele din urmă, CEPD menționează că Directiva privind ordinul european de anchetă prevede restituirea probelor de către statul emitent către autoritatea de executare[8]. Cu toate acestea, propunerea de regulament privind probele electronice nu menționează o astfel de posibilitate. Nu este clar ce se întâmplă cu probele electronice după transmiterea acestora către autoritatea emitentă.

Prin urmare, CEPD recomandă ca propunerea de regulament să furnizeze mai multe informații cu privire la utilizarea probelor electronice după transferul lor către autoritatea emitentă în scopul de a

[3] A se vedea articolul 37 din Directiva privind ordinul european de anchetă.
[4] Articolul 12 alineatul (3) din Directiva privind ordinul european de anchetă.
[5] Articolul 12 alineatul (4) din Directiva privind ordinul european de anchetă.
[6] Articolul 6 din Directiva privind ordinul european de anchetă.
[7] Articolul 5 alineatul (1) litera (c) din RGPD.
[8] Articolul 13 alineatele (3) și (4) din Directiva privind ordinul european de anchetă.

respecta RGPD și principiul transparenței[9], precum și principiul specificității stabilit prin tratatele de asistență judiciară reciprocă.

b) Abandonarea principiului dublei incriminări

CEPD admite că recunoașterea reciprocă depinde de aplicarea principiului dublei incriminări, care este o modalitate prin care statele membre își mențin suveranitatea. Cu toate acestea, dubla incriminare este considerată din ce în ce mai mult drept un obstacol în calea cooperării judiciare. Statele membre ale UE sunt din ce în ce mai dispuse să coopereze, chiar dacă măsurile de investigare vizează acte care nu sunt considerate infracțiuni în legislația lor națională. Cu toate acestea, CEPD reamintește că principiul dublei incriminări urmărește să ofere o garanție suplimentară pentru a se asigura că un stat nu poate recurge la asistența unui alt stat pentru a aplica o sancțiune penală care nu există în dreptul unui alt stat. Acest lucru ar împiedica, de exemplu, un stat să solicite ajutorul unui alt stat pentru a priva de libertate o persoană pentru opiniile sale politice, în cazul în care aceste opinii nu sunt incriminate în statul vizat de solicitare, sau pentru a urmări penal o persoană care a recurs la o întrerupere de sarcină, în cazul în care persoana respectivă își are reședința într-un alt stat în care acest lucru nu este ilegal. De asemenea, principiul dublei incriminări este însoțit adesea de limitări sau de garanții suplimentare în ceea ce privește sancțiunile în cazul în care acestea diferă prea mult între statul care transmite solicitarea și statul de executare. Principalul exemplu este angajamentul de a nu aplica pedeapsa cu moartea în cadrul anumitor tratate de asistență judiciară reciprocă atunci când aceasta nu este prevăzută în legislația uneia dintre cele două părți.

CEPD constată că principiul dublei incriminări nu este inclus în propunerea de regulament privind probele electronice. Aceasta are însă drept rezultat nu numai eliminarea formalităților obișnuite de recunoaștere reciprocă, ci și eliminarea garanțiilor legate de principiul dublei incriminări.

Într-adevăr, CEPD menționează că nu se face nicio trimitere la legislația țării în care este stabilit furnizorul de servicii vizat de solicitare și că ordinul de păstrare a oricăror date, precum și de divulgare a datelor privind abonații și accesul poate fi emis pentru toate infracțiunile[10], indiferent dacă există sau nu infracțiuni similare prevăzute în alte state membre.

Între timp, ordinele de divulgare pot fi emise și executate numai dacă o măsură similară este disponibilă pentru aceeași infracțiune într-o situație internă comparabilă din statul emitent[11]. În plus, conform explicațiilor Comisiei din expunerea de motive a propunerii de regulament, se stabilește specificitatea datelor privind operațiunile sau a datelor referitoare la conținut, întrucât acestea sunt considerate a fi mai sensibile. Într-adevăr, ordinele referitoare la datele privind operațiunile sau datele referitoare la conținut se bazează pe un prag pentru o pedeapsă maximă cu închisoarea de cel puțin trei ani în scopul de a asigura respectarea principiului proporționalității și a drepturilor persoanelor afectate[12]. Cu toate acestea, CEPD subliniază că încă nu a existat o armonizare în cadrul UE în ceea ce privește infracțiunile penale sancționate cu pedeapsa cu închisoarea pentru o perioadă maximă de cel puțin trei ani.

CEPD se opune renunțării la principiul dublei incriminări, care are scopul de a asigura că un stat nu poate să apeleze la ajutorul altor state pentru ca dreptul său penal național să fie aplicat în afara teritoriului statului de către un stat care nu a adoptat aceeași abordare, în special având în vedere dispariția altor garanții importante tradiționale în domeniul dreptului penal [a se vedea punctul 3 de

[9] Articolul 5 alineatul (1) litera (a) din RGPD.
[10] Articolul 5 alineatul (3) și articolul 6 alineatul (2) din propunerea de regulament privind probele electronice.
[11] Articolul 5 alineatul (2) din propunerea de regulament privind probele electronice.
[12] Articolul 5 alineatul (4) litera (a) din propunerea de regulament privind probele electronice.

mai jos privind criteriile de localizare și punctul 7 litera (g) privind potențialele conflicte cu legislațiile țărilor terțe].

c)Consecința adresării directe către societățile comerciale

CEPD recunoaște faptul că probele electronice sunt disponibile din ce în ce mai mult pe infrastructura privată și pot fi localizate în afara țării de investigare și deținute de furnizorii de servicii.

CEPD constată că, în urma deciziilor în cauzele *Yahoo!* [13] și *Skype*[14] din Belgia, precum și în contextul atacurilor teroriste, este necesară o cooperare mai facilă și mai rapidă între entitățile publice și private. În evaluarea impactului, Comisia se referă la trei tipuri de instrumente procedurale care implică atât autoritățile publice, cât și furnizorii de servicii. Acestea sunt cooperarea judiciară, cooperarea directă și accesul direct. În timp ce primul dintre acestea nu plasează responsabilitatea de a executa ordinul european de anchetă asupra furnizorului de servicii, ci asupra autorității de executare[15], cel de al doilea instrument, cooperarea directă, se bazează pe cooperarea furnizorului de servicii. Cel mai intruziv din perspectiva unui furnizor de servicii este accesul direct, întrucât autoritățile publice sunt în măsură să acceseze datele fără ajutorul unui intermediar.

Prin urmare, CEPD exprimă temerea că, atunci când sunt abordați în mod direct, furnizorii de servicii nu vor asigura protecția datelor cu caracter personal la fel de eficient precum sunt capabile și obligate autoritățile publice și subliniază faptul că aceasta conduce, de asemenea, la inaplicabilitatea anumitor garanții procedurale prevăzute în contextul cooperării judiciare pentru persoane fizice, precum și pentru societățile în sine[16]. Într-adevăr, de exemplu, un furnizor de servicii solicitat ar trebui să se prezinte în fața instanței unui alt stat (membru) pentru a contesta ordinul în timp ce, în contextul cooperării judiciare, acesta ar trebui să trateze cu autoritățile din statul în care este stabilit. CEPD recomandă includerea unor temeiuri suplimentare în propunerea de regulament care să certifice faptul că furnizorii de servicii vor proteja drepturile individuale fundamentale, cum ar fi protecția datelor cu caracter personal și respectarea vieții private și de familie, precum și informațiile furnizate de autoritatea competentă de protecție a datelor în scopul de a asigura controlul.

3. Noul motiv de competență și așa-numita dispariție a criteriilor de localizare

CEPD remarcă faptul că, așa cum subliniază Comisia, una dintre modificările majore aduse de aceste propuneri este dispariția criteriilor de localizare și posibilitatea ca autoritățile competente să solicite divulgarea și păstrarea datelor indiferent de locul în care aceste date sunt stocate efectiv.

Din perspectiva protecției datelor, nu este o noutate că legislația UE privind protecția datelor se aplică indiferent de locul în care sunt stocate datele persoanelor în cauză. Într-adevăr, aplicabilitatea RGPD depinde fie de faptul că operatorul sau persoana împuternicită de operator este stabilită pe

[13] Hof van Cassatie of Belgium, YAHOO! Inc., nr. P.13.2082.N din 1 decembrie 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, Nr. ME20.F1.105151-12 din 27 octombrie 2016. (Skype a atacat decizia).
[15] Articolele 10-16.
[16] A se vedea, de asemenea, din perspectiva protecției datelor la nivel internațional, „Documentul de lucru privind standardele pentru protecția datelor și a vieții private în cererile de date la nivel transfrontalier în scopul aplicării legii", Grupul de lucru internațional pentru protecția datelor în sectorul telecomunicațiilor, cea de a 63-a reuniune, 9-10 aprilie 2018, Budapesta (Ungaria).

teritoriul UE, fie de faptul dacă sunt prelucrate date ale persoanelor vizate din UE, inclusiv atunci când operatorul sau persoana împuternicită de operator nu este stabilită pe teritoriul UE[17], caz în care aceasta trebuie, de asemenea, să desemneze un reprezentant legal în UE[18]. Din perspectiva protecției datelor, este important de remarcat faptul că domeniul de aplicare teritorial extins urmărește să ofere o protecție mai completă persoanelor vizate din UE, indiferent de locul în care este stabilită societatea care le prelucrează datele.

Prin urmare, deși dispariția criteriilor de localizare ar putea reprezenta o noutate în domeniul dreptului penal, aceasta nu apare ca o schimbare majoră din perspectiva protecției datelor. În plus, CEPD menționează, de asemenea, că o legătură continuă să fie menținută pe teritoriul UE, întrucât numai furnizorii de servicii care oferă servicii în cadrul Uniunii intră în domeniul de aplicare a propunerilor, iar faptul că cererile pot fi abordate numai în contextul cercetărilor penale implică o legătură cu UE (fie pentru că infracțiunea a fost comisă pe teritoriul unui stat membru, fie pentru că victima sau infractorul era cetățean al unui stat membru).

În cazul în care dispariția criteriilor de localizare ar trebui aplicată în prezent în dreptul penal, cea mai importantă întrebare pentru CEPD se referă la modul de a asigura că o astfel de evoluție nu afectează protecția datelor și drepturile procedurale penale ale persoanelor vizate și ale furnizorilor de servicii care au primit solicitarea. Din această perspectivă, CEPD recunoaște că, în cadrul UE, garanțiile procedurale au fost armonizate, cel puțin parțial, și trebuie furnizate în conformitate cu Convenția europeană a drepturilor omului. Prin urmare, se poate argumenta că dispariția criteriilor de localizare ar avea, probabil, consecințe mai limitate atunci când probele sunt solicitate în cadrul UE în comparație cu situația inversă în care autoritățile din țări terțe solicită date societăților stabilite pe teritoriul UE în aceleași condiții ca cele prevăzute în proiectul de regulament privind probele electronice. Într-adevăr, CEPD este preocupat în special de faptul că acest lucru ar putea conduce la situații mai problematice. În acest context, autoritățile dintr-o țară terță în care se aplică garanții procedurale diferite și eventual mai puține în domeniul dreptului penal ar putea avea acces la date care ar fi protejate prin garanții suplimentare în cadrul UE. Din această perspectivă, CEPD își reafirmă preocupările cu privire la un standard dublu și la o slăbire a drepturilor fundamentale atunci când furnizorii de servicii și persoanele vizate nu beneficiază de garanțiile procedurale prevăzute în legislația UE în cazul în care cererea este prezentată de o autoritate dintr-o țară terță.

În plus, întrucât acest nou motiv de competență „indiferent de localizarea datelor" este însoțit de o procedură care se bazează în principal pe solicitări directe din partea autorităților competente către furnizorii de servicii, CEPD este preocupat de faptul că garanțiile privind protecția datelor ar putea să nu fie aplicate de către societățile private care primesc cereri și care nu sunt obligate să respecte un instrument juridic cum ar fi un tratat de asistență judiciară reciprocă, care reglementează în mod tradițional schimburile de date între autoritățile judiciare și care prevede garanții. În special, în contextul tratatelor de asistență judiciară reciprocă, garanțiile minime în materie de protecție a datelor implică, de exemplu, obligațiile de confidențialitate și principiul specificității, ceea ce presupune faptul că datele nu vor fi prelucrate în alt scop.

Cel puțin, CEPD reamintește că ar trebui să se aplice garanțiile prevăzute în Directiva 2016/680, inclusiv în ceea ce privește transferurile de date, în special articolul 39 în cazul în care furnizorul de servicii ar fi stabilit într-o țară terță fără o decizie privind caracterul adecvat în acest domeniu. În special, CEPD subliniază că această dispoziție implică, în special, informarea autorității competente pentru protecția datelor din statul membru din care face parte autoritatea emitentă a ordinului

[17] A se vedea articolul 3, în special alineatul (2).
[18] A se vedea articolul 27.

(ordinelor) și a documentației aferente transferului, inclusiv în ceea ce privește justificarea privind ineficacitatea sau caracterul inadecvat al unui transfer către autoritatea competentă din țara terță.

4. Noțiunea de „furnizori de servicii” ar trebui restrânsă sau completată de garanții suplimentare pentru drepturile persoanelor vizate

În ceea ce privește furnizorii de servicii, CEPD salută definiția largă care permite includerea atât a serviciilor de comunicații, cât și a serviciilor OTT, întrucât toate aceste servicii sunt echivalente din punct de vedere funcțional și, prin urmare, măsurile prevăzute ar putea avea un impact similar asupra dreptului la viață privată și asupra dreptului la confidențialitatea comunicațiilor, așa cum se subliniază în declarația GL29 și, anterior, în Avizul 01/2017 cu privire la propunerea de regulament privind viața privată și comunicațiile electronice. Într-adevăr, propunerea de regulament privind probele electronice vizează furnizorii de servicii care furnizează servicii de comunicații electronice, așa cum sunt definite la articolul 2 alineatul (4) din Directiva de instituire a Codului european al comunicațiilor electronice, servicii ale societății informaționale, așa cum sunt definite la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535, „pentru care stocarea datelor este o componentă definitorie a serviciului furnizat utilizatorului, inclusiv rețelele sociale, piețe online care facilitează tranzacțiile între utilizatorii lor sau alți furnizori de servicii de găzduire” sau serviciile de alocare de nume de domenii de internet și de adrese IP „cum ar fi furnizorii de adrese IP, registrele de nume de domenii, operatorii de registre de nume de domenii și serviciile de anonimizare și proxy conexe”[19].

Cu toate acestea, întrucât un furnizor de servicii în sensul proiectului de regulament este „orice persoană fizică sau juridică care oferă una sau mai multe dintre următoarele categorii de servicii”, CEPD este preocupat de faptul că acest instrument ar putea viza atât operatorii, cât și persoanele împuternicite de operatori în sensul RGPD. Într-adevăr, întrucât „oferirea de servicii”, așa cum este definită la articolul 2 alineatul (4) din proiectul de regulament, include permiterea atât persoanelor juridice, cât și persoanelor fizice din unul sau mai multe state membre să utilizeze serviciile enumerate și crearea unei legături strânse cu statul (statele) membru (membre) în cauză, aceste activități includ activitățile desfășurate de o persoană împuternicită de operator pentru un operator, cum ar fi stocarea de date, de exemplu.

Prin urmare, CEPD se teme că, în lipsa unor limitări ale furnizorilor de servicii care acționează în calitate de operatori în sensul RGPD și fără nicio obligație specifică a persoanei împuternicite de operator de a notifica operatorul de date atunci când primește un ordin de divulgare sau de păstrare, drepturile persoanelor vizate ar putea fi eludate. Acest lucru este valabil în special în cazul în care, în contextul posibilelor obligații conflictuale care împiedică destinatarul să răspundă ordinelor primite, autoritățile judiciare sunt încurajate, de asemenea, în proiectul de regulament, să se adreseze celui mai adecvat factor, indiferent de normele aplicabile în materie de protecție a datelor, în special având în vedere faptul că orice date ar putea fi solicitate, și nu doar datele cu caracter personal care fac obiectul RGPD[20].

În conformitate cu RGPD, o persoană împuternicită de operator acționează numai în conformitate cu instrucțiunile date de operator. Prin urmare, este responsabilitatea operatorului să asigure

[19] Articolul 2 alineatul (3) litera (c) din propunerea de regulament privind probele electronice.
[20] A se vedea articolul 7 alineatele (3) și (4).

respectarea drepturilor persoanelor vizate și să pună la dispoziția acestora informațiile relevante, inclusiv în ceea ce privește destinatarii datelor lor, de exemplu în contextul exercitării dreptului lor de acces. Persoana împuternicită de operator nu va primi aceste cereri de la persoanele vizate și nu va fi în măsură să răspundă, cu excepția cazului în care acest lucru este solicitat în mod expres de către operator.

Prin urmare, cu excepția cazului în care drepturile lor au fost limitate în ceea ce privește aplicarea RGPD, CEPD subliniază că persoanele vizate care beneficiază de aplicarea RGPD ar putea să nu își exercite drepturile în mod eficient în cazul în care operatorul nu este în măsură să furnizeze informații complete. CEPD menționează, de asemenea, că probabilitatea absenței informațiilor este chiar mai mare în lipsa unei obligații specifice impuse persoanei împuternicite de operator de a informa operatorul atunci când datele solicitate se referă la persoanele vizate care nu beneficiază de protecția acordată prin RGPD. Într-adevăr, autoritățile judiciare care solicită date nu vor avea neapărat obligația de a informa persoanele vizate cu privire la prelucrarea lor ulterioară în acest caz. Prin urmare, CEPD face apel la restricționarea domeniului de aplicare la operatorii în sensul RGPD sau la introducerea unei dispoziții care să clarifice faptul că, în cazul în care furnizorul de servicii vizat de solicitare nu este operatorul datelor, acesta informează operatorul.

5. Noțiunile de „sediu” și de „reprezentant legal” în contextul acestor propuneri ar trebui să se distingă în mod clar de noțiunile în contextul RGPD

Având în vedere inaplicabilitatea criteriilor de localizare în ceea ce privește datele, destinatarii ordinelor de divulgare și de păstrare care intră în domeniul de aplicare a propunerii de regulament se limitează la furnizorii de servicii care oferă servicii în Uniune, indiferent dacă sunt stabiliți sau nu în UE, cu obligația de a numi un reprezentant legal, în conformitate cu normele propuse în proiectul de directivă. Prin urmare, aceste noțiuni de „sediu” și de „reprezentant legal” sunt definite în proiectele de instrumente.

CEPD menționează că aceste noțiuni apar, de asemenea, în contextul altor instrumente ale UE, în special în cadrul RGPD. În consecință, ar trebui să se furnizeze clarificări cu privire la definirea și delimitarea acestor noțiuni în contextul proiectelor de propuneri și în contextul RGPD.

a) Sediu

CEPD reamintește, de asemenea, că noțiunea de „sediu” în contextul proiectului de regulament nu trebuie confundată cu noțiunea din cadrul RGPD. Într-adevăr, în sensul proiectului de regulament, noțiunea de sediu, astfel cum este definită la articolul 2 alineatul (5), este mai largă decât cea din RGPD deoarece include „fie exercitarea efectivă a unei activități economice pentru o perioadă nedeterminată prin intermediul unei infrastructuri stabile de unde este exercitată activitatea de prestare de servicii, fie o infrastructură stabilă de unde este gestionată activitatea”, indiferent dacă prelucrarea datelor cu caracter personal are sau nu loc în cadrul activităților acestui sediu. Prin urmare, deși conceptul de „sediu” în sensul RGPD este, fără îndoială, inclus în conceptul de „sediu” definit în proiectul de regulament, este posibil să nu fie valabil și contrariul.

Prin urmare, CEPD avertizează că este posibil ca existența unor sedii ale furnizorilor de servicii în sensul proiectului de regulament să nu implice în mod necesar îndeplinirea condițiilor de aplicare a

RGPD în conformitate cu articolul 3 alineatul (1). În acest context, operatorii și persoanele împuternicite de operatori sunt invitate, prin urmare, să verifice dacă aplicabilitatea RGPD nu derivă din articolul 3 alineatul (2), ceea ce ar implica desemnarea unui reprezentant legal în cadrul UE și absența unui sistem de ghișeu unic.

b) Reprezentant legal

În declarația sa, GL29 a subliniat că ar trebui evitată orice confuzie între obligația de a desemna un reprezentant legal în temeiul articolului 27 din RGPD și reprezentantul legal prevăzut în proiectul de regulament privind probele electronice.

În cazul proiectului de propunere, CEPD ar dori să reamintească aceste recomandări și, în special, să sublinieze faptul că, în opinia sa, reprezentantul legal în sensul proiectului de directivă privind numirea unui reprezentant legal în contextul propunerilor privind probele electronice este desemnat în toate cazurile, este învestit cu funcții specifice, independent de mandatul oferit de furnizorul de servicii, are competența de a răspunde cererilor și de a acționa în numele furnizorului de servicii și deține o răspundere mai mare decât reprezentantul legal prevăzut în RGPD.

În plus, CEPD subliniază că obligația de a desemna în toate cazurile un reprezentant legal în temeiul proiectelor de propuneri privind probele electronice, indiferent dacă furnizorul de servicii este stabilit sau nu în UE, posibilitatea de a desemna chiar mai mulți reprezentanți legali pentru același furnizor de servicii în temeiul proiectului de directivă privind probele electronice, precum și obligația de a notifica desemnarea reprezentantului legal autorităților statelor membre diferă de RGPD, care nu prevede o astfel de obligație de a notifica reprezentantul legal desemnat, derogările de la desemnare și responsabilitățile limitate ale reprezentantului legal.

Prin urmare, având în vedere diferențele semnificative în ceea ce privește rolul, răspunderea și relația cu celelalte sedii ale furnizorului de servicii, într-un caz, și ale operatorului sau persoanei împuternicite de operator, în celălalt caz, CEPD recomandă ca, în cazul în care un furnizor de servicii nu este stabilit în UE, dar face obiectul atât al RGPD, în temeiul articolului 3 alineatul (2), cât și al Regulamentului privind probele electronice, ar trebui să fie desemnați doi reprezentanți legali distincți, fiecare cu funcții clar diferite, în conformitate cu instrumentul pe baza căruia este desemnat fiecare reprezentant.

6. Noile categorii de date

Propunerea de regulament definește diferite categorii de date la articolul 2: date privind abonații, date privind accesul, date privind operațiunile și date referitoare la conținut. Considerentul 20 din propunerea Comisiei prevede, de asemenea, că *„categoriile de date reglementate de prezentul regulament includ datele privind abonații, datele privind accesul, datele privind operațiunile (aceste trei categorii fiind denumite în continuare «date care nu se referă la conținut») și datele referitoare la conținut. Această distincție, în afară de datele privind accesul, există în legislația multor state membre și, de asemenea, în actualul cadru juridic al SUA care permite furnizorilor de servicii să partajeze în mod voluntar datele care nu se referă la conținut cu autoritățile străine de aplicare a legii”.*

În acest context, CEPD subliniază, în primul rând, că toate cele patru categorii de date menționate mai sus trebuie considerate date cu caracter personal în conformitate cu legislația UE privind

protecția datelor, întrucât acestea conțin informații referitoare la o persoană fizică identificată sau identificabilă, indiferent dacă persoana vizată este denumită „abonat” sau „utilizator” în propunerea de regulament. În mod similar, trebuie remarcat faptul că „probele electronice”, astfel cum sunt definite la articolul 2 alineatul (6) din propunerea Comisiei, cuprind toate cele patru categorii de date și, prin urmare, se referă la date cu caracter personal. În consecință, în loc să stabilească normele privind accesul la probe, definite și clasificate în conformitate cu legislația națională și procedurile judiciare, regulamentul propus prevede noi condiții de fond și procedurale legate de accesul la datele cu caracter personal.

În timp ce regulamentul propus stabilește noi subcategorii de date cu caracter personal pentru care se aplică condiții procedurale de acces diferite, CEPD reamintește că, în conformitate cu jurisprudența relevantă a CJUE, pentru a stabili existența unei atingeri aduse dreptului fundamental la viață privată nu contează dacă informațiile cu privire la viețile private în cauză sunt sensibile sau dacă persoanele în cauză au fost puse în situații dificile în orice mod.

În plus, CEPD reamintește că, în ceea ce privește „datele care nu se referă la conținut”, care cuprind datele privind abonații, datele privind accesul și datele privind operațiunile în conformitate cu propunerea Comisiei, Curtea de Justiție a Uniunii Europene a decis, în hotărârea sa în cauzele conexate C-203/15 și C-698/15, *Tele 2 Sverige AB*, că metadatele precum datele privind traficul și datele privind localizarea oferă mijloace de stabilire a unui profil al persoanelor vizate, iar aceste informații nu sunt mai puțin sensibile, având în vedere dreptul la viață privată, decât conținutul real al comunicărilor[21].

Așa cum s-a precizat deja în declarația GL29 din 29 noiembrie 2017privind protecția datelor și aspectele de confidențialitate ale accesului transfrontalier la probele electronice, CEPD își reiterează, prin urmare, îndoielile și preocupările în ceea ce privește delimitarea actuală între datele care nu se referă la conținut și datele care se referă la conținut, precum și cele patru categorii de date cu caracter personal prevăzute în propunerea de regulament. Într-adevăr, cele patru categorii propuse nu par să fie clar delimitate, iar definiția „datelor privind accesul” rămâne încă vagă, în comparație cu celelalte categorii. Prin urmare, CEPD regretă faptul că evaluarea impactului și propunerea elaborate de Comisie nu au justificat în continuare motivul creării acestor noi subcategorii de date cu caracter personal și își exprimă preocupările în ceea ce privește diferitele niveluri de garanții legate de condițiile de fond și procedurale pentru accesul la categoriile de date cu caracter personal, în special având în vedere dificultatea practică de a evalua în ce categorie de date se vor încadra datele solicitate în unele cazuri. De exemplu, adresele IP ar putea fi clasificate atât ca date privind operațiunile, cât și ca date privind abonații.

În acest context, CEPD reamintește, de asemenea, că în considerentul 14 din propunerea sa de regulament privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice (Regulamentul privind viața privată și comunicațiile electronice), Comisia consideră că „datele transmise în cadrul comunicațiilor electronice ar trebui să fie definite într-un mod suficient de larg și de neutru din punct de vedere tehnologic astfel încât să cuprindă orice informații referitoare la conținutul transmis sau schimbat (conținutul comunicațiilor electronice) și informațiile cu privire la un utilizator final de servicii de comunicații electronice prelucrate în vederea transmiterii, a distribuirii sau a schimbului de conținut al comunicațiilor electronice, inclusiv datele pentru urmărirea și identificarea sursei și a destinației unei comunicații, a localizării geografice, precum și a datei, orei, duratei și tipului de comunicare”. Dat fiind că actualul și viitorul cadru privind viața privată și comunicațiile electronice, precum și limitările aferente ale dreptului la viață privată se

[21] Hotărârea CJUE din 21 decembrie 2016, punctul 99.

vor aplica normelor care reglementează accesul la probele electronice în scopul aplicării legii, CEPD recomandă ca propunerea de regulament să includă o definiție mai largă a datelor transmise în cadrul comunicațiilor electronice, astfel încât să se asigure că garanțiile și condițiile adecvate de acces care urmează să fie stabilite acoperă în mod consecvent atât „datele care nu se referă la conținut", cât și „datele care se referă la conținut".

7. Analiza procedurilor pentru ordinele europene de divulgare și de păstrare a probelor electronice

În sens larg, procedura de adresare a unui ordin de divulgare sau de păstrare pare să fie următoarea:

- Autoritatea judiciară competentă – autoritatea emitentă – în funcție de tipul de date solicitat și de tipul de ordin, emite ordinul în conformitate cu condițiile (reduse) enumerate la articolele 5 și 6, apoi îl trimite reprezentantului legal al furnizorului de servicii sau la oricare dintre sediile sale din cadrul UE – destinatarul – utilizând un certificat armonizat.

- La primirea certificatului, destinatarul execută ordinul – în sensul că acesta transmite datele în termen de 10 zile sau de 6 ore în caz de urgență, sau le păstrează până la 60 de zile – cu excepția cazului în care acest lucru este imposibil deoarece certificatul este incomplet sau din motive de forță majoră sau de imposibilitate *de facto* pentru destinatar, sau din cauză că destinatarul refuză pe motiv de obligații contradictorii fie cu privire la respectarea drepturilor fundamentale sau a intereselor fundamentale ale unei țări terțe, fie din alte motive.

- În cazul în care destinatarul nu a respectat ordinul primit fără a oferi motive acceptate de autoritatea emitentă, sunt prevăzute proceduri de executare a ordinelor de către o autoritate competentă de executare din statul membru în care furnizorul de servicii este reprezentat sau instituit, cu excepția cazului în care se aplică motivele de refuz limitate, iar autoritatea de executare se opune recunoașterii sau executării ordinului.

- În cazul în care destinatarul a formulat o obiecție motivată cu privire la ordin pe motiv de obligații contradictorii, autoritatea emitentă înaintează cazul instanței competente din statul său membru, căreia îi revine în consecință să evalueze posibilul conflict și să mențină ordinul în absența unui conflict. În cazul unui conflict, instanța competentă fie se adresează autorităților centrale din țara terță prin intermediul autorităților sale centrale naționale, stabilind un termen de 15 zile pentru furnizarea unui răspuns, care poate fi prelungit cu 30 de zile în urma unei cereri motivate în caz de obligații contradictorii în ceea ce privește drepturile fundamentale sau interesele fundamentale ale unei țări terțe, fie stabilește ea însăși dacă menține sau retrage ordinul din alte motive de refuz invocate de către destinatar.

- Fără a aduce atingere căilor de atac disponibile în temeiul RGPD și al Directivei privind aplicarea legii, persoanele ale căror date au fost obținute prin intermediul unui ordin de divulgare au, de asemenea, dreptul la căi de atac eficiente împotriva ordinului respectiv.

CEPD a evaluat procedurile prevăzute și garanțiile stabilite în proiectul de regulament pentru a acoperi diferitele etape, iar pentru fiecare dintre aspectele prezentate în continuare recomandă următoarele măsuri de protecție și modificări.

a) Pragurile pentru emiterea ordinelor ar trebui să fie ridicate, iar ordinele ar trebui să fie emise sau autorizate de către instanțe

În ceea ce privește condițiile pentru emiterea ordinelor, CEPD salută principiul asigurării unor garanții mai mari pentru a avea acces la datele privind operațiunile sau datele referitoare la conținut. Cu toate acestea, Comisia constată că, având în vedere absența unei armonizări depline a sancțiunilor penale între statele membre, trimiterea la „infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani”[22] implică în continuare praguri divergente și discrepanțe în ceea ce privește protecția datelor lor cu privire la persoanele vizate din cadrul UE.

În plus, CEPD subliniază că, având în vedere în special definiția largă a datelor privind abonații, pragul prevăzut pare mai degrabă mic pentru ordinele de păstrare și pentru ordinele de divulgare referitoare la datele privind abonații sau privind accesul, întrucât toate infracțiunile pot, în principiu, să justifice emiterea unor astfel de ordine. În mod similar, autoritățile abilitate să emită astfel de ordine sunt mai limitate în ceea ce privește ordinele de divulgare a probelor electronice care vizează datele privind operațiunile sau datele referitoare la conținut, decât pentru emiterea ordinelor de păstrare sau a ordinelor de divulgare a probelor electronice care vizează date privind abonații și date privind accesul, întrucât procurorii pot emite sau autoriza numai cele din urmă ordine, în timp ce orice judecător, instanță judecătorească sau judecător de instrucție poate emite sau autoriza orice ordin.

În special, CEPD regretă faptul că cel mai scăzut prag care prevede posibilitatea ca autoritățile de aplicare a legii să solicite acces la datele privind abonații și datele privind accesul pentru orice infracțiune se bazează pe o interpretare „a contrario” a jurisprudenței CJUE (care se axează pe alte date) pentru a face distincții precum garanțiile care urmează să fie acordate. Într-adevăr, CJUE a subliniat în mod special că, pentru datele privind traficul și localizarea, accesul autorităților competente este limitat numai la combaterea infracțiunilor grave[23]. CEPD ar putea înțelege că propunerea ar oferi posibilitatea de a solicita accesul la informații de bază care ar permite doar identificarea unei persoane fără a dezvălui niciun fel de date transmise în cadrul comunicațiilor fără o autorizare prealabilă din partea unei instanțe. Cu toate acestea, CEPD deplânge interpretarea „a contrario” a acestei hotărâri de către Comisie și solicită introducerea unor garanții mai mari pentru a limita motivele de acces la alte date privind abonații și la datele privind accesul. CEPD sugerează restricționarea accesului la aceste date fie la o listă de infracțiuni prevăzute în proiectul de regulament, fie cel puțin la „infracțiuni grave”, având în vedere, în special, pragul inferior al autorizării prealabile prevăzut pentru aceste date.

În plus, CEPD subliniază că această interpretare „ a contrario ” conduce, de asemenea, la faptul că propunerea oferă procurorilor posibilitatea de a emite sau de a autoriza emiterea de ordine. CEPD este de opinie că, exceptând cazul solicitărilor de informații de bază care ar permite identificarea unei persoane fără a dezvălui datele transmise în cadrul comunicațiilor, acest lucru constituie un pas înapoi în comparație cu jurisprudența CJUE privind accesul la datele privind comunicațiile. Într-adevăr, în jurisprudența sa privind accesul la datele transmise în cadrul comunicațiilor în scopul aplicării legii, CJUE a limitat posibilitatea de a furniza un astfel de acces, printre alte criterii, și *„cu*

[22] A se vedea articolul 5 alineatul (3) litera (a).
[23] A se vedea cauza 203/15 – punctul 125.

excepția unor situații de urgență justificate corespunzător"[24], la „*un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă*", „*în urma unei cereri motivate formulate de autoritățile respective în cadrul unor proceduri de prevenire, de detectare sau de urmărire penală*". [25]

CEPD reamintește că noțiunea de „instanță judecătorească" este o noțiune autonomă a dreptului UE și că CJUE a subliniat în mod constant și a reamintit criteriile care trebuie îndeplinite pentru a fi considerată drept o instanță judecătorească, inclusiv criteriile de independență[26], ceea ce nu pare a fi cazul procurorilor, astfel cum a reamintit, de asemenea, CEDO în jurisprudența sa[27].

În consecință, articolul 4 alineatul (1) literele (a) și (b) și articolul 3 literele (a) și (b) au ca rezultat proceduri în care se vor aplica garanții în mod semnificativ mai reduse pentru datele privind abonații și datele privind accesul, întrucât un procuror va putea solicita de unul singur date, fără niciun alt control din partea autorității statului din care provin datele solicitate sau din partea autorității de care va ține reprezentantul legal al societății vizate de solicitare și fără niciun control din partea unei autorități administrative independente.

În plus, CEPD ia notă de așa-numitele garanții suplimentare prevăzute la articolul 5 alineatul (2), care limitează posibilitatea de a emite un ordin de divulgare atunci când o măsură similară este disponibilă pentru aceeași infracțiune într-o situație internă asemănătoare. Cu toate acestea, CEPD avertizează în legătură cu efectul contraproductiv al unei astfel de dispoziții: în loc să ofere garanții suplimentare, aceasta pare a fi o încurajare pentru statele membre să își extindă posibilitățile naționale de a solicita divulgarea datelor privind abonații sau datele privind accesul în scopul de a se asigura că ordinele de divulgare ar putea fi emise în temeiul acestui regulament.

b) Termenele de transmitere a datelor ar trebui să fie justificate

CEPD ia notă de faptul că ordinele europene de divulgare primesc un răspuns în termen de cel mult 10 zile de la primirea certificatului, cu excepția cazului în care autoritatea emitentă precizează motivele pentru o divulgare mai rapidă, și cel târziu în termen de 6 ore în cazuri de urgență, astfel cum se prevede la articolul 9 alineatele (1) și (2).

Cu toate acestea, CEPD nu a identificat niciun criteriu pentru încadrarea obligației autorităților de a demonstra urgența divulgării datelor, chiar și *ex post*, pentru a permite un posibil control al utilizării acestei proceduri foarte rapide, în timp ce un termen de șase ore ar putea implica un control superficial înainte de divulgarea datelor, dacă nu absența unui control al furnizorului de servicii. Într-adevăr, evaluarea impactului subliniază necesitatea ca autoritățile competente să aibă acces la date în timp util. Cu toate acestea, toate exemplele oferite în evaluarea impactului vizează probele necesare în cazul comiterii unor infracțiuni grave (cazuri de terorism în care s-au înregistrat ostatici, situații de abuz sexual asupra copiilor în curs), însă justificarea bazată pe volatilitatea probelor nu pare să fie adecvată atunci când nu există o urgență specifică, alta decât această posibilă volatilitate a datelor. În plus, volatilitatea datelor nu oferă o justificare suplimentară în ceea ce privește proporționalitatea de a avea acces la date cu mai puține garanții în situațiile în care nu există alte situații de urgență în afară de volatilitatea datelor.

În plus, CEPD și-a exprimat îndoiala cu privire la necesitatea de a prevedea un termen de șase ore stipulând, în același timp, ca acest termen să nu se aplice până când autoritatea emitentă nu

[24] A se vedea cauza 203/15 – punctul 120.
[25] A se vedea cauzele conexate C 293/12 și C 594/12 – punctul 62.
[26] A se vedea, de exemplu, cauza C 203/14.
[27] A se vedea, de exemplu, cauza Moulin/Franța din 23 noiembrie 2010.

furnizează clarificări suplimentare „în termen de cinci zile” în cazul în care furnizorul de servicii nu își poate respecta obligația.

Prin urmare, CEPD solicită prezentarea unor elemente suplimentare în evaluarea impactului pentru a justifica necesitatea acestor termene în cazurile în care infracțiunea comisă sau urmărită în justiție nu este gravă și, cu excepția cazului în care sunt furnizate astfel de elemente detaliate, prezentarea unor criterii explicite care justifică urgența în cazul în care sunt emise EPOC-urile. De exemplu, s-ar putea prevedea același model ca în Directiva privind ordinul european de anchetă. Directiva privind ordinul european de anchetă prevede un termen mai scurt atunci când acest lucru este justificat de „termenele procedurale, gravitatea infracțiunii sau alte împrejurări urgente” [a se vedea articolul 12 alineatul (2)] sau un termen de 24 de ore pentru luarea unei decizii cu privire la măsurile provizorii [a se vedea articolul 32 alineatul (2)]. Într-adevăr, evaluarea impactului care însoțește proiectul de regulament nu prevede elemente detaliate care să justifice de ce aceste termene nu sunt eficiente, singurele elemente subliniate fiind că numărul de cereri trimise împovărează autoritățile judiciare destinatare care nu pot respecta termenele.

c) Ordinele europene de divulgare și de păstrare nu se utilizează pentru a solicita date privind o persoană vizată din alt stat membru fără a informa cel puțin autoritățile competente ale statului membru respectiv, în special pentru datele referitoare la conținut

CEPD reamintește faptul că, în cadrul instrumentelor existente, se asigură cooperarea judiciară și, prin urmare, garanții suplimentare, în special pentru a controla necesitatea și proporționalitatea cererilor, și subliniază că aceste garanții sunt cu atât mai justificate în cazurile în care datele solicitate sunt date referitoare la conținut care implică mai multe limitări ale drepturilor persoanelor vizate de a li se proteja datele cu caracter personal și viața privată. În această privință, CEPD reamintește că Directiva privind ordinul european de anchetă prevede, de asemenea, posibilitatea de a intercepta telecomunicațiile cu asistență tehnică din partea unui alt stat membru (a se vedea articolul 30), precum și obligația de a notifica orice interceptare a datelor către autoritatea competentă a unui alt stat membru în cazul în care nu este necesară asistența atunci când persoana vizată este sau va fi pe teritoriul statului membru respectiv (a se vedea articolul 31).

CEPD nu găsește nicio justificare pentru procedura prevăzută în proiectul de regulament privind probele electronice care permite divulgarea de date referitoare la conținut fără implicarea cel puțin a autorităților competente din statul membru în care se află persoana vizată.

d) Ordinele europene de păstrare nu se utilizează pentru a eluda obligațiile de păstrare a datelor ale furnizorilor de servicii

CEPD observă că obiectivul principal al ordinului european de păstrare a probelor electronice este de a preveni ștergerea datelor.

Deși CEPD recunoaște că acest lucru ar putea fi necesar și proporțional în unele cazuri, acesta regretă lipsa de garanții în ceea ce privește emiterea unor astfel de ordine. În particular, CEPD recomandă ca, atunci când ordinele de păstrare a probelor electronice se referă numai la date specifice, caz în care proiectul pare să permită cereri ample, și atunci când astfel de ordine sunt emise pentru date programate să fie șterse în conformitate cu principiul păstrării datelor, ordinul nu trebuie să reprezinte în niciun caz un temei pentru ca furnizorul de servicii să prelucreze datele după data inițială de ștergere. Cu alte cuvinte, datele ar trebui să fie „înghețate”.

În plus, ar trebui să fie consolidată legătura dintre ordinul de păstrare a probelor electronice și cererea ulterioară de divulgare a datelor, prin intermediul unui ordin european de divulgare a probelor electronice, al unei cereri privind ordinul european de anchetă sau al unei cereri de asistență judiciară reciprocă, pentru a se asigura faptul că ordinele europene de păstrare a probelor electronice sunt emise numai atunci când cealaltă cerere este certă (și nu este doar avută în vedere ca o posibilitate) și că ordinul de păstrare expiră la rândul său atunci când se refuză cealaltă cerere, fără a fi necesar să se aștepte o perioadă de 60 de zile[28] dacă cererea ulterioară este respinsă mai devreme.

e) Confidențialitatea și informațiile despre utilizatori

CEPD ia notă de faptul că un anumit articol[29] referitor la confidențialitatea ordinelor adresate a fost introdus în proiectul de regulament. Pentru a se evita orice confuzie și neînțelegere cu privire la dreptul la protecția datelor, CEPD reamintește că, deși RGPD prevede că limitările drepturilor persoanelor vizate pentru a garanta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor ar trebui să fie prevăzute prin lege și, prin urmare, să fie accesibile publicului[30] și că aceste măsuri legislative conțin dispoziții specifice referitoare la dreptul persoanelor vizate de a fi informate cu privire la restricții, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției[31], regulamentul nu prevede obligația de a informa individual persoanele vizate cu privire la fiecare cerere de acces formulată de autoritățile de aplicare a legii.

Cu toate acestea, între timp, CEPD reamintește că Directiva privind protecția datelor prevede acest drept de informare a persoanelor vizate chiar de către autoritățile competente, cu excepția cazului în care acest drept a fost limitat pentru orice persoană vizată, fără a limita acest drept numai la persoanele vizate care își au reședința pe teritoriul UE.

f) Procedura de executare a unui ordin în cazul în care furnizorul de servicii refuză să îl execute

CEPD constată că articolul 14 din proiectul de regulament prevede o procedură pentru a asigura executarea unui ordin atunci când destinatarul nu se conformează acestuia, bazându-se pe o cooperare judiciară între autoritatea emitentă și o autoritate competentă din statul de executare.

Cu toate acestea, se pare că această procedură nu permite autorității de executare să refuze executarea ordinului transmis din alte motive decât cele pur procedurale (aceleași cu cele ale destinatarului, în special din cauza lipsei de informații furnizate sau a imposibilității faptice de a furniza datele), deoarece datele în cauză sunt protejate de o imunitate sau de un privilegiu în temeiul dreptului său intern sau din cauză că divulgarea lor poate avea un impact asupra intereselor sale fundamentale, cum ar fi securitatea și apărarea națională[32].

Prin urmare, CEPD își reiterează preocupările cu privire la eliminarea oricărui control dublu de către autoritatea competentă destinatară a ordinului transmis, în comparație cu celelalte instrumente. Inclusiv motivul pentru a refuza executarea unui ordin deoarece acesta ar încălca Carta pare a fi superior pragului clasic referitor la o încălcare a drepturilor fundamentale ale persoanei în cauză. Prin urmare, urmând exemplele mandatului european de arestare, care prevăd motive obligatorii și

[28] A se vedea articolul 10 alineatul (1).
[29] A se vedea articolul 11.
[30] A se vedea articolul 23 alineatul (1) litera (d).
[31] A se vedea articolul 23 alineatul (2) litera (h).
[32] A se vedea articolul 14 alineatul (2).

motive opționale de refuz, sau cel puțin ale Directivei privind ordinul european de anchetă, care prevede, în general, că „crearea unui spațiu de libertate, securitate și justiție în cadrul Uniunii se bazează pe încredere reciprocă și pe o prezumție de respectare de către statele membre a dreptului Uniunii și, în particular, a drepturilor fundamentale" este relativă[33], proiectul de regulament ar trebui să prevadă cel puțin derogarea clasică minimă conform căreia, în cazul în care există motive întemeiate să se considere că executarea unui ordin ar avea ca rezultat încălcarea unui drept fundamental al persoanei în cauză și că statul de executare nu și-ar respecta obligațiile privind protecția drepturilor fundamentale recunoscute în Cartă, ar trebui să se refuze executarea ordinului.

g) Executarea ordinelor și obligațiile contradictorii în temeiul legislației unei țări terțe (articolele 15-16)

CEPD salută posibilitatea prevăzută în proiectul de regulament pentru destinatari de a refuza un ordin pe motiv că acesta ar intra în conflict cu drepturile fundamentale, având ca scop furnizarea de garanții în cazul unor obligații juridice contradictorii. De asemenea, acesta consideră esențial faptul că propunerea prevede consultarea autorităților din țări terțe, cel puțin în cazul în care apare un conflict, precum și obligația de a ridica ordinul în cazul în care autoritatea dintr-o țară terță ridică obiecții.

Prin urmare, procedura prevăzută de a refuza executarea unui ordin pe motiv de obligații contradictorii în temeiul legislației unei țări terțe ar trebui să fie îmbunătățită considerabil.

În primul rând, CEPD constată că proiectul de regulament încredințează unei societăți private, în calitate de destinatar al unui ordin de divulgare, să evalueze dacă respectivul ordin ar fi sau nu în conflict cu legislația aplicabilă a unei țări terțe care interzice divulgarea datelor solicitate. Societatea trebuie să prezinte o obiecție motivată care să includă toate detaliile relevante cu privire la legislația țării terțe, la aplicabilitatea sa în cazul vizat și la natura obligațiilor contradictorii.

Cel mai important, CEPD este preocupat de faptul că, atunci când se ridică o astfel de obiecție, numai instanța competentă din statul membru al autorității emitente evaluează dacă există sau nu un conflict, întrucât abia atunci când instanța constată prezența unui conflict aceasta contactează autoritățile din țara terță. Prin urmare, instanței competente din UE i se acordă competența de a interpreta în mod concludent legislația unei țări terțe în acest context, fără a fi specializată în materie. CEPD consideră că obligația de a consulta autoritățile competente din țara terță este, prin urmare, prea limitată în propunerea actuală. În domeniul protecției datelor, CEPD atrage atenția legiuitorului asupra faptului că, în cazul în care o instanță competentă dintr-o țară terță ar interpreta RGPD pentru a evalua dacă acesta este în contradicție cu propriile cerințe, autoritățile pentru protecția datelor din UE și instanțele competente ar rămâne competente să evalueze legalitatea transferului pe baza unei hotărâri a unei instanțe sau a unui tribunal sau pe baza unei decizii a unei autorități administrative dintr-o țară terță care solicită un transfer sau o divulgare de date cu caracter personal în domeniul de aplicare a RGPD[34].

În plus, CEPD subliniază că evaluarea legislației țării terțe de către instanța competentă a statului membru al UE care a transmis solicitarea trebuie să se bazeze pe elemente obiective și este preocupată de criteriile care trebuie luate în considerare de către instanța competentă atunci când evaluează legislația țării terțe în conformitate cu articolul 15 alineatul (4) și articolul 16 alineatul (5) litera (a) din proiectul de regulament. Într-adevăr, instanța ar trebui să evalueze faptul că, „în loc să

[33] A se vedea considerentul 19 din Directiva privind ordinul european de anchetă.
[34] A se vedea articolul 48 din RGPD.

vizeze protejarea drepturilor fundamentale sau a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională", legislația țării terțe „încearcă în mod evident să protejeze alte interese sau are drept obiectiv protejarea unor activități ilegale împotriva cererilor de aplicare a legii în contextul anchetelor penale" sau „interesul protejat de legislația relevantă a țării terțe, inclusiv interesul țării terțe în ceea ce privește împiedicarea divulgării datelor". De exemplu, deși în principiu această evaluare ar trebui să prevadă o evaluare bazată pe dovezi luând în considerare toate informațiile disponibile având în vedere impactul potențial al unei astfel de decizii, cel puțin formularea („urmărește să") pare neclară și ar trebui să fie adaptată („are scopul/obiectivul de").

CEPD regretă faptul că singurul caz în care autoritățile dintr-o țară terță ar fi consultate și ar putea formula obiecții cu privire la executarea unui ordin de divulgare ar fi cel în care instanța competentă a UE ar considera că există un conflict relevant, ar transmite toate elementele către autoritățile centrale din țara terță în cauză, iar autoritatea centrală a țării terțe în cauză s-ar opune în termenele scurte de maximum 50 de zile (15 zile, eventual prelungit cu 30 de zile și, după o ultimă notificare posibilă, cu încă 5 zile). În toate celelalte cazuri, instanța competentă ar fi în măsură să mențină ordinul de divulgare și să aplice o sancțiune pecuniară furnizorului de servicii care refuză să execute ordinul. În consecință, CEPD este preocupat de faptul că instanțele competente ale UE nu vor avea o obligație mai largă de a consulta autoritățile competente ale țărilor terțe în cauză în scopul de a se asigura că procedura va garanta în mod mai sistematic că argumentele ambelor părți vor fi luate în considerare și de a demonstra și mai mult respect pentru legislația țărilor terțe.

Așa cum s-a subliniat deja în declarația GL29 și mai sus, CEPD reamintește că ar trebui să se acorde o atenție deosebită adoptării de către țările terțe a unor instrumente similare care ar putea afecta drepturile persoanelor vizate și dreptul acestora la viață privată în cadrul UE, în special riscul unor instrumente similare care ar intra în conflict direct cu legislația UE privind protecția datelor.

În plus, CEPD subliniază că instanța competentă din statul membru al autorității emitente ar putea să nu fie nici măcar instanța competentă să execute ordinul prevăzut la articolul 14 din proiectul de regulament, ceea ce ar conduce la creșterea riscului de apariție a unor proceduri contradictorii și lipsa contracontroalelor în caz de legi contradictorii. Aceasta rezultă din faptul că, în unele cazuri, ar putea fi implicate trei state: autoritatea care emite ordinul, țara terță a furnizorului de servicii și statul membru în care se află reprezentantul legal al furnizorului de servicii în UE și în care ordinul ar trebui executat. Prin urmare, în conformitate cu procedura prevăzută în prezent, instanța autorității care a transmis solicitarea din statul membru A ar putea face propria interpretare a legislației din țara terță B a furnizorului de servicii, fără a solicita punctele de vedere ale autorităților din țara terță respectivă (în timp ce acestea s-ar fi opus ordinului) și poate solicita unei instanțe dintr-un alt stat membru C să pună în aplicare decizia sa, fără nicio posibilitate de a formula obiecții.

Pe lângă aceasta, CEPD salută, de asemenea, introducerea unor căi de atac specifice împotriva ordinelor de divulgare a datelor, în plus față de măsurile corective prevăzute în RGPD și în Directiva privind aplicarea legii. GL29 a solicitat deja astfel de garanții în declarația sa anterioară. Cu toate acestea, CEPD regretă faptul că astfel de căi de atac nu sunt prevăzute, de asemenea, împotriva ordinelor de păstrare a datelor, întrucât aceste ordine pot conduce, de asemenea, la limitări ale drepturilor fundamentale ale persoanelor ale căror date sunt păstrate. Într-adevăr, ordinele de păstrare a datelor pot avea ca efect păstrarea unor date pentru o perioadă mai lungă de timp decât cea prevăzută în normele privind protecția datelor. Prin urmare, ordinul privind păstrarea datelor conduce, în sine, la o limitare a drepturilor fundamentale ale persoanei vizate, a cărei justificare trebuie să facă obiectul unei revizuiri și al unor căi de atac specifice, în special în cazurile în care ordinul de păstrare a datelor a fost emis împreună cu un ordin de divulgare pentru a obține datele.

Așa cum recomandă GL29 în declarația sa, ar trebui să se prevadă căi de atac cel puțin echivalente cu cele disponibile la nivel național.

h) Securitatea transferurilor de date atunci când se răspunde unui ordin

CEPD constată că proiectul de regulament prevede doar ca ordinele să fie adresate destinatarilor din cadrul Uniunii Europene și, prin urmare, nu prevede niciun canal specific pentru transferul datelor între destinatari și furnizorii de servicii situați în afara Uniunii Europene.

Deși CEPD salută absența unor derogări suplimentare de la cadrul general al UE pentru protecția datelor, acesta reamintește că orice ordin trimis către un destinatar, care ar implica ulterior un transfer în afara UE, ar trebui să respecte cadrul juridic prevăzut de RGPD. Într-adevăr, eludarea cadrului juridic al cooperării judiciare, care prevede respectarea garanțiilor pentru protecția datelor, nu ar trebui să rezulte, de asemenea, în eludarea cerințelor privind transferul de date de către destinatarii ordinelor de divulgare sau de păstrare a datelor pentru a se conforma acestor ordine.

În plus, în timp ce CEPD apreciază absența unei dispoziții care să impună obligația de a decripta datele criptate[35], acesta este preocupat de faptul că proiectele de propuneri nu prevăd nicio cerință specifică pentru destinatari de a evalua autenticitatea datelor divulgate și subliniază că această evaluare reprezintă, de asemenea, o valoare adăugată a instrumentelor tradiționale care se bazează pe cooperarea judiciară și avertizează în legătură cu riscurile crescute prezentate pentru persoanele vizate în cauză în absența unei astfel de evaluări.

Concluzii

Pe baza acestei evaluări, CEPD dorește să adreseze colegiuitorilor următoarele recomandări:

1) Temeiul juridic al regulamentului nu ar trebui să fie articolul 82 alineatul (1) din TFUE.

2) Necesitatea unui nou instrument în comparație cu Directiva privind ordinul european de anchetă sau Tratatul de asistență judiciară reciprocă existent ar trebui să fie demonstrată într-un mod mai adecvat, inclusiv printr-o analiză detaliată a mijloacelor mai puțin intruzive în ceea ce privește drepturile fundamentale, cum ar fi modificările aduse acestor instrumente existente sau restrângerea domeniului de aplicare a instrumentului propus la ordinele de păstrare a datelor, în combinație cu alte proceduri existente de solicitare a accesului la date.

3) Regulamentul ar trebui să prevadă un termen mai lung pentru a permite furnizorului de servicii care execută ordinul să asigure garanții în ceea ce privește protecția drepturilor fundamentale.

4) Principiul dublei incriminări ar trebui menținut, în special în cazul în care criteriile de localizare a datelor sunt abandonate pentru a menține obligația de a lua în considerare garanțiile furnizate în ambele state în cauză (statul autorității care transmite solicitarea și statul în care se află furnizorul de servicii).

5) Domeniul de aplicare a regulamentului ar trebui să fie limitat la operatorii în sensul RGPD sau ar trebui să includă o dispoziție conform căreia, în cazul în care furnizorul de servicii vizat de solicitare nu este operatorul datelor, ci persoana împuternicită de operator, aceasta din urmă este obligată să informeze operatorul.

[35] A se vedea considerentul 19 și pagina 240 din evaluarea impactului.

6) Regulamentul ar trebui să includă garanții privind transferurile de date în cazul în care furnizorul de servicii ar fi stabilit într-o țară terță fără o decizie privind caracterul adecvat în acest domeniu sau să facă trimitere la Directiva (UE) 2016/680, întrucât aceste garanții vor fi aplicabile.

7) Întrucât desemnarea obligatorie a unui reprezentant legal diferă de RGPD, regulamentul ar trebui să precizeze că reprezentantul legal desemnat în temeiul Regulamentului privind probele electronice ar trebui să fie distinct de cel desemnat în temeiul articolului 3 alineatul (2) din RGPD.

8) Regulamentul ar trebui să conțină o definiție mai largă a datelor transmise în cadrul comunicațiilor electronice pentru a se asigura că garanțiile adecvate și condițiile de acces care urmează să fie stabilite acoperă atât datele care nu se referă la conținut, cât și datele referitoare la conținut.

9) Regulamentul ar trebui să ridice pragurile pentru emiterea de ordine, iar ordinele ar trebui să fie emise sau autorizate de instanțe, cu excepția datelor privind abonații, cu condiția ca definiția acestei categorii de date să fie restrânsă în mod drastic la informațiile de bază permițând doar identificarea unei persoane fără a implica accesul la oricare date transmise în cadrul comunicațiilor.

10) Regulamentul ar trebui să restricționeze accesul la datele privind abonații și datele privind accesul la o listă de infracțiuni stabilită în mod strict sau cel puțin la „infracțiuni grave”.

11) Termenul de transmitere a datelor, în special în cazul unei urgențe, ar trebui să fie mai bine justificat în regulament, iar posibilitatea de a utiliza o procedură rapidă de 6 ore ar trebui să includă obligația ca autoritățile care transmit solicitarea să demonstreze urgența care determină recurgerea la această procedură, chiar și *a posteriori*, în scopul de a permite controlul utilizării acestor competențe excepționale.

12) Ar trebui să se renunțe la procedura care permite divulgarea de date privind conținutul fără implicarea autorităților competente ale statului membru în care este stabilită persoana vizată.

13) Ar trebui îmbunătățite garanțiile privind emiterea ordinelor europene de păstrare a probelor electronice în regulament.

14) Regulamentul ar trebui să includă cel puțin derogarea clasică minimă conform căreia, în cazul în care există motive întemeiate să se considere că executarea unui ordin ar conduce la încălcarea unui drept fundamental al persoanei în cauză, determinând statul de executare să nu țină seama de obligațiile sale privind protecția drepturilor fundamentale recunoscute în Cartă, executarea ordinului ar trebui să fie refuzată.

15) Regulamentul ar trebui să prevadă o obligație mai amplă de a consulta autoritățile competente dintr-o țară terță în care este stabilit furnizorul de servicii căruia i s-a solicitat să furnizeze date în caz de conflict de legi pentru a evita interpretări subiective din partea unei singure instanțe.

16) Valabilitatea și durata ordinelor de păstrare ar trebui să fie mai corelate cu ordinele de divulgare pe care le însoțesc.

17) Securitatea transferurilor de date ar trebui să fie mai bine garantată.

18) Ar trebui să se prevadă verificarea autenticității datelor, în special în cazul în care ar putea fi furnizate date criptate.

Pentru Comitetul European pentru Protecția Datelor,

Președinte

(Andrea Jelinek)