

Bruxelles, 18 aprilie 2018
(OR. en)

8110/18

**Dosar interinstituțional:
2018/0108 (COD)**

JAI 323
COPEN 104
CYBER 66
DROIPEN 53
JAIEX 27
ENFOPOL 171
TELECOM 94
DAPIX 106
EJUSTICE 27
MI 269
IA 101
CODEC 577

PROPUNERE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Data primirii:	18 aprilie 2018
Destinatar:	DI Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2018) 225 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală

În anexă, se pune la dispoziția delegațiilor documentul COM(2018) 225 final.

Anexă: COM(2018) 225 final



COMISIA
EUROPEANĂ

Strasbourg, 17.4.2018
COM(2018) 225 final

2018/0108 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
privind ordinele europene de divulgare și de păstrare a probelor electronice în materie
penală

{SWD(2018) 118 final} - {SWD(2018) 119 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Utilizarea platformelor de comunicare socială, a webmail-ului, a serviciilor și a aplicațiilor de mesagerie pentru a comunica, a lucra, a socializa și a obține informații a devenit în prezent o practică curentă în multe părți ale lumii. Aceste servicii conectează între ei sute de milioane de utilizatori. Ele generează beneficii semnificative pentru bunăstarea economică și socială a utilizatorilor din întreaga Uniune și de dincolo de frontierele acesteia. Cu toate acestea, ele pot fi utilizate, de asemenea, în mod necorespunzător ca instrumente pentru a săvârși infracțiuni sau a facilita săvârșirea de infracțiuni, inclusiv infracțiuni grave, cum ar fi atacurile teroriste. Când se întâmplă acest lucru, aceste servicii și aplicații sunt adesea singurul loc unde anchetatorii pot găsi indicii pentru a stabili cine a comis o infracțiune și pentru a obține dovezi care pot fi folosite în instanță.

Având în vedere caracterul „fără frontiere” al internetului, aceste servicii pot fi furnizate de oriunde în lume și nu necesită neapărat o infrastructură fizică, prezența unei întreprinderi sau a unor angajați în statele membre în care sunt oferite serviciile sau pe piața internă în ansamblu. De asemenea, acestea nu necesită o amplasare specifică pentru stocarea datelor, care este adesea aleasă de prestatorul de servicii pe baza unor considerații legitime cum ar fi securitatea datelor, economiile de scară și rapiditatea accesului. Prin urmare, într-un număr tot mai mare de cazuri penale care implică toate tipurile de infracțiuni¹, autoritățile statelor membre solicită acces la date care ar putea servi drept probe și care sunt stocate în afara țării lor și/sau de către prestatori de servicii din alte state membre sau din țări terțe.

Pentru situațiile în care fie probele, fie prestatorul de servicii, se găsesc în altă parte, au fost dezvoltate mecanisme de cooperare între țări în urmă cu mai multe decenii². În ciuda unor reforme periodice, aceste mecanisme de cooperare se află sub o presiune crescândă rezultată din necesitatea tot mai mare de a dispune de un acces transfrontalier rapid la probe electronice. Pentru a răspunde acestei necesități, mai multe state membre și țări terțe au recurs la extinderea instrumentelor lor naționale. Fragmentarea rezultată în urma acestui demers generează

insecuritate juridică și obligații contradictorii și ridică semne de întrebare cu privire la protecția drepturilor fundamentale și a garanțiilor procedurale pentru persoanele vizate de astfel de solicitări.

În 2016, Consiliul a solicitat măsuri concrete bazate pe o abordări comună a UE pentru a spori eficiența asistenței judiciare reciproce, pentru a îmbunătăți cooperarea între autoritățile statelor membre și prestatorii de servicii cu sediul în țări din afara UE și pentru a propune soluții la problema reprezentată de stabilirea și asigurarea respectării jurisdicției³ în spațiul cibernetic⁴. Parlamentul European a evidențiat, de asemenea, provocările pe care actualul cadru juridic fragmentat le poate crea pentru prestatorii de servicii care încearcă să respecte

¹ A se vedea secțiunile 2.1.1 și 2.3 din evaluarea impactului.

² În Uniune, mecanisme de recunoaștere reciprocă, bazate în prezent pe directiva privind ordinul european de anchetă; cu țările terțe, mecanisme de asistență judiciară reciprocă (AJR).

³ În prezentul document, termenul „asigurarea respectării jurisdicției” se referă la competența autorităților relevante de a întreprinde o măsură de investigare.

⁴ [Concluziile Consiliului Uniunii Europene privind îmbunătățirea justiției penale în spațiul cibernetic, ST9579/16.](#)

cererile de aplicare a legii și a solicitat instituirea unui cadru juridic european, care să includă garanții pentru drepturile și libertățile tuturor părților vizate⁵.

Prezenta propunere vizează problema specifică reprezentată de caracterul volatil al probelor electronice și de dimensiunea internațională a acestora. Aceasta are drept obiectiv adaptarea mecanismelor de cooperare la era digitală, oferind instrumentele judiciare și de aplicare a legii necesare pentru a ține seama de modul în care infractorii comunică în prezent și combaterea formelor moderne de criminalitate. Astfel de instrumente sunt subordonate controlului exercitat de mecanisme puternice de protecție a drepturilor fundamentale. Prezenta propunere vizează îmbunătățirea securității juridice pentru autorități, prestatorii de servicii și persoanele afectate și menținerea unui standard ridicat pentru cererile de aplicare a legii, asigurând astfel protecția drepturilor fundamentale, transparența și asumarea răspunderii. De asemenea, aceasta accelerează procesul de obținere și de colectare a probelor electronice care sunt stocate și/sau deținute de prestatorii de servicii stabiliți în altă jurisdicție. Acest instrument va coexista cu actualele instrumente de cooperare judiciară care sunt încă relevante și poate fi utilizat în mod corespunzător de către autoritățile competente. În paralel, Comisia depune eforturi pentru consolidarea mecanismelor de cooperare judiciară existente prin măsuri precum crearea unei platforme sigure pentru schimbul rapid de cereri între autoritățile judiciare în cadrul UE și investiția în valoare de 1 milion EUR pentru a oferi formare practicienilor din toate statele membre ale UE în domeniul asistenței judiciare reciproce și al cooperării, punând accentul pe Statele Unite în calitate de țară terță care primește cel mai mare număr de cereri din partea UE⁶.

Pentru notificarea și executarea ordinelor în temeiul acestui instrument, autoritățile ar trebui să se bazeze pe reprezentantul legal desemnat de către prestatorii de servicii. Comisia prezintă astăzi o propunere menită să asigure faptul că acești reprezentanți legali sunt desemnați în mod efectiv. Ea oferă o soluție comună la nivelul UE pentru transmiterea ordinelor juridice către prestatorii de servicii prin intermediul unui reprezentant legal.

- **Coerența cu dispozițiile legislative ale UE în domeniul de politică și cu Convenția de la Budapesta a Consiliului Europei**

Cadrul juridic actual al UE constă în instrumente de cooperare în materie penală, cum ar fi Directiva 2014/41/UE privind ordinul european de anchetă în materie penală⁷, Convenția privind asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene⁸, Decizia 2002/187/JAI a Consiliului de instituire a Eurojust⁹,

⁵ [P8_TA\(2017\)0366](#).

⁶ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

⁷ [Directiva 2014/41/UE](#) a Parlamentului European și a Consiliului din 3 aprilie 2014 privind ordinul european de anchetă în materie penală (JO L 130, 1.5.2014, p. 1).

⁸ [Actul Consiliului din 29 mai 2000](#) de elaborare, în temeiul articolului 34 din Tratatul privind Uniunea Europeană, a Convenției privind asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene.

⁹ [Decizia 2002/187/JAI a Consiliului](#) din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate. În 2013, Comisia a adoptat o [propunere de regulament](#) de reformare a Eurojust [Propunere de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust), COM/2013/0535 final].

Regulamentul (UE) 2016/794 privind Europol¹⁰, Decizia-cadru 2002/465/JAI a Consiliului privind echipele comune de anchetă¹¹, precum și acorduri bilaterale între Uniune și țările terțe, cum ar fi Acordul privind asistența judiciară reciprocă („AJR”) între UE și SUA¹² și Acordul privind AJR între UE și Japonia¹³.

Prin introducerea ordinelor europene de divulgare a probelor electronice și de păstrare a probelor electronice, propunerea facilitează obținerea și colectarea de probe electronice pentru procedurile penale stocate sau deținute de prestatorii de servicii dintr-o altă jurisdicție. Directiva privind ordinul european de anchetă, care a înlocuit în mare măsură Convenția privind asistența judiciară reciprocă în materie penală, reglementează toate măsurile de investigare¹⁴. Aceasta include accesul la probe electronice, însă Directiva privind ordinul european de anchetă nu conține nicio dispoziție specifică privind acest tip de probe¹⁵. Noul instrument nu va înlocui ordinul european de anchetă pentru obținerea de probe electronice, însă le oferă autorităților un instrument suplimentar. Pot exista situații, de exemplu atunci când mai multe măsuri de investigare trebuie să fie întreprinse în statul membru de executare, în care ordinul european de anchetă poate fi opțiunea preferată pentru autoritățile publice. Crearea unui nou instrument pentru probele electronice este o alternativă mai bună decât modificarea Directivei privind ordinul european de anchetă, având în vedere provocările specifice inerente obținerii de probe electronice care nu afectează celelalte măsuri de investigare reglementate de Directiva privind ordinul european de anchetă.

Pentru a facilita colectarea transfrontalieră de probe electronice, noul instrument se va baza pe principiile recunoașterii reciproce. Autoritățile din țara în care se află destinatarul ordinului nu vor trebui să participe în mod direct la notificarea și executarea ordinului, cu excepția cazului în care ordinul nu este respectat, caz în care va fi necesară executarea, iar autoritatea competentă din țara în care este se află reprezentantul va interveni. Prin urmare, instrumentul necesită o serie de garanții și dispoziții solide, cum ar fi validarea de către o autoritate judiciară în fiecare caz. De exemplu, ordinele europene de divulgare a probelor electronice pentru divulgarea de date privind operațiunile sau de date referitoare la conținut (spre deosebire de datele privind abonații și de cele privind accesul) pot fi emise doar pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani sau pentru anumite infracțiuni pur informatice, facilitate de calculator sau legate de terorism, astfel cum sunt menționate în propunere.

¹⁰ [Regulamentul \(UE\) 2016/794](#) al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului.

¹¹ [Decizia-cadru 2002/465/JAI a Consiliului](#) din 13 iunie 2002 privind echipele comune de anchetă.

¹² [Decizia 2009/820/PESC a Consiliului](#) din 23 octombrie 2009 privind încheierea, în numele Uniunii Europene, a Acordului privind extrădarea între Uniunea Europeană și Statele Unite ale Americii și a Acordului privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii.

¹³ [Decizia 2010/616/UE a Consiliului](#) din 7 octombrie 2010 privind încheierea Acordului între Uniunea Europeană și Japonia privind asistența judiciară reciprocă în materie penală

¹⁴ Cu excepția echipelor comune de anchetă (a se vedea articolul 3 din Directiva privind ordinul european de anchetă); nu toate statele membre participă la Directiva privind ordinul european de anchetă (Irlanda, Danemarca).

¹⁵ Cu excepția unei trimiteri la identificarea unei persoane care deține o adresă IP la articolul 10 alineatul (2) litera (e), pentru care nu poate fi invocată dubla incriminare drept motiv pentru refuzul recunoașterii și executării cererii.

Datele cu caracter personal reglementate de prezenta propunere sunt protejate și pot fi prelucrate doar în conformitate cu Regulamentul general privind protecția datelor (RGPD)¹⁶ și cu Directiva privind protecția datelor destinată autorităților polițienești și judiciare (Directiva privind protecția datelor în materie de asigurare a respectării legii)¹⁷. RGPD va intra în vigoare la 25 mai 2018, în timp ce Directiva privind protecția datelor în materie de asigurare a respectării legii trebuie să fie transpusă de statele membre până la 6 mai 2018.

Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică (CETS nr. 185), ratificată de majoritatea statelor membre ale UE, stabilește mecanisme internaționale pentru cooperarea împotriva criminalității informatice¹⁸. Convenția se referă la infracțiuni săvârșite prin intermediul internetului și al altor rețele informatice. De asemenea, aceasta le solicită părților să stabilească competențe și proceduri pentru obținerea de probe electronice și să își furnizeze asistență juridică reciprocă, fără a se limita la actele de criminalitate informatică. În special, convenția le solicită părților să instituie ordine de divulgare pentru a obține date informatice din partea prestatorilor de servicii de pe teritoriul lor și date privind abonații din partea prestatorilor de servicii care oferă servicii pe teritoriul lor. În plus, convenția prevede ordine de divulgare în cazurile în care există motive pentru a considera că datele informatice sunt deosebit de vulnerabile la pierdere sau modificare. Notificarea și caracterul executoriu ale ordinelor naționale de divulgare împotriva prestatorilor stabiliți în afara teritoriului unei părți la convenție ridică alte semne de întrebare. În această privință, sunt în prezent în curs de examinare măsuri suplimentare pentru a îmbunătăți accesul transfrontalier la probele electronice¹⁹.

• **Rezumatul regulamentului propus**

Regulamentul propus introduce ordine europene de divulgare a probelor electronice și de păstrare a probelor electronice cu caracter obligatoriu. Ambele ordine trebuie să fie emise sau validate de o autoritate judiciară a unui stat membru. Un ordin poate fi emis pentru a solicita păstrarea sau divulgarea datelor care sunt stocate de un prestator de servicii dintr-o altă jurisdicție și care sunt necesare ca probe în cadrul anchetelor sau procedurilor penale. Astfel de ordine nu pot fi emise decât dacă o măsură similară este disponibilă pentru aceeași infracțiune într-o situație internă comparabilă în statul emitent. Ambele ordine pot fi notificate prestatorilor de servicii de comunicații electronice, rețelelor sociale, piețelor online, altor prestatori de servicii de găzduire și furnizorilor de infrastructură de internet, cum ar fi adrese IP și registre de nume de domenii, sau reprezentanților legali ai acestora, după caz. Ordinul

¹⁶ [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.

¹⁷ [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.

¹⁸ În Strategia de securitate cibernetică a Uniunii Europene din 2013, Convenția de la Budapesta a fost recunoscută ca fiind principalul cadru multilateral pentru lupta împotriva criminalității informatice - Comunicarea comună a Comisiei și a Înalțului Reprezentant al Uniunii pentru afaceri externe și politica de securitate privind Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, JOIN(2013) 1 final.

¹⁹ La cea de a 17-a sa sesiune plenară (iunie 2017), Comitetul pentru Convenția privind criminalitatea informatică (T-CY) a adoptat mandatul pentru pregătirea unui al doilea protocol adițional la convenție (denumit în continuare „al doilea protocol adițional”), care urmează să fie întocmit și finalizat de T-CY până în decembrie 2019. Obiectivul este ca locul de stocare a datelor să nu mai fie considerat drept un factor decisiv.

european de păstrare, ca și ordinul european de divulgare, este adresat reprezentantului legal din afara jurisdicției statului membru emitent pentru a păstra datele unei cereri ulterioare de divulgare a acestora, de exemplu prin intermediul canalelor de asistență judiciară reciprocă în cazul țărilor terțe sau prin intermediul unui ordin european de anchetă între statele membre participante. Spre deosebire de măsurile de supraveghere sau de obligațiile de păstrare a datelor prevăzute de lege, care nu sunt prevăzute în prezentul regulament, ordinul european de păstrare a probelor electronice este un ordin emis sau validat de o autoritate judiciară în cadrul unei proceduri penale concrete, în urma unei evaluări individuale a proporționalității și a necesității în fiecare caz în parte. La fel ca ordinul european de divulgare a probelor electronice, acesta se referă la autori specifici, cunoscuți sau necunoscuți, ai unei infracțiuni care a avut deja loc. Ordinul european de păstrare a probelor electronice permite doar păstrarea datelor care sunt deja stocate în momentul primirii ordinului, nu și accesul la date la o dată ulterioară după primirea ordinului european de păstrare a probelor electronice.

Ambele ordine pot fi utilizate numai în cadrul procedurilor penale, începând cu faza inițială de urmărire penală și până la încheierea procedurilor printr-o hotărâre judecătorească sau o altă decizie. Ordinele de divulgare de date privind abonații și a celor privind accesul pot fi emise pentru orice infracțiune, în timp ce ordinul de divulgare de date privind operațiile sau de date referitoare la conținut pot fi emise doar pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani sau pentru anumite infracțiuni menționate în propunere și în cazul în care există o legătură specifică cu instrumente și infracțiuni electronice reglementate de Directiva 2017/541/UE privind terorismul.

Având în vedere diferitele niveluri de ingerință ale măsurilor impuse în legătură cu datele solicitate, propunerea stabilește o serie de condiții și garanții. Printre acestea se numără obligația de a obține validarea prealabilă a ordinelor de către o autoritate judiciară. Propunerea se aplică doar datelor stocate. Interceptarea telecomunicațiilor în timp real nu este reglementată de prezenta propunere. Măsura este limitată la ceea ce este necesar și proporțional în scopul procedurilor penale relevante. De asemenea, aceasta permite prestatorilor de servicii să solicite clarificări de la autoritățile emitente, dacă este necesar. În cazul în care acestor probleme nu pot fi rezolvate și autoritatea emitentă decide să continue executarea, prestatorii de servicii pot invoca aceleași motive pentru a se opune executării ordinului de către propriile autorități. În plus, se instituie o procedură specifică pentru situațiile în care obligația de a furniza date intră în conflict cu o obligație contradictorie care decurge din legislația unei țări terțe.

Legislația UE protejează drepturile persoanelor suspectate și ale persoanelor acuzate în cadrul procedurilor penale și există deja norme de protecție a datelor cu caracter personal. Cu toate acestea, pentru persoanele ale căror date sunt solicitate, aceste garanții suplimentare prevăzute în propunere prevăd drepturi procedurale pentru aceste persoane în cadrul sau în afara procedurilor penale. Acestea includ posibilitatea de a contesta legalitatea, necesitatea sau proporționalitatea ordinului fără a restricționa motivele care stau la baza contestării în conformitate cu legislația națională. Drepturile în conformitate cu legea statului de executare sunt respectate pe deplin prin asigurarea faptului că imunitățile și privilegiile care protejează datele solicitate în statul membru al prestatorului de servicii sunt luate în considerare în statul emitent. Acest lucru este valabil în special în cazul în care aceste imunități și privilegii oferă o mai bună protecție decât legea statului emitent.

Ordinele în temeiul regulamentului propus sunt executorii în același mod ca și ordinele interne comparabile în jurisdicția în care prestatorul de servicii primește ordinul.

Regulamentul prevede că statele membre ar trebui să instituie sancțiuni eficiente și proporționale.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temei juridic

Temeiul juridic pentru sprijinirea acțiunilor în acest domeniu îl constituie articolul 82 alineatul (1) din Tratatul privind funcționarea Uniunii Europene. Articolul 82 alineatul (1) prevede că se pot adopta măsuri în conformitate cu procedura legislativă ordinară pentru a institui norme și proceduri care să asigure recunoașterea, în întreaga Uniune, a tuturor categoriilor de hotărâri judecătorești și de decizii judiciare. De asemenea, se pot adopta măsuri pentru a facilita cooperarea dintre autoritățile judiciare sau echivalente ale statelor membre în procedurile penale și de executare a hotărârilor.

Acest temei juridic se aplică mecanismelor reglementate de prezentul regulament. Articolul 82 alineatul (1) asigură recunoașterea reciprocă a hotărârilor judiciare prin care o autoritate judiciară din statul emitent se adresează unei persoane juridice dintr-un alt stat membru și chiar îi impune acesteia obligații, fără intervenția prealabilă a unei autorități judiciare din celălalt stat membru. Ordinul european de divulgare sau de păstrare a probelor electronice poate duce la intervenția unei autorități judiciare a statului de executare atunci când acest lucru este necesar pentru executarea deciziei.

• Alegerea instrumentului

Articolul 82 alineatul (1) din TFUE oferă legiuitorului Uniunii posibilitatea de a adopta regulamente și directive.

Întrucât propunerea se referă la proceduri transfrontaliere care necesită norme uniforme, nu este necesar să se prevadă o marjă care să permită statelor membre să transpună aceste norme. Un regulament este direct aplicabil, oferă claritate și o mai mare securitate juridică și evită interpretări divergente în statele membre și alte probleme de transpunere întâmpinate de deciziile-cadru privind recunoașterea reciprocă a hotărârilor judecătorești și a deciziilor judiciare. În plus, un regulament permite ca aceeași obligație să fie impusă în mod uniform în Uniune. Din aceste motive, forma considerată ca fiind cea mai adecvată pentru acest instrument de recunoaștere reciprocă este aceea a unui regulament.

• Subsidiaritate

Având în vedere dimensiunea transfrontalieră a problemelor abordate, măsurile incluse în propunere trebuie să fie adoptate la nivelul Uniunii pentru a realiza obiectivele vizate. Infracțiunile pentru care există probe electronice implică deseori situații în care infrastructura de stocare a probelor electronice și prestatorul de servicii care gestionează infrastructura se supun unui cadru juridic național, în cadrul Uniunii sau în afara acesteia, diferit de cadrul juridic național al victimei sau al autorului infracțiunii. Prin urmare, accesul efectiv la probe electronice la nivel transfrontalier poate necesita mult timp și poate fi dificil pentru țara competentă în lipsa unor norme comune minime. În special, ar fi dificil pentru statele membre care acționează pe cont propriu să abordeze următoarele aspecte:

- fragmentarea cadrelor legislative din statele membre, care a fost identificată ca fiind o provocare majoră de către prestatorii de servicii care încearcă să se conformeze cererilor bazate pe diferite legislații naționale;

- o cooperare judiciară mai rapidă pe baza legislației existente a Uniunii, în special prin intermediul ordinului european de anchetă.

Având în vedere diversitatea de abordări juridice, numărul domeniilor de politică vizate (securitate, drepturi fundamentale, inclusiv drepturile procedurale și protecția datelor cu caracter personal, aspecte economice) și gama largă de părți interesate, legislația la nivelul Uniunii este mijlocul cel mai adecvat pentru abordarea problemelor identificate.

• **Proportionalitate**

Propunerea stabilește normele în temeiul cărora o autoritate competentă a unui stat membru poate cere unui prestator de servicii care oferă servicii în Uniune dar care este stabilit într-un alt stat membru să divulge sau să păstreze probe electronice. Caracteristicile-cheie ale propunerii, cum ar fi domeniul de aplicare material al ordinului european de divulgare a probelor electronice, condițiile pentru garantarea curtoaziei, mecanismul de sancționare și sistemul de garanții și căi de atac, limitează propunerea la ceea ce este necesar pentru atingerea obiectivelor sale principale. În special, propunerea se limitează la cererile privind datele stocate (nu sunt vizate datele provenite din interceptarea telecomunicațiilor în timp real) și la ordinele emise în cadrul procedurilor penale pentru o anumită infracțiune care face obiectul unei anchete în curs. Prin urmare, aceasta nu acoperă prevenirea criminalității sau alte tipuri de proceduri sau încălcări (cum ar fi procedurile administrative pentru încălcări ale normelor de drept) și nu impune prestatorilor să colecteze sau să stocheze sistematic mai multe date decât cele necesare din motive profesionale sau pentru respectarea altor cerințe legale. În plus, în timp ce ordinele de divulgare de date privind abonații și de date privind accesul pot fi emise pentru orice infracțiune, ordinul de divulgare de date privind operațiile sau de date referitoare la conținut poate fi emis doar pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani sau pentru anumite infracțiuni pur informatice și facilitate de calculator definite în propunere, precum și pentru infracțiuni legate de terorism. În sfârșit, propunerea clarifică normele procedurale și garanțiile aplicabile accesului transfrontalier la probe electronice, însă nu merge atât de departe încât să armonizeze măsurile interne. Aceasta se limitează la ceea ce este necesar și proporțional pentru a satisface nevoile autorităților de aplicare a legii și ale autorităților judiciare în era digitală.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

• **Consultările cu părțile interesate**

Timp de un an și jumătate, Comisia a consultat toate părțile interesate relevante pentru a se identifica problemele și căile de urmat. Ea a realizat acest lucru prin intermediul sondajelor, de la o consultare publică deschisă până la sondaje specifice cu autoritățile publice relevante. De asemenea, au fost organizate reuniuni ale grupurilor de experți și reuniuni bilaterale pentru a discuta efectele potențiale ale legislației UE. Conferințele pe tema accesului transfrontalier la probele electronice au fost utilizate, de asemenea, pentru a colecta feedback cu privire la inițiativă.

În ansamblu, persoanele care au participat la sondaje au considerat că utilizarea sporită a serviciilor informatice constituie o provocare în materie de aplicare a legii, întrucât autoritățile competente nu dispun adesea de echipamentele necesare pentru a procesa probele online. Procesul îndelungat de obținere a probelor este considerat, de asemenea, ca fiind unul dintre principalele obstacole. Printre alte aspecte esențiale evidențiate de autoritățile publice se

numără lipsa unei cooperări fiabile cu prestatorii de servicii, lipsa de transparență și incertitudinea juridică legată de jurisdicție în ceea ce privește măsurile de investigare. Cooperarea transfrontalieră directă între autoritățile de aplicare a legii și prestatorii de servicii digitale ar aduce o valoare adăugată în cadrul unei anchete penale. Prestatorii de servicii și unele organizații ale societății civile au subliniat necesitatea de a asigura securitatea juridică în cadrul cooperării cu autoritățile publice și de a evita conflictele de legi. Referitor la preocupările cu privire la modul în care noua legislație a UE ar putea aduce atingere drepturilor, părțile interesate au considerat că ar trebui aplicate garanții specifice ca o condiție necesară pentru orice instrument transfrontalier.

Feedbackul colectat în urma evaluării inițiale a impactului a arătat că părțile interesate consideră că remedierea lacunelor din cadrul actualului sistem de asistență judiciară reciprocă ar spori eficiența acestuia și ar îmbunătăți securitatea juridică. Unele organizații ale societății civile s-au opus legislației la nivelul UE privind cooperarea directă. Acestea preferau ca acțiunea UE să se limiteze la îmbunătățirea procedurilor de asistență judiciară reciprocă. Această idee va fi dezvoltată în cadrul măsurilor practice aprobate de Consiliu în iunie 2016.

În urma unui sondaj specific adresat autorităților publice din statele membre, a reieșit faptul că nu există nicio abordare comună privind obținerea accesului transfrontalier la probele electronice, întrucât fiecare stat membru are propriile sale practici naționale. De asemenea, prestatorii de servicii reacționează în mod diferit la cererile din partea autorităților străine de aplicare a legii, iar timpul de răspuns variază în funcție de statul membru solicitant. Acest lucru creează incertitudine juridică pentru toate părțile interesate implicate.

În general, consultarea părților interesate a indicat că actualul cadru juridic este fragmentat și complex. Acest lucru poate duce la întârzieri în timpul etapei de executare și poate compromite eficacitatea anchetelor și a urmăririlor penale ale infracțiunilor care implică accesul transfrontalier la probe electronice.

• **Evaluarea impactului**

Comitetul de analiză a reglementării a emis un aviz pozitiv cu privire la evaluarea impactului care sprijină prezenta propunere²⁰ și a formulat diverse sugestii de îmbunătățire²¹. În urma acestui aviz, evaluarea impactului a fost modificată pentru a aborda mai mult aspectele privind drepturile fundamentale legate de schimbul transfrontalier de date, în special legăturile dintre diferitele măsuri care fac parte din opțiunea preferată. De asemenea, evaluarea a fost modificată pentru a reflecta mai bine opiniile părților interesate și ale statelor membre și modul în care acestea au fost luate în considerare. În plus, contextul politic a fost revizuit pentru a include trimiteri suplimentare la diverse aspecte, cum ar fi discuțiile din cadrul grupurilor de experți care au contribuit la elaborarea inițiativei. Complementaritatea dintre diferitele măsuri (în special Directiva privind ordinul european de anchetă, negocierile referitoare la un protocol adițional la Convenția de la Budapesta și reexaminarea comună a acordului dintre UE și SUA privind AJR) a fost clarificată în ceea ce privește domeniul de

²⁰ Document de lucru al serviciilor Comisiei — Evaluarea impactului care însoțește propunerea de regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală și propunere de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul colectării de probe în cadrul procedurilor penale, SWD(2018) 118.

²¹ Comitetul de analiză a reglementării al Comisiei Europene — Aviz privind evaluarea impactului — Propunerea de regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală și propunerea de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul colectării de probe în cadrul procedurilor penale, SEC(2018) 199.

aplicare, calendarul și profunzimea, iar scenariul de referință a fost revizuit pentru a reflecta mai bine evoluțiile care sunt susceptibile să apară independent de adoptarea măsurilor propuse. În sfârșit, au fost adăugate diagrame pentru a descrie mai bine fluxurile de lucru pentru schimbul de date.

Au fost luate în considerare patru opțiuni de politică principale pe lângă scenariul de referință (opțiunea O): mai multe măsuri practice pentru a îmbunătăți atât procedurile de cooperare judiciară, cât și cooperarea directă între autoritățile publice și prestatorii de servicii (opțiunea A: nelegislativă); o opțiune care combină măsurile practice propuse la opțiunea A cu soluții internaționale la nivel bilateral sau multilateral (opțiunea B: legislativă); o opțiune care combină măsurile anterioare prevăzute la opțiunea B cu un ordin european de divulgare a probelor electronice și cu o măsură de îmbunătățire a accesului la bazele de date care furnizează la cerere informații privind abonații, cum ar fi baza WHOIS de nume de domenii (opțiunea C: legislativă); și o opțiune care combină toate măsurile anterioare prevăzute la opțiunea C cu o legislație privind accesul direct la date stocate la distanță (opțiunea D: legislativă)²².

Dacă nu adoptă nicio măsură (opțiunea O), numărul tot mai mare de cereri va duce la o înrăutățire a situației. Toate celelalte opțiuni contribuie la îndeplinirea obiectivelor inițiativei, dar într-o măsură variabilă. Opțiunea A ar îmbunătăți eficiența procedurilor actuale, de exemplu prin îmbunătățirea calității cererilor, însă posibilitatea de îmbunătățire ar fi limitată de deficiențele structurale ale sistemului actual.

Opțiunea B ar duce la mai multe îmbunătățiri oferind soluții acceptate la nivel internațional, însă rezultatul acestor soluții internaționale ar depinde în mare măsură de state terțe. Prin urmare, aceste soluții sunt nesigure și este puțin probabil să fie la fel de eficace și să ofere la fel de multe garanții ca o soluție la nivelul Uniunii.

Opțiunea C ar aduce în mod clar o valoare adăugată în comparație cu opțiunile precedente instituind, de asemenea, un instrument în interiorul UE privind cooperarea directă cu prestatorii de servicii care ar aborda majoritatea problemelor identificate atunci când există un prestator de servicii care deține datele în cauză.

Opțiunea D reprezintă pachetul de soluții cel mai complet. În afară de măsurile precedente, ea prevede o măsură legislativă privind accesul direct pentru situațiile în care nu este necesară implicarea unui prestator de servicii.

Prezenta inițiativă legislativă pe care o propune Comisia se bazează pe constatările evaluării impactului. Acest act legislativ va fi completat prin măsuri practice astfel cum se descrie în evaluarea impactului și prin continuarea lucrărilor referitoare la un protocol adițional la Convenția de la Budapesta. Pe baza propunerii sale legislative, Comisia va discuta, de asemenea, cu SUA și cu alte țări terțe posibilitatea unor viitoare acorduri bilaterale sau multilaterale privind accesul transfrontalier la probele electronice, cu garanțiile aferente. Pentru măsurile privind accesul direct și accesul la bazele de date, care fac parte din opțiunea

²² Pentru detalii, a se vedea Documentul de lucru al serviciilor Comisiei — Evaluarea impactului care însoțește propunerea de regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală și propunere de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul colectării de probe în cadrul procedurilor penale, SWD(2018) 118.

D, Comisia nu propune în prezent niciun act legislativ, însă va reflecta în continuare în legătură cu cea mai bună cale de urmat cu privire la aceste două aspecte.

Este de așteptat ca inițiativa să permită efectuarea unor anchete și urmăriri penale mai eficiente și mai eficace, îmbunătățind în același timp transparența și asumarea răspunderii și asigurând respectarea drepturilor fundamentale. De asemenea, aceasta ar trebui să consolideze încrederea în piața unică digitală îmbunătățind securitatea și reducând percepția privind impunitatea pentru infracțiunile comise pe dispozitivele conectate în rețea sau prin intermediul acestora.

Se preconizează că inițiativa va genera costuri inițiale de punere în aplicare pentru autoritățile publice, care vor fi compensate pe termen lung prin economii privind costurile recurente. Autoritățile naționale ar trebui să se adapteze la noile proceduri și să urmeze cursuri de formare. Cu toate acestea, aceste autorități vor resimți ulterior beneficiile generate de raționalizare și centralizare și de cadrul juridic clar de reglementare a cererilor de acces la date, întrucât acestea ar trebui să genereze câștiguri în materie de eficiență. De asemenea, întrucât opțiunea preferată ar determina o scădere a presiunii exercitate asupra canalelor de cooperare judiciară, țările care primesc cereri ar trebui să observe o scădere a numărului de cereri pe care trebuie să le prelucereze.

Prestatorii de servicii ar trebui să se adapteze la un nou cadru legislativ prin instituirea de (noi) proceduri și prin formarea personalului. Pe de altă parte, un cadru armonizat ar putea reduce sarcina asupra acelor prestatori care răspund în mod curent cererilor de date care nu se referă la conținut, pe care trebuie să le evalueze în conformitate cu diferitele legislații din toate statele membre. De asemenea, securitatea juridică și standardizarea procedurilor ar trebui să aibă un impact pozitiv asupra întreprinderilor mici și mijlocii, întrucât ar reduce sarcina administrativă și ar favoriza competitivitatea. În ansamblu, se preconizează că inițiativa le va permite, de asemenea, să realizeze economii.

• **Drepturi fundamentale**

Propunerea ar putea aduce atingere mai multor drepturi fundamentale:

- drepturile persoanelor ale căror date sunt consultate: dreptul la protecția datelor cu caracter personal; dreptul la respectarea vieții private și de familie; dreptul la libertatea de exprimare; dreptul la apărare; dreptul la o cale de atac eficientă și la un proces echitabil;
- drepturile prestatorului de servicii: dreptul la libertatea de a desfășura o activitate comercială; dreptul la o cale de atac eficientă;
- drepturile tuturor cetățenilor: dreptul la libertate și la siguranță.

Luând în considerare acquis-ul relevant în materie de protecție a datelor, în regulamentul propus sunt incluse garanții suficiente și importante pentru a asigura faptul că drepturile acestor persoane sunt protejate.

Întrucât ordinele pot fi emise numai în cadrul procedurilor penale și în cazul în care există situații naționale comparabile, atât în faza de urmărire penală, cât și în faza de judecată, toate garanțiile procedurale în materie de drept penal sunt aplicabile. Printre acestea se numără în special dreptul la un proces echitabil consacrat la articolul 6 al CEDO și la articolele 47 și 48 din Carta drepturilor fundamentale, precum și legislația relevantă la nivelul UE privind drepturile procedurale în cadrul procedurilor penale: Directiva 2010/64/UE privind dreptul la interpretare și traducere în cadrul procedurilor penale, Directiva 2012/13/UE privind dreptul

la informare cu privire la drepturi și la acuzațiile aduse, precum și la dreptul de a avea acces la dosarul cauzei, Directiva 2013/48/UE privind dreptul persoanelor arestate sau deținute de a primi consiliere de la un avocat și de a comunica cu rudele, Directiva 2016/343 privind consolidarea anumitor aspecte ale prezumției de nevinovăție și a dreptului de a fi prezent la propriul proces, Directiva 2016/800 privind garanțiile procedurale în cazul copiilor și Directiva 2016/1919 privind asistența judiciară pentru persoanele suspectate sau acuzate în cadrul procedurilor penale și pentru persoanele căutate în cadrul procedurii privind mandatul european de arestare.

Mai precis, intervenția prealabilă a unei autorități judiciare atunci când ordinul este emis garantează că au fost verificate legalitatea măsurii, precum și necesitatea și proporționalitatea sa în cazul respectiv. Acest fapt asigură, de asemenea, că ordinul nu aduce atingere în mod nejustificat drepturilor fundamentale, inclusiv efectelor principiilor juridice cum ar fi privilegiul juridic profesional. Autoritatea emitentă are obligația de a se asigura în fiecare caz că măsura este necesară și proporțională, inclusiv având în vedere gravitatea infracțiunii care face obiectul anchetei. Propunerea include, de asemenea, praguri pentru datele privind operațiile și datele referitoare la conținut, garantând faptul că ordinul european de divulgare a probelor electronice va fi utilizat numai pentru forme mai grave de infracțiuni legate de aceste date.

De asemenea, este abordat în mod explicit dreptul la o cale de atac eficientă pentru persoanele ale căror date sunt solicitate. Imunitățile și privilegiile legate de anumite profesii, cum ar fi cea de avocat, precum și interesele fundamentale în materie de securitate sau de apărare națională în statul destinatarului trebuie, de asemenea, să fie luate în considerare în cursul procesului în statul emitent. Revizuirea efectuată de către o autoritate judiciară constituie în acest caz o garanție suplimentară.

Întrucât ordinul este o măsură cu caracter obligatoriu, acesta aduce atingere, de asemenea, drepturilor prestatorilor de servicii, în special libertății de a desfășura o activitate comercială. Propunerea include un drept al prestatorului de servicii de a formula anumite revendicări în statul membru emitent, de exemplu în cazul în care ordinul nu a fost emis sau validat de o autoritate judiciară. În cazul în care ordinul este transmis spre executare către statul de executare, autoritatea de executare poate decide să nu recunoască sau să nu execute ordinul dacă în momentul primirii acestuia oricare dintre motivele de opoziție limitate sunt evidente și în urma consultării cu autoritatea emitentă. În plus, în cazul în care este lansată procedura de executare, destinatarul însuși va putea să se opună ordinului în fața autorității de executare pe baza oricăruia dintre aceste motive limitate. Printre acestea se numără, de exemplu, cazurile în care este evident că ordinul nu a fost emis sau validat de o autoritate competentă sau în care respectarea ordinului ar încălca în mod vădit Carta sau ar fi în mod vădit abuzivă. Acest lucru nu exclude dreptul destinatarului la o cale de atac eficientă împotriva unei decizii de impunere a unei sancțiuni.

O eventuală problemă referitoare la măsurile UE în acest domeniu este posibilitatea ca țările terțe să introducă obligații reciproce pentru prestatorii de servicii din UE care nu sunt coerente cu condițiile UE referitoare la drepturile fundamentale, inclusiv nivelul ridicat de protecție a datelor asigurat de acquis-ul UE. Propunerea abordează această situație în două moduri: în primul rând, prin introducerea unei măsuri care conține garanții solide și trimiteri explicite la condițiile și garanțiile prevăzute deja în acquis-ul UE, servind astfel drept model pentru legislația străină; și în al doilea rând, prin includerea unei clauze privind „obligațiile contradictorii” care le permite prestatorilor de servicii să identifice și să semnaleze obligațiile contradictorii cu care se confruntă, ducând astfel la efectuarea unui control jurisdicțional.

Această clauză este menită să asigure respectarea atât a legilor generale privind blocarea, de exemplu Legea privind confidențialitatea comunicațiilor electronice din SUA (*Electronic Communications Privacy Act* - ECPA), care interzice divulgarea în legătură cu datele referitoare la conținut din zona sa geografică, cu excepția unor circumstanțe limitate, cât și a legilor care nu interzic în general divulgarea, dar care ar putea să o facă în anumite cazuri specifice. Pentru cazurile legate de ECPA, accesul la datele referitoare la conținut ar putea fi împiedicat în anumite situații în prezent și, prin urmare, asistența judiciară reciprocă ar trebui să rămână principalul instrument pentru a avea acces la astfel de date. Cu toate acestea, având în vedere modificările care decurg din adoptarea Legii CLOUD²³ din SUA, legea privind blocarea ar putea fi suspendată în cazul în care UE ar încheia un acord cu SUA. Acordurile internaționale suplimentare și cu alți parteneri-cheie ar permite reducerea în continuare a situațiilor de conflicte de legi.

Având în vedere cele de mai sus, măsurile din prezenta propunere sunt compatibile cu drepturile fundamentale.

4. IMPLICAȚIILE BUGETARE

Propunerea legislativă de regulament nu are un impact asupra bugetului Uniunii.

5. ALTE ELEMENTE

- **Planuri de punere în aplicare și măsuri de monitorizare, evaluare și raportare**

Regulamentul este direct aplicabil în Uniune. Acesta va fi aplicat direct aplicabil de către practicieni, fără a fi necesară modificarea sistemelor juridice interne.

Regulamentul va fi evaluat și Comisia va prezenta un raport Parlamentului European și Consiliului cel târziu la 5 ani de la data intrării sale în vigoare. Pe baza constatărilor raportului, în special privind lacunele pe care le-ar putea lăsa regulamentul și care sunt relevante în practică și luând în considerare evoluțiile tehnologice, Comisia va evalua necesitatea de a extinde domeniul de aplicare al regulamentului. Dacă este necesar, Comisia va prezenta propuneri în vederea adaptării prezentului regulament. Statele membre îi vor furniza Comisiei informațiile necesare pentru întocmirea raportului. Statele membre vor colecta datele necesare pentru monitorizarea anuală a regulamentului.

Dacă este necesar, Comisia va furniza orientări prestatorilor de servicii pentru a le permite acestora să respecte obligațiile prevăzute în regulament.

- **Explicații detaliate cu privire la prevederile specifice ale propunerii**

	REGULAMENT	
	Articolul	Considerentul
I. Obiect, definiții și	1. Obiect	1-15

²³ La 23 martie 2018, Legea CLOUD (*Clarifying Lawful Overseas Use of Data*) a fost adoptată în Statele Unite. Legea CLOUD este disponibilă [aici](#).

domeniu de aplicare	2. Definiții	16-23
	3. Domeniul de aplicare	24-27
II. Ordinul european de divulgare a probelor electronice, ordinul european de păstrare a probelor electronice și certificatele aferente, reprezentantul legal	4. Autoritatea emitentă	30
	5. Condițiile pentru emiterea unui ordin european de divulgare a probelor electronice	28-29, 31-35
	6. Condițiile pentru emiterea unui ordin european de păstrare a probelor electronice	36
	7. Destinatarul unui ordin european de divulgare a probelor electronice și al unui ordin european de păstrare a probelor electronice	37
	8. Certificatul de ordin european de divulgare a probelor electronice și certificatul de ordin european de păstrare a probelor electronice	38-39
	9. Executarea unui EPOC	40-41
	10. Executarea unui EPOC-PR	42
	11. Confidențialitate și informații destinate utilizatorilor	43
	12. Rambursarea cheltuielilor	Nu există
III. Sancțiuni și executare	13. Sancțiuni	Nu există
	14. Procedura de executare	44-45, 55
IV. Căi de atac	15. și 16. Procedura de control jurisdicțional în cazul unor obligații contradictorii care rezultă din legea unei țări terțe	47-53
	17. Căi de atac eficiente	54
	18. Respectarea privilegiilor și a imunităților în temeiul legislației statului de executare	35
V. Dispoziții finale	19. Monitorizarea și raportarea	58
	20. Modificarea certificatelor și a formularelor	59-60
	21. Exercițarea delegării	60
	22. Notificări	Nu există
	23. Relația cu ordinele europene de anchetă	61

	24. Evaluare	62
	25. Intrarea în vigoare	Nu există

Capitolul 1: Obiect, definiții și domeniu de aplicare

Articolul 1: Obiect

Acest articol stabilește domeniul general de aplicare și scopul propunerii, și anume de a stabili normele în temeiul cărora o autoritate judiciară competentă din Uniunea Europeană poate cere unui prestator de servicii care oferă servicii în Uniune să divulge sau să păstreze probe electronice, prin intermediul unui ordin european de divulgare sau de păstrare a probelor electronice. Aceste instrumente pot fi folosite numai în situațiile transfrontaliere, mai precis în situațiile în care prestatorul de servicii este stabilit sau reprezentat într-un alt stat membru.

Prezentul regulament oferă instrumente suplimentare autorităților de anchetă în vederea obținerii de probe electronice, fără a limita însă competențele deja prevăzute de dreptul intern de a impune obligații prestatorilor de servicii stabiliți sau reprezentați pe teritoriul lor. Prin urmare, în cazul în care prestatorul de servicii este stabilit sau reprezentat în același stat membru, autoritățile statului membru respectiv utilizează măsuri naționale pentru a impune obligații prestatorului de servicii.

Datele solicitate prin intermediul unui ordin european de divulgare a probelor electronice ar trebui să fie transmise în mod direct autorităților fără intervenția autorităților din statul membru în care este stabilit sau reprezentat prestatorul de servicii. De asemenea, în temeiul regulamentului, amplasarea datelor nu mai este considerată drept un factor de conexiune determinant, întrucât în mod normal stocarea datelor nu implică niciun fel de control din partea statului pe al cărui teritoriu sunt stocate datele. Condițiile de stocare sunt stabilite în majoritatea cazurilor de către prestator, pe baza unor considerente de ordin comercial²⁴.

În plus, regulamentul se aplică, de asemenea, în cazul în care prestatorii de servicii nu sunt stabiliți sau reprezentați în Uniune, însă oferă servicii în Uniune. Această dispoziție se regăsește la articolul 3 alineatul (1).

Atunci când propunerea se referă la un prestator de servicii stabilit sau reprezentat într-un stat membru prin intermediul unui reprezentant legal, simplul fapt de a desemna un reprezentant legal nu duce la crearea unui sediu al prestatorului de servicii în sensul prezentului regulament.

La articolul 1 alineatul (2) se reamintește că prezentul regulament nu are ca efect modificarea obligației de respectare a drepturilor fundamentale și a principiilor juridice astfel cum sunt consacrate la articolul 6 din TUE.

Articolul 2: Definiții

Acest articol stabilește definițiile care se aplică pentru întregul instrument.

²⁴ Evaluarea impactului conține explicații suplimentare.

Următoarele tipuri de prestatori de servicii intră în domeniul de aplicare al regulamentului: prestatorii de servicii de comunicații electronice, prestatorii de servicii ale societății informaționale pentru care stocarea datelor este o componentă definitorie a serviciului furnizat utilizatorului, inclusiv rețelele sociale, în măsura în care acestea nu se califică drept servicii de comunicații electronice, piețe online care facilitează tranzacțiile între utilizatorii lor (cum ar fi consumatori sau întreprinderi) sau alți prestatori de servicii de găzduire, precum și prestatorii de servicii de nume de domenii și de numerotare de internet.

Domeniul de aplicare al regulamentului acoperă prestatorii de servicii de comunicații electronice, astfel cum sunt definite în [Directiva de instituire a Codului european al comunicațiilor electronice]. Serviciile tradiționale de telecomunicații, consumatorii și întreprinderile utilizează tot mai mult noile servicii bazate pe internet care permit comunicațiile interpersonale, cum ar fi serviciile de telefonie prin internet, de mesagerie instantanee și de e-mail, în locul serviciilor de comunicații tradiționale. Prin urmare, aceste servicii, împreună cu rețelele de socializare, cum ar fi Twitter sau Facebook, care le permit utilizatorilor să partajeze conținut, ar trebui să fie reglementate de prezenta propunere.

În multe cazuri, datele nu mai sunt stocate într-un dispozitiv al utilizatorului, ci sunt puse la dispoziție în infrastructuri „cloud”, care permit în principiu accesarea acestora de oriunde. Prestatorii de servicii nu trebuie să fie stabiliți sau să aibă servere în fiecare jurisdicție, ci utilizează o administrație centralizată și sisteme descentralizate pentru a stoca datele și a-și presta serviciile. Ei procedează astfel pentru a optimiza echilibrarea sarcinilor și a reduce timpul de răspuns la solicitările de date din partea utilizatorilor. Rețelele de distribuție de conținut (CDN) sunt de obicei utilizate pentru a accelera distribuția de conținut prin copierea conținutului în mai multe servere distribuite în întreaga lume. Acest lucru le permite societăților să furnizeze conținut de la serverul care este cel mai aproape de utilizator sau care poate direcționa comunicarea prin intermediul unei rețele mai puțin congestionate. Pentru a ține seama de această evoluție, definiția acoperă serviciile „cloud” și alte servicii de găzduire care oferă o varietate de resurse de informatice precum rețelele, serverele sau alte infrastructuri, servicii de stocare, aplicații și servicii care permit stocarea datelor în diferite scopuri. De asemenea, instrumentul se aplică piețelor digitale care le permit consumatorilor și/sau întreprinderilor să încheie tranzacții prin intermediul vânzărilor sau al contractelor de servicii online. Astfel de tranzacții se efectuează fie pe site-ul web al pieței online, fie pe site-ul web al unui comerciant care utilizează serviciile informatice furnizate de piața online. Prin urmare, această piață este în posesia unor probe electronice care pot fi necesare în cursul procedurilor penale.

Serviciile pentru care stocarea datelor nu este o componentă definitorie nu sunt reglementate de propunere. Deși majoritatea serviciilor furnizate de prestatori implică o anumită formă de stocare a datelor, în special atunci când acestea sunt furnizate online la distanță, serviciile pentru care stocarea datelor nu este o caracteristică principală și, prin urmare, are doar o natură accesorie, pot fi tratate separat, inclusiv serviciile juridice, de arhitectură, de inginerie și de contabilitate prestate online la distanță.

Datele deținute de prestatorii de servicii de infrastructură de internet, cum ar fi registrele de nume de domenii, operatorii de registre de nume de domenii și prestatorii de servicii de protecție a vieții private în sectorul comunicațiilor electronice și de servicii de proxy sau registrele regionale de internet pentru adrese de protocol de internet, pot fi relevanți în cadrul procedurilor penale, întrucât aceștia pot oferi indicii care permit identificarea unei persoane sau entități implicate în activități criminale.

Printre categoriile de date care poate fi obținute prin intermediul unui ordin european de divulgare a probelor electronice de către autoritățile competente se numără datele privind abonații, datele privind accesul, datele privind operațiile (aceste trei categorii fiind denumite în general în mod colectiv „date care nu se referă la conținut”) și datele referitoare la conținut stocate. Această distincție, în afară de datele privind accesul, există în ordinea juridică a multor state membre și, de asemenea, în cadrele juridice ale unor țări terțe.

Toate categoriile conțin date cu caracter personal care sunt astfel acoperite de garanții în temeiul acquis-ului UE în materie de protecție a datelor. Intensitatea impactului asupra drepturilor fundamentale variază între acestea, în special datele privind abonații, pe de parte, și datele privind operațiile și cele referitoare la conținut, pe de altă parte. Este esențial ca toate aceste categorii să fie reglementate de instrument: datele privind abonații și datele privind accesul sunt adesea un punct de plecare pentru a obține indicii în cadrul unei anchete cu privire la identitatea unui suspect, în timp ce datele privind operațiile și datele referitoare la conținut sunt cele mai relevante ca element probatoriu. Din cauza gradului diferit de interferență cu drepturile fundamentale, se justifică impunerea unor condiții diferite pentru datele privind abonații, pe de o parte, și datele privind operațiile și cele referitoare la conținut, pe de altă parte, astfel cum se prevede în mai multe dispoziții din regulament.

Este adecvat să se identifice datele privind accesul drept o categorie specifică de date utilizată în prezentul regulament. Datele privind accesul astfel cum sunt definite aici sunt solicitate pentru același obiectiv ca și datele privind abonații, și anume pentru a identifica utilizatorul, iar nivelul de interferență cu drepturile fundamentale este similar. În consecință, acestea ar trebui să se supună acelorași condiții ca și datele privind abonații. Prin urmare, prezenta propunere introduce o nouă categorie de date, care trebuie să fie tratate în același mod ca și datele privind abonații, în cazul în care se urmărește același obiectiv.

Articolul 2 definește statele membre și autoritățile care ar putea participa la procedură. La articolul 4 este inclusă o definiție a autorității emitente.

Cazurile de urgență sunt situații excepționale care necesită adesea o reacție rapidă din partea prestatorilor de servicii și pentru care sunt aplicabile condiții speciale. Prin urmare, ele sunt definite separat în acest articol.

Articolul 3: Domeniul de aplicare

Acest articol definește domeniul de aplicare al propunerii. Regulamentul se aplică tuturor prestatorilor de servicii care oferă servicii în Uniune, inclusiv prestatorilor de servicii care nu sunt stabiliți în Uniune. Furnizarea activă de servicii în Uniune, cu toate avantajele care decurg din aceasta, justifică faptul că acești prestatori de servicii fac, de asemenea, obiectul regulamentului și să creeze condiții de concurență echitabile între participanții de pe aceleași piețe. În plus, în cazul în care acești prestatori de servicii nu ar intra sub incidența regulamentului, acest lucru ar crea o lacună și ar facilita eludarea domeniului de aplicare al regulamentului de către infractori.

Pentru a stabili dacă sunt oferite servicii, autoritățile trebuie să evalueze dacă prestatorul de servicii le permite unor persoane juridice sau fizice din unul sau mai multe state membre să utilizeze serviciile sale. Cu toate acestea, simpla accesibilitate a serviciului (care ar putea să rezulte, de asemenea, din accesibilitatea site-ului web al prestatorului de servicii sau al unui intermediar sau din accesibilitatea unei adrese de e-mail și a altor date de contact), nu ar trebui să fie o condiție suficientă pentru aplicarea prezentului regulament. Prin urmare, este necesară

existența unei legături substanțiale cu acele state membre pentru a stabili o legătură suficientă între prestator și teritoriul pe care își oferă serviciile. O astfel de legătură substanțială există atunci când un prestator de servicii dispune de un sediu în unul sau mai multe state membre. În absența unui sediu în Uniune, criteriul referitor la o legătură substanțială cu Uniunea ar trebui să fie evaluat pe baza existenței unui număr semnificativ de utilizatori în unul sau mai multe state membre sau a orientării activităților către unul sau mai multe state membre. Orientarea activităților către unul sau mai multe state membre poate fi stabilită pe baza tuturor circumstanțelor relevante, inclusiv pe baza unor factori precum utilizarea unei limbi sau a unei monede folosite în general într-un stat membru. Orientarea activităților către un stat membru ar putea să reiasă, de asemenea, din disponibilitatea unei aplicații în magazinul de aplicații naționale relevante, din oferirea de publicitate locală sau de publicitate în limba folosită într-un stat membru, din utilizarea oricărei informații provenite de la persoane din statele membre în cursul activităților sale sau din gestionarea relațiilor cu clienții, de exemplu prin furnizarea de servicii pentru clienți în limba folosită în general într-un stat membru. De asemenea, trebuie să se presupună existența unei legături substanțiale atunci când un prestator de servicii își direcționează activitățile spre unul sau mai multe state membre, astfel cum se prevede la articolul 17 alineatul (1) litera (c) din Regulamentul nr. 1215/2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială.

Ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice sunt măsuri de investigare care pot fi emise doar în cadrul unor anchete sau proceduri penale pentru infracțiuni concrete. Legătura cu o anchetă concretă le diferențiază de măsurile preventive sau de obligațiile de păstrare a datelor prevăzute de lege și asigură aplicarea drepturilor procedurale aplicabile procedurilor penale. Prin urmare, competența de a deschide anchete pentru o anumită infracțiune este o condiție prealabilă pentru utilizarea regulamentului.

Ca o cerință suplimentară, datele solicitate trebuie să fie legate de serviciile oferite de prestatorul de servicii în Uniune.

Capitolul 2: Ordinul european de divulgare a probelor electronice, ordinul european de păstrare a probelor electronice și certificatele aferente

Articolul 4: Autoritatea emitentă

Atunci când este emis un ordin european de divulgare sau de păstrare a probelor electronice, ar trebui să intervină întotdeauna o autoritate judiciară fie în calitate de autoritate de emitere, fie în calitate de autoritate de validare. Pentru ordinele de divulgare de date privind operațiunile sau de date referitoare la conținut este necesară intervenția unui judecător sau a unei instanțe. Pentru datele privind abonații și cele privind accesul, acest lucru poate fi realizat și de către un procuror.

Articolul 5: Condițiile pentru emiterea unui ordin european de divulgare a probelor electronice

Articolul 5 stabilește condițiile pentru emiterea unui ordin european de divulgare a probelor electronice. Acestea trebuie să fie evaluate de către autoritatea judiciară emitentă.

Ordinul european de divulgare a probelor electronice poate fi emis doar dacă acest lucru este necesar și proporțional în cazul respectiv. În plus, acesta nu ar trebui emis decât dacă o măsură similară ar fi disponibilă într-o situație internă comparabilă în statul emitent.

Ordinele de divulgare de date privind abonații și de date privind accesul pot fi emise pentru orice infracțiune. Datele privind operațiile și cele referitoare la conținut ar trebui să facă obiectul unor cerințe mai stricte pentru a reflecta natura mai sensibilă a acestor date și gradul proporțional mai ridicat de intruziune al ordinelor care vizează astfel de date, în comparație cu datele privind abonații și datele privind accesul. Prin urmare, ordinele pot fi emise numai pentru infracțiuni care se pedepsesc cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani sau mai mult. Stabilirea unui prag pe baza pedepsei maxime cu închisoarea permite o abordare mai proporțională, împreună cu o serie de alte condiții și garanții *ex ante* și *ex post* pentru a asigura respectarea proporționalității și a drepturilor persoanelor afectate.

În același timp, pragul nu ar trebui să submineze eficacitatea instrumentului și utilizarea sa de către practicieni. Statele membre aplică diferite praguri maxime ale pedepsei în funcție de sistemul lor național. Codurile penale naționale variază și nu sunt armonizate. Acest lucru este valabil pentru infracțiunile și pentru sancțiunile aplicabile acestora. De asemenea, codurile de procedură naționale diferă în ceea ce privește pragurile pentru obținerea de date privind operațiile sau de date referitoare la conținut: unele state membre nu stabilesc niciun prag specific; altele au stabilit o listă de infracțiuni. Un prag de trei ani limitează domeniul de aplicare a instrumentului la infracțiuni mai grave, fără a afecta excesiv posibilitățile sale de utilizare de către practicieni. Acest prag exclude din domeniul de aplicare o gamă largă de infracțiuni, în funcție de codul penal al statului membru (de exemplu, în unele state membre participarea la activitatea unui grup infracțional organizat și la răpiri, dar și infracțiuni precum furturile minore, fraudă sau agresiunea, pentru care utilizarea unui ordin transfrontalier de divulgare pentru datele mai sensibile poate fi considerată disproporționată). Pe de altă parte, un prag de trei ani include infracțiuni care necesită o abordare mai eficientă, cum ar fi apartenența la o organizație criminală, finanțarea grupurilor teroriste, sprijin sau promovarea unei organizații criminale, formarea în vederea comiterii de infracțiuni teroriste, anumite infracțiuni săvârșite cu intenția de a comite acte de terorism și pregătirea unei infracțiuni care să fie săvârșită cu intenția de a comite acte de terorism sau pregătirea unei luări de ostatic, care altfel ar fi excluse în cazul în care s-ar aplica un prag mai ridicat, în funcție de statul membru. Acest prag a fost ales pentru a asigura un echilibru pentru toate statele membre între eficiența anchetelor penale și protecția drepturilor și a proporționalității. De asemenea, stabilirea unui prag are avantajul de a fi ușor de aplicat în practică.

În plus, ordinele de divulgare de date privind operațiile sau de date referitoare la conținut pot fi emise, de asemenea, pentru infracțiuni armonizate specifice enumerate în dispoziție pentru care vor fi disponibile probe în general doar în format electronic. Acest lucru justifică aplicarea regulamentului și în cazurile în care pedeapsa maximă cu închisoarea este mai mică decât pragul menționat mai sus; în caz contrar, aceste infracțiuni nu ar putea fi anchetate în mod adecvat, ceea ce ar putea conduce la impunitate. Infracțiunile fac obiectul următoarelor dispoziții specifice: (i) Decizia-cadru 2001/413/JAI a Consiliului de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul, (ii) Directiva 2011/92/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului și (iii) Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului. De asemenea, pot fi emise ordine pentru infracțiunile enumerate în Directiva (UE) 2017/541 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului. Unele dintre aceste infracțiuni au un prag minim al pedepsei maxime de cel puțin 1 an, altele de 2 ani, însă niciun prag minim nu este inferior unui prag maxim de 1 an.

De asemenea, articolul stabilește informațiile obligatorii pe care trebuie să le conțină ordinul european de divulgare a probelor electronice pentru a permite prestatorului de servicii să identifice și să divulge datele solicitate. Ordinul european de divulgare a probelor electronice include, de asemenea, raționamentul privind motivele pentru care această măsură este necesară și proporțională.

Ordinul european de divulgare a probelor electronice este pus în aplicare prin emiterea unui certificat de ordin european de divulgare a probelor electronice (EPOC) (a se vedea articolul 8), care este tradus și transmis prestatorului de servicii. EPOC conține aceleași informații obligatorii ca și ordinul, cu excepția motivelor pentru necesitatea și proporționalitatea măsurii sau a unor detalii suplimentare cu privire la caz.

În situațiile în care datele solicitate sunt stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei societăți, cel mai frecvent în cazul serviciilor de găzduire sau de software, societatea însăși ar trebui să fie principalul destinatar al unei cereri formulate de către autoritățile de anchetă. Acest demers ar putea necesita un ordin european de anchetă sau o procedură de asistență judiciară reciprocă în cazul în care această societate nu ar fi un prestator de servicii care intră sub incidența prezentului regulament. Prestatorul de servicii poate fi destinatarul unui ordin european de divulgare a probelor electronice doar în cazul în care nu ar fi adecvat ca cererea să fie adresată societății, în special atunci când acest lucru ar risca să pericliteze ancheta, de exemplu atunci când societatea însăși face obiectul anchetei.

Înainte de a emite un ordin european de divulgare a probelor electronice, autoritatea emitentă trebuie să ia în considerare, de asemenea, imunitățile și privilegiile acordate în temeiul legislației statului membru al destinatarului ordinului sau orice impact asupra intereselor fundamentale ale statului membru respectiv, cum ar fi securitatea și apărarea națională. Obiectivul acestei dispoziții este acela de a garanta faptul că imunitățile și privilegiile care protejează datele solicitate în statul membru al prestatorului de servicii sunt luate în considerare în statul emitent, în special în cazul în care acestea oferă o mai bună protecție decât legea statului emitent.

Articolul 6: Condițiile pentru emiterea unui ordin european de păstrare a probelor electronice

Un ordin european de păstrare a probelor electronice face obiectul unor condiții similare cu cele ale ordinului european de divulgare a probelor electronice. El poate fi emis pentru o infracțiune în conformitate cu celelalte condiții prevăzute la articolul 6. Obiectivul său este de a împiedica eliminarea, ștergerea sau modificarea datelor în situațiile în care poate dura mai mult timp obținerea divulgării acestor date, de exemplu întrucât vor fi utilizate canale de cooperare judiciară. Având în vedere, de exemplu, că ordinul european de anchetă poate fi emis în general pentru orice infracțiune fără a fi limitat la vreun prag, nici ordinul european de păstrare a probelor electronice nu va fi limitat. În caz contrar, acest instrument nu ar fi eficace. Pentru a permite autorităților de anchetă să acționeze rapid și având în vedere faptul că cererea relevantă de divulgare a datelor va fi cererea ulterioară în cazul căreia toate condițiile vor face obiectul unei noi examinări, ordinele europene de păstrare a probelor electronice pot fi emise sau validate și de către un procuror.

Articolul 7: Destinatarul unui ordin european de divulgare a probelor electronice sau al unui ordin european de păstrare a probelor electronice

Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice ar trebui adresate unui reprezentant legal desemnat de către prestatorul de servicii, în scopul de a aduna probe în cadrul procedurilor penale, în conformitate cu directiva de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul colectării de probe în cadrul procedurilor penale. Transmiterea se va efectua sub forma unui certificat de ordin european de divulgare a probelor electronice (EPOC) sau a unui certificat de ordin european de păstrare a probelor electronice (EPOC-PR), astfel cum se menționează la articolul 8. Acest reprezentant legal va fi responsabil cu primirea certificatelor și cu executarea lor deplină și în timp util. Prestatorii de servicii pot alege astfel modul lor de organizare în vederea divulgării datelor solicitate de autoritățile statului membru.

În cazul în care nu a fost desemnat niciun reprezentant legal, ordinele pot fi adresate oricărui sediu al prestatorului de servicii în Uniune. Această opțiune alternativă are rolul de a asigura eficacitatea sistemului în cazul în care prestatorul de servicii nu a desemnat (încă) un reprezentant special, de exemplu în cazul în care nu există obligația de a desemna un reprezentant legal în conformitate cu directiva, întrucât prestatorii de servicii sunt stabiliți și își desfășoară activitatea doar într-un stat membru sau în cazurile în care obligația de a desemna un reprezentant legal nu este încă în vigoare, înainte de termenul de transpunere a directivei.

În cazul nerespectării ordinului de către reprezentantul legal, există două situații în care ordinul poate fi adresat de către autoritatea emitentă oricărui sediu al prestatorului de servicii situat în Uniune: în cazuri de urgență astfel cum sunt definite la articolul 9 alineatul (2) și în cazurile în care reprezentantul legal nu își respectă obligațiile în temeiul articolelor 9 și 10 și în care autoritatea emitentă consideră că există riscuri clare de pierdere a datelor.

Articolul 8: Certificatul de ordin european de divulgare a probelor electronice și de ordin european de păstrare a probelor electronice

EPOC și EPOC-PR servesc la transmiterea ordinelor către destinatarul definit la articolul 7. Modelele pentru ambele certificate sunt prevăzute în anexele I și II la regulament; acestea trebuie să fie traduse în una dintre limbile oficiale ale statului membru în care se află destinatarul. Prestatorul de servicii poate declara că ordinele vor fi acceptate și în alte limbi oficiale ale Uniunii. Obiectivul certificatelor este de a furniza toate informațiile necesare care urmează a fi transmise destinatarului într-un format standardizat, reducând la minimum sursele de erori, permițând identificarea facilă a datelor și evitând cât mai mult posibil textul liber, ceea ce duce la o diminuare a costurilor de traducere. Pentru a evita punerea în pericol a anchetelor, certificatul nu include raționamentul integral pe baza motivelor referitoare la necesitate și proporționalitate sau detalii suplimentare cu privire la caz. Prin urmare, acesta este necesar doar ca parte a ordinului, pentru a-i permite persoanei suspectate să îl conteste ulterior în cursul procedurilor penale.

Unii prestatori de servicii au instituit deja platforme pentru depunerea cererilor de către autoritățile de aplicare a legii. Utilizarea acestor platforme nu este împiedicată de regulament, întrucât oferă multe avantaje, inclusiv posibilitatea unei autentificări facile și a unei transmiteri sigure a datelor. Cu toate acestea, aceste platforme trebuie să permită transmiterea EPOC și a EPOC-PR în formatul prevăzut în anexele I și II, fără a solicita date suplimentare cu privire la ordin.

Platformele instituite de statele membre sau organismele Uniunii pot oferi, de asemenea, mijloace securizate de transmitere și pot facilita autentificarea ordinelor și colectarea de statistici. Ar trebui să se aibă în vedere o eventuală extindere a platformelor eCodex și SIRIUS pentru a include o conexiune securizată cu prestatorii de servicii în scopul transmiterii EPOC și EPOC-PR și, după caz, a răspunsurilor din partea prestatorilor de servicii.

Articolul 9: Executarea unui EPOC

Articolul 9 le impune destinatarilor să răspundă la EPOC și introduce termene obligatorii. Termenul normal este de 10 zile, însă autoritățile pot stabili un termen mai scurt atunci când acest lucru se justifică. În plus, în cazuri de urgență, definite drept situații în care există o amenințare iminentă la adresa vieții sau a integrității fizice a unei persoane sau la adresa unei infrastructuri critice, termenul este de 6 ore.

Dispoziția asigură, de asemenea, posibilitatea unui dialog între destinatar și autoritatea emitentă. În cazul în care EPOC este incomplet, vădit eronat sau nu conține suficiente informații pentru executarea acestuia de către prestatorul de servicii, destinatarul contactează autoritatea emitentă și solicită clarificări, utilizând formularul prevăzut în anexa III. De asemenea, el informează autoritatea emitentă în cazurile în care nu poate furniza datele din motive de forță majoră sau de imposibilitate *de facto*. Acesta este cazul dacă, de exemplu, persoana ale cărei date sunt solicitate nu este un client al serviciului respectiv sau — de exemplu în temeiul altor obligații de confidențialitate — datele au fost eliminate în mod legal de către prestatorul de servicii înainte ca acesta sau reprezentantul său legal să primească ordinul. Autoritatea emitentă ar trebui să fie informată cu privire la aceste circumstanțe pentru a reacționa rapid, pentru a colecta eventual probele electronice de la un alt prestator de servicii și pentru a evita ca autoritatea emitentă să lanseze o procedură de executare în cazul în care acest lucru nu ar avea sens.

În cazul în care destinatarul nu furnizează informațiile sau nu le furnizează în mod exhaustiv sau în termenul stabilit, din alte motive decât cele menționate mai sus, acesta trebuie să informeze autoritatea emitentă cu privire la motivele sale, utilizând formularul prevăzut în anexa III. Astfel, destinatarii pot semnală autorității emitente orice problemă legată de executarea EPOC. Acest lucru îi permite autorității emitente să corecteze sau să reexamineze EPOC într-un stadiu incipient, înainte de etapa executării.

În cazul în care datele nu sunt divulgate imediat, în special atunci când se lansează un dialog între destinatar și autoritatea emitentă, ceea ce înseamnă că termenele-limită prevăzute la articolul 9 alineatul (1) nu vor mai fi respectate, prestatorul de servicii are obligația de a păstra datele pentru a evita pierderea lor, începând din momentul primirii EPOC, cu condiția ca datele să poată fi identificate. Păstrarea poate fi necesară pentru EPOC-ul clarificat sau pentru o cerere ulterioară de asistență judiciară reciprocă sau de ordin european de anchetă care va fi trimisă în locul EPOC inițial.

Articolul 10: Executarea unui EPOC-PR

Executarea unui EPOC-PR necesită păstrarea datelor disponibile în momentul primirii ordinului. Prestatorii de servicii ar trebui să păstreze date atât timp cât este necesar pentru a divulga datele la cerere, cu condiția ca autoritatea emitentă să confirme în termen de 60 de zile de la data la care a emis ordinul că a lansat cererea ulterioară de divulgare. Acest lucru

presupune că au fost adoptate cel puțin unele măsuri oficiale, de exemplu, trimiterea unei cereri de asistență juridică reciprocă pentru a fi tradusă.

Pe de altă parte, cererile de păstrare ar trebui emise sau menținute doar atâta timp cât este necesar pentru a permite introducerea unei cereri ulterioare de divulgare a acestor date. Pentru a evita păstrarea datelor în mod inutil sau pentru prea mult timp, autoritatea care a emis ordinul european de păstrare a probelor electronice informează destinatarul imediat ce se adoptă o decizie de a nu emite sau de a retrage un ordin de divulgare sau o cerere de cooperare judiciară.

Dispoziția asigură, de asemenea, posibilitatea unui dialog între destinatar și autoritatea emitentă, în mod similar cu dispozițiile de la articolul 9. În cazul în care EPOC-PR este incomplet, vădit eronat sau nu conține suficiente informații pentru executarea acestuia de către prestatorul de servicii, destinatarul contactează autoritatea emitentă și solicită clarificări, utilizând formularul prevăzut în anexa III. De asemenea, el informează autoritatea emitentă în cazurile în care nu poate furniza datele din cauza unor circumstanțe considerate ca fiind forță majoră sau imposibilitate *de facto* sau din alte motive.

Articolul 11: Confidențialitate și informații destinate utilizatorilor

Este necesar să fie protejată confidențialitatea anchetei în curs, inclusiv faptul că a existat un ordin pentru obținerea datelor relevante. Acest articol se inspiră din articolul 19 din Directiva privind ordinul european de anchetă. El prevede obligația ca destinatarul și prestatorul de servicii, în cazul în care acesta este diferit de destinatar, să protejeze confidențialitatea EPOC sau EPOC-PR, în special abținându-se de la a informa persoana ale cărei date sunt solicitate, în cazul în care acest lucru este solicitat de către autoritatea emitentă, pentru a proteja anchetarea infracțiunilor, în conformitate cu articolul 23 din RGPD.

Pe de altă parte, este important, inclusiv pentru exercitarea căilor de atac, ca persoana ale cărei date au fost solicitate să fie informată. În cazul în care acest lucru nu se realizează de către prestatorul de servicii la cerere autorității emitente, aceasta din urmă informează persoana respectivă în conformitate cu articolul 13 din Directiva privind protecția datelor în materie de asigurare a respectării legii în momentul în care nu mai există riscul periclitării anchetei și include și informații privind căile de atac disponibile. Întrucât aceste informații interferează mai puțin cu drepturile în cauză, ele nu sunt furnizate în cazul unui ordin european de păstrare a probelor electronice, ci doar în cazul unui ordin european de divulgare a probelor electronice.

Articolul 12: Rambursarea cheltuielilor

Prestatorul de servicii poate solicita, de asemenea, rambursarea cheltuielilor sale de către statul emitent, dacă acest lucru este prevăzut în dreptul intern al statului emitent pentru ordinele naționale în cazuri interne similare, în conformitate cu aceste dreptul intern al statului emitent. Această dispoziție asigură tratamentul egal al prestatorilor de servicii care sunt destinatari ai unui ordin intern și al celor care sunt destinatari ai unui EPOC de către același stat membru, în cazul în care statul membru respectiv a ales să ramburseze anumiți prestatori de servicii. Pe de altă parte, regulamentul propus nu armonizează rambursarea costurilor, întrucât statele membre au făcut alegeri diferite în această privință.

Costurile pot fi revendicate fie direct de către prestatorul de servicii sau prin intermediul reprezentantului său legal. Ele nu pot fi rambursate decât o singură dată.

Capitolul 3: Sancțiuni și executare

Articolul 13: Sancțiuni

Statele membre se asigură că există sancțiuni pecuniare eficace, proporționale și disuasive în cazul în care prestatorii de servicii nu își respectă obligațiile în temeiul articolelor 9, 10 sau 11. Acest lucru nu aduce atingere legislațiilor naționale care prevăd impunerea de sancțiuni penale pentru astfel de situații.

Articolul 14: Procedura de executare

Articolul 14 prevede o procedură pentru executarea ordinelor în cazul nerespectării acestora, cu ajutorul statului membru în care se află destinatarul certificatului transmis. În funcție de destinatarul inițial, acesta este fie statul membru al prestatorului de servicii, fie cel al reprezentantului legal. Autoritatea emitentă transferă ordinul integral, inclusiv raționamentul privind necesitatea și proporționalitatea, însoțit de certificat, autorității competente din statul de executare, care îl execută în conformitate cu dreptul său intern și utilizând, dacă este necesar, sancțiunile menționate la articolul 13. În cazul în care ordinul este transmis spre executare către statul de executare, autoritatea de executare poate decide să nu recunoască sau să nu execute ordinul dacă, în momentul primirii acestuia, consideră că se aplică unul dintre motivele de opoziție limitate și în urma consultării cu autoritatea emitentă. În plus, în cazul în care este lansată procedura de executare, destinatarul însuși va putea să se opună ordinului în fața autorității de executare. Destinatarul poate face acest lucru pe baza oricăruia dintre aceste motive, cu excepția imunităților și a privilegiilor, dar incluzând cazurile în care este evident faptul că ordinul nu a fost emis sau validat de o autoritate competentă sau că respectarea sa ar încălca în mod vădit Carta drepturilor fundamentale a Uniunii Europene sau ar fi în mod vădit abuzivă. De exemplu, un ordin care solicită divulgarea de date referitoare la conținut privind o categorie nedefinită de persoane dintr-o zonă geografică sau care nu are nicio legătură cu procedura penală efectivă ar ignora în mod evident condițiile pentru emiterea unui ordin european de divulgare a probelor electronice și acest lucru ar reieși deja chiar din conținutul certificatului. Alte motive pot fi invocate numai de către persoana ale cărei date sunt solicitate, în cadrul căilor de atac de care dispune în statul emitent (a se vedea articolul 17 de mai jos). În plus, prestatorii de servicii trebuie să dispună de o cale de atac împotriva deciziei autorității de executare prin care li se impune o sancțiune.

Procedura de executare conține mai multe termene-limită pentru ca autoritatea de executare și autoritatea emitentă pentru să evite orice întârzieri suplimentare în cursul acestei proceduri.

Capitolul 4: Căi de atac

Articolele 15 și 16: Procedura de control jurisdicțional în cazul unor obligații contradictorii care rezultă din legea unei țări terțe

Articolele 15 și 16 prevăd o procedură de control jurisdicțional în cazul în care prestatorii de servicii cu sediul în țări terțe se confruntă cu obligații contradictorii. Aceste dispoziții sunt, de asemenea, foarte importante pentru asigurarea protecției drepturilor individuale și a curtoaziei internaționale. Prin stabilirea unui standard ridicat, acestea vizează să încurajeze țările terțe să ofere un nivel similar de protecție. În situația inversă, în care autoritățile unei țări terțe încearcă să obțină date cu privire la un cetățean al UE de la un prestator de servicii din UE, legislația Uniunii sau a statelor membre care protejează drepturile fundamentale, cum ar fi *acquis-ul* în materie de protecție a datelor, poate împiedica divulgarea în mod similar.

Uniunea Europeană se așteaptă ca țările terțe să respecte aceste interdicții astfel cum o face prezenta propunere.

Procedura prevăzută la articolul 15 poate fi declanșată de către destinatar în cazul în care respectarea unui ordin european de divulgare a probelor electronice ar duce la încălcarea uneia sau mai multor legi ale unei țări terțe care interzic divulgarea datelor în cauză pe motiv că acest lucru este necesar pentru protecția fie a drepturilor fundamentale ale persoanelor în cauză, fie a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională. Destinatarul are obligația de a informa autoritatea emitentă prin intermediul unei obiecții motivate cu privire la motivele pe care se bazează concluzia sa cu privire la existența unor obligații contradictorii. O astfel de obiecție motivată nu poate fi întemeiată pe faptul că nu există dispoziții similare în legislația țării terțe și nici pe circumstanța unică în care datele ar fi stocate într-o țară terță. Obiecția motivată se ridică în conformitate cu procedura prevăzută la articolul 9 alineatul (5) pentru notificarea intenției de a nu se conforma ordinului, utilizând formularul prevăzut în anexa III.

Pe baza acestei obiecții motivate, autoritatea emitentă își reexaminează ordinul. În cazul în care autoritatea emitentă alege să retragă ordinul, procedura se încheie. În cazul în care autoritatea emitentă ar dori să mențină ordinul, cazul este transferat către instanța competentă din statul său membru. Instanța evaluează apoi, pe baza obiecției motivate și luând în considerare toate elementele relevante ale cazului, dacă legea țării terțe se aplică în cazul respectiv și — în caz afirmativ — dacă există un conflict în cazul respectiv. Atunci când efectuează această evaluare, instanța ar trebui să ia în considerare dacă legea țării terțe, în loc să vizeze protejarea drepturilor fundamentale sau a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, 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.

În cazul în care instanța concluzionează că există într-adevăr un conflict cu obligațiile ce decurg din legile care protejează drepturile fundamentale ale persoanelor sau interesele fundamentale ale țării terțe legate de securitatea sau apărarea națională, aceasta trebuie să solicite un aviz din partea țării terțe relevante prin intermediul autorităților centrale naționale ale țării terțe. În cazul în care țara terță consultată confirmă existența unui conflict și obiectează față de executarea ordinului, instanța trebuie să retragă ordinul.

În cazul în care conflictul apare pe baza unei alte dispoziții legislative a țării terțe care nu vizează protejarea fie a drepturilor fundamentale ale persoanelor, fie a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, instanța adoptă decizia sa punând în balanță interesele în favoarea și împotriva menținerii ordinului.

Condițiile prevăzute la articolul 9, în special obligațiile de păstrare descrise la articolul 9 alineatul (6), se aplică, de asemenea, în situațiile în care există obligații contradictorii care derivă din legislația unei țări terțe. În cazul în care instanța ajunge la concluzia că ordinul trebuie menținut, autoritatea emitentă și prestatorul de servicii sunt informați în vederea executării acestuia. În cazul în care ordinul este revocat, poate fi emis un ordin european de păstrare a probelor electronice separat pentru a asigura disponibilitatea datelor în cazul în care acestea ar putea fi obținute prin intermediul unei cereri de asistență juridică reciprocă.

Având în vedere că ordinul european de păstrare a probelor electronice nu duce la divulgarea de date și, prin urmare, nu dă naștere unor preocupări similare, procedura de control jurisdicțional este limitată la ordinul european de divulgare a probelor electronice.

Articolul 17: Căi de atac eficiente

Această dispoziție asigură faptul că persoanele vizate de ordinul european de divulgare a probelor electronice dispun de căi de atac eficiente. Aceste căi de atac sunt exercitate în statul emitent, în conformitate cu legislația națională. În cazul persoanelor suspectate și acuzate, căile de atac sunt exercitate în mod normal în cursul procedurilor penale. Nu sunt puse la dispoziție căi de atac specifice pentru ordinul european de păstrare a probelor electronice, care nu permite în sine divulgarea datelor, decât în cazurile în care este urmat de un ordin european de divulgare a probelor electronice sau de un alt instrument care conduce la divulgare, caz în care sunt prevăzute căi de atac specifice.

Persoanele ale căror date au fost solicitate fără ca acestea să fie persoane suspectate sau acuzate în cadrul procedurilor penale au, de asemenea, dreptul la o cale de atac în statul emitent. Toate aceste drepturi nu aduc atingere niciunei căi de atac disponibile în temeiul Directivei privind protecția datelor în materie de asigurare a respectării legii și al RGPD.

Spre deosebire de ceea ce se prevede pentru prestatorii de servicii, regulamentul nu limitează motivele posibile pe care toate aceste persoane le pot prezenta pentru a contesta legalitatea ordinului. Printre aceste motive se numără necesitatea și proporționalitatea ordinului.

Exercitarea căilor de atac în statul emitent nu reprezintă o sarcină disproporționată pentru persoanele afectate. Ca și în cazul ordinelor executate prin intermediul altor forme de cooperare judiciară, instanțele din statul emitent sunt cel mai în măsură să examineze legalitatea ordinelor europene de divulgare a probelor electronice emise de propriile lor autorități și să evalueze compatibilitatea cu propria legislație națională. În plus, în cursul etapei de executare, destinatarii se pot opune în mod separat executării EPOC sau EPOC-PR în statul lor membru gazdă pe baza unei liste de motive enumerate în regulament (a se vedea articolul 14 de mai sus).

Articolul 18: Respectarea privilegiilor și a imunităților în temeiul legislației statului de primire

Această dispoziție urmărește același obiectiv ca și articolul 5 alineatul (7), și anume de a asigura luarea în considerare în statul emitent a imunităților și privilegiilor care protejează datele solicitate în statul membru al prestatorului de servicii, în special în cazul în care există diferențe între aceste state membre, precum și a intereselor fundamentale ale statului membru respectiv, cum ar fi securitatea și apărarea națională. Articolul 18 prevede că instanța din statul emitent trebuie să le ia în considerare ca și când ar fi fost prevăzute în dreptul său intern. Din cauza diferențelor dintre statele membre atunci când evaluează relevanța și admisibilitatea probelor, dispoziția lasă o anumită flexibilitate instanțelor cu privire la modalitatea de a lua în considerare aceste aspecte.

Capitolul 5: Dispoziții finale

Articolul 19: Monitorizarea și raportarea

Acest articol impune statelor membre obligația de a comunica informațiile specifice legate de aplicarea regulamentului cu scopul de a sprijini Comisia în exercitarea atribuțiilor sale în temeiul articolului 24. Comisia instituie un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament.

Articolul 20: Modificarea certificatelor și a formularelor

Certificatele și formularele prevăzute în anexele I, II și III la prezenta propunere vor facilita executarea unui EPOC și a unui EPOC-PR. Din acest motiv, este necesar ca în viitor să fie posibilă îmbunătățirea conținutului certificatului și a formularului cât mai rapid posibil, atunci când ar fi necesar acest lucru. Modificarea celor trei anexe prin intermediul procedurii legislative ordinare nu corespunde acestei cerințe, iar acestea constituie elemente neesențiale ale actelor legislative, elementele principale fiind definite la articolul 8. Prin urmare, articolul 20 prevede o procedură mai rapidă și mai flexibilă de modificare, prin acte delegate.

Articolul 21: Exercițarea delegării

Acest articol stabilește condițiile în care Comisia are competența de a adopta acte delegate pentru a se efectua eventualele modificări necesare ale certificatului și ale formularelor anexate la propunere. Acesta stabilește o procedură standard pentru adoptarea unor astfel de acte delegate.

Articolul 22: Notificări

Statele membre sunt obligate să notifice Comisiei care sunt autoritățile competente emitente și de executare și ce instanțe sunt competente să soluționeze obiecțiile motivate ale prestatorilor de servicii în cazul unui conflict de legi.

Articolul 23: Relația cu ordinele europene de anchetă

Această dispoziție clarifică faptul că regulamentul nu împiedică autoritățile din statul membru să emită ordine europene de anchetă în conformitate cu Directiva 2014/41/UE pentru a obține probe electronice.

Articolul 24: Evaluare

Această dispoziție precizează că Comisia realizează o evaluare a prezentului regulament în conformitate cu Orientările Comisiei privind o mai bună legiferare și în temeiul punctului 22 din Acordul interinstituțional din 13 aprilie 2016²⁵. Comisia va prezenta un raport Parlamentului European și Consiliului privind concluziile acestei evaluări, inclusiv o evaluare a necesității de a extinde domeniul său de aplicare la servicii care nu sunt încă reglementate, dar care ar putea deveni mai relevante pentru anchete, la 5 ani de la intrarea în vigoare a regulamentului propus.

Articolul 25: Intrarea în vigoare

Propunerea de regulament va intra în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene. Regulamentul se va aplica după 6 luni de la data intrării sale în vigoare.

²⁵ Acordul interinstituțional între Parlamentul European, Consiliul Uniunii Europene și Comisia Europeană privind o mai bună legiferare din 13 aprilie 2016; JO L 123, 12.5.2016, p. 1-14.

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI**privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală**

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamente naționale,

având în vedere avizul Comitetului Economic și Social European²⁶,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

- (1) Uniunea și-a stabilit obiectivul de a menține și de a dezvolta un spațiu de libertate, securitate și justiție. În vederea instituirii progresive a unui astfel de spațiu, Uniunea trebuie să adopte măsuri privind cooperarea judiciară în materie penală bazată pe principiul recunoașterii reciproce a hotărârilor judecătorești și a deciziilor judiciare, care este considerat, începând cu Consiliul European de la Tampere din 15-16 octombrie 1999, ca fiind piatra de temelie a cooperării judiciare în materie penală în cadrul Uniunii.
- (2) Măsurile care vizează obținerea și păstrarea probelor electronice sunt din ce în ce mai importante pentru a permite desfășurarea anchetelor penale și a urmărilor penale în întreaga Uniune. Mecanismele eficace de obținere a probelor electronice sunt esențiale pentru combaterea criminalității, sub rezerva unor condiții care să asigure deplina conformitate cu drepturile fundamentale și cu principiile recunoscute în Carta drepturilor fundamentale a Uniunii Europene, consacrate în tratate, în special principiile necesității și proporționalității, respectarea garanțiilor procedurale, protecția datelor, secretul corespondenței și viața privată.
- (3) Declarația comună a miniștrilor justiției și afacerilor interne și a reprezentanților instituțiilor UE cu privire la atentatele teroriste din 22 martie 2016 de la Bruxelles a subliniat necesitatea prioritară de a găsi modalități de obținere și păstrare mai rapide și mai eficiente a probelor electronice și de a identifica măsuri concrete de abordare a acestui aspect.
- (4) Concluziile Consiliului din 9 iunie 2016 au subliniat importanța tot mai mare a probelor electronice în cadrul procedurilor penale și a protejării spațiului cibernetic împotriva abuzurilor și a activităților infracționale în beneficiul economiilor și al societăților și, prin urmare, necesitatea ca autoritățile de aplicare a legii și cele

²⁶

JO C , , p. .

judiciare să dispună de instrumente eficace în vederea investigării și a urmăririi penale a infracțiunilor legate de spațiul cibernetic.

- (5) În comunicarea comună din 13 septembrie 2017 privind reziliența, prevenirea și apărarea²⁷, Comisia a subliniat că anchetarea și urmărirea penală eficace a infracțiunilor facilitate de calculator reprezintă un factor-cheie de descurajare a atacurilor cibernetice și că actualul cadru procedural trebuie să fie mai bine adaptat la era internetului. Procedurile actuale nu au putut ține pasul uneori cu rapiditatea atacurilor cibernetice, care conduc la o necesitate deosebită a unei cooperări transfrontaliere rapide.
- (6) Parlamentul European a reiterat aceste preocupări în rezoluția sa privind combaterea criminalității cibernetice din 3 octombrie 2017²⁸, evidențiind provocările pe care actualul cadrul juridic fragmentat le poate crea pentru prestatorii de servicii care doresc să respecte cererile de aplicare a legii și solicitând Comisiei să prezinte un cadru juridic al Uniunii privind probele electronice care să conțină garanții suficiente pentru drepturile și libertățile tuturor părților implicate.
- (7) Serviciile în rețea pot fi prestate de oriunde și nu necesită o infrastructură fizică, instalații sau personal în țara respectivă. Prin urmare, probele relevante sunt adesea stocate în afara statului care desfășoară investigarea sau de către un prestator de servicii stabilit în afara acestui stat. Adesea, nu există nicio altă legătură între cazul care face obiectul anchetei în statul respectiv și statul în care sunt stocate probele sau în care se află sediul principal al prestatorului de servicii.
- (8) Din cauza acestei lipse de legătură, cererile de cooperare judiciară sunt adesea adresate statelor care găzduiesc un număr mare de prestatori de servicii, dar care nu au nicio altă legătură cu cazul respectiv. În plus, numărul de cereri a crescut având în vedere utilizarea tot mai mare a serviciilor în rețea, care sunt fără frontiere prin natura lor. Prin urmare, obținerea de probe electronice prin intermediul canalelor de cooperare judiciară necesită adesea un timp îndelungat - mai îndelungat decât perioada în care ar putea rămâne disponibile eventualele indicii. De asemenea, nu există un cadru clar de cooperare cu prestatorii de servicii, deși anumiți prestatori din țări terțe acceptă cereri directe referitoare la date care nu se referă la conținut, în măsura în care acest lucru este permis de legislația lor națională aplicabilă. În consecință, toate statele membre se bazează pe canalul de cooperare cu prestatorii de servicii atunci când acesta este disponibil, utilizând diferite instrumente, condiții și proceduri naționale. În plus, pentru datele referitoare la conținut, unele state membre au luat măsuri unilaterale, în timp ce altele continuă să se bazeze pe cooperarea judiciară.
- (9) Cadrul juridic fragmentat creează provocări pentru prestatorii de servicii care doresc să respecte cererile de aplicare a legii. Prin urmare, este necesar să se instituie un cadru juridic european pentru probele electronice astfel încât prestatorii de servicii vizați de domeniul de aplicare al instrumentului să fie obligați să răspundă în mod direct autorităților fără implicarea unei autorități judiciare din statul membru al prestatorului de servicii.
- (10) Ordinele în temeiul prezentului regulament ar trebui să fie adresate reprezentanților legali ai prestatorilor de servicii desemnați în acest scop. În cazul în care un prestator de servicii stabilit în Uniune nu a desemnat un reprezentant legal, ordinele pot fi

²⁷ JOIN(2017) 450 final.

²⁸ 2017/2068(INI).

adresate oricărui sediu al prestatorului de servicii în Uniune. Această opțiune alternativă servește la asigurarea eficacității sistemului în cazul în care prestatorul de servicii nu a desemnat (încă) un reprezentant special.

- (11) Mecanismul privind ordinul european de divulgare și ordinul european de păstrare a probelor electronice în materie penală poate funcționa doar pe baza unui nivel înalt de încredere reciprocă între statele membre, care reprezintă o premisă esențială pentru funcționarea adecvată a acestui instrument.
- (12) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene. Printre acestea se numără dreptul la libertate și securitate, respectarea vieții private și de familie, protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare, principiile legalității și proporționalității, precum și dreptul de a nu fi judecat sau condamnat penal de două ori pentru aceeași infracțiune. În cazul în care statul membru emitent dispune de indicii conform cărora ar putea fi în curs proceduri penale paralele într-un alt stat membru, acesta consultă autoritățile statului membru respectiv în conformitate cu Decizia-cadru 2009/948/JAI a Consiliului²⁹.
- (13) Pentru a garanta respectarea deplină a drepturilor fundamentale, prezentul regulament se referă în mod explicit la standardele necesare în ceea ce privește obținerea oricăror date cu caracter personal, prelucrarea acestor date, controlul jurisdicțional al utilizării măsurii de investigare prevăzute de prezentul instrument și căile de atac disponibile.
- (14) Prezentul regulament ar trebui aplicat fără a aduce atingere drepturilor procesuale în procedurile penale prevăzute în Directivele 2010/64/UE³⁰, 2012/13/UE³¹, 2013/48/UE³², 2016/343³³, 2016/800³⁴ și 2016/1919³⁵ ale Parlamentului European și ale Consiliului.

²⁹ [Decizia-cadru 2009/948/JAI a Consiliului](#) din 30 noiembrie 2009 privind prevenirea și soluționarea conflictelor referitoare la exercitarea competenței în cadrul procedurilor penale (JO L 328, 15.12.2009, p. 42).

³⁰ [Directiva 2010/64/UE](#) a Parlamentului European și a Consiliului din 20 octombrie 2010 privind dreptul la interpretare și traducere în cadrul procedurilor penale (JO L 280, 26.10.2010, p. 1).

³¹ [Directiva 2012/13/UE](#) a Parlamentului European și a Consiliului din 22 mai 2012 privind dreptul la informare în cadrul procedurilor penale (JO L 142, 1.6.2012, p. 1).

³² [Directiva 2013/48/UE](#) a Parlamentului European și a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un avocat în cadrul procedurilor penale și al procedurilor privind mandatul european de arestare, precum și dreptul ca o persoană terță să fie informată în urma privării de libertate și dreptul de a comunica cu persoane terțe și cu autorități consulare în timpul privării de libertate (JO L 294, 6.11.2013, p. 1).

³³ [Directiva \(UE\) 2016/343](#) a Parlamentului European și a Consiliului din 9 martie 2016 privind consolidarea anumitor aspecte ale prezumției de nevinovăție și a dreptului de a fi prezent la proces în cadrul procedurilor penale (JO L 65, 11.3.2016, p. 1).

³⁴ [Directiva \(UE\) 2016/800](#) a Parlamentului European și a Consiliului din 11 mai 2016 privind garanțiile procedurale pentru copiii care sunt persoane suspectate sau acuzate în cadrul procedurilor penale (JO L 132, 21.5.2016, p. 1).

³⁵ [Directiva \(UE\) 2016/1919](#) a Parlamentului European și a Consiliului din 26 octombrie 2016 privind asistența juridică gratuită pentru persoanele suspectate și persoanele acuzate în cadrul procedurilor penale și pentru persoanele căutate în cadrul procedurilor privind mandatul european de arestare (JO L 297, 4.11.2016, p. 1).

- (15) Prezentul instrument stabilește normele în temeiul cărora o autoritate judiciară competentă a unui stat membru poate cere unui prestator de servicii care oferă servicii în Uniune să divulge sau să păstreze probe electronice, prin intermediul unui ordin european de divulgare sau de păstrare a probelor electronice. Prezentul regulament se aplică în toate cazurile în care prestatorul de servicii este stabilit sau reprezentat într-un alt stat membru. Pentru situațiile interne în care instrumentele prevăzute în prezentul regulament nu pot fi utilizate, regulamentul nu ar trebui să limiteze competențele autorităților naționale competente prevăzute de dreptul intern de a impune obligații prestatorilor de servicii stabiliți sau reprezentați pe teritoriul lor.
- (16) Prestatorii de servicii cei mai relevanți pentru procedurile penale sunt prestatorii de servicii de comunicații electronice și anumiți prestatori de servicii ale societății informaționale care facilitează interacțiunea dintre utilizatori. Prin urmare, ambele categorii ar trebui să fie reglementate de prezentul regulament. Prestatorii de servicii de comunicații electronice sunt definiți în Propunerea de directivă de instituire a Codului european al comunicațiilor electronice. Printre serviciile oferite de aceștia se numără comunicațiile interpersonale, cum ar fi telefonie VOIP, mesageria instantanee și serviciile de e-mail. Categoriile de servicii ale societății informaționale incluse aici sunt cele pentru care stocarea datelor este o componentă definitorie a serviciului furnizat utilizatorului și se referă în special la rețelele sociale, în măsura în care acestea nu se califică drept servicii de comunicații electronice, piețe online care facilitează tranzacțiile între utilizatorii lor (cum ar fi consumatori sau întreprinderi) sau alte servicii de găzduire, inclusiv în cazul în care serviciul este furnizat prin intermediul tehnologiei de tip cloud computing. Serviciile societății informaționale pentru care stocarea datelor nu este o componentă definitorie a serviciului furnizat utilizatorului și pentru care aceasta are doar o natură accesorie, cum ar fi serviciile juridice, de arhitectură, de inginerie și de contabilitate prestate online la distanță, ar trebui să fie excluse din domeniul de aplicare al prezentului regulament, chiar și atunci când s-ar putea încadra în definiția serviciilor societății informaționale în conformitate cu Directiva (UE) 2015/1535.
- (17) În multe cazuri, datele nu mai sunt stocate sau prelucrate într-un dispozitiv al utilizatorului, ci sunt puse la dispoziție în infrastructuri „cloud”, pentru a fi accesate de oriunde. Pentru a gestiona aceste servicii, prestatorii de servicii nu trebuie să fie stabilit sau să aibă servere într-o anumită jurisdicție. Prin urmare, aplicarea prezentului regulament nu ar trebui să depindă de localizarea efectivă a sediului prestatorului sau de unitatea de prelucrare sau de stocare a datelor.
- (18) Prestatorii de servicii de infrastructură de internet legate de alocarea de nume și numere, cum ar fi registrele de nume de domenii, operatorii de registre de nume de domenii și prestatorii de servicii de protecție a vieții private în sectorul comunicațiilor electronice și servicii de proxy sau registrele regionale de internet pentru adrese de protocol de internet („IP”), sunt deosebit de importanți pentru identificarea actorilor din spatele site-urilor web rău intenționate sau compromise. Aceștia dețin date care prezintă o relevanță deosebită pentru procedurile penale, întrucât pot permite identificarea unei persoane sau a unei entități din spatele unui site web utilizat în activități infracționale sau a victimei unei activități infracționale, în cazul unui site web compromis care a fost piratat către infractori.
- (19) Prezentul regulament reglementează doar colectarea de date stocate, și anume datele deținute de un prestator de servicii în momentul primirii unui certificat de ordin de divulgare sau de păstrare a probelor electronice. El nu stabilește o obligație generală de păstrare a datelor, și nici nu autorizează interceptarea datelor sau obținerea datelor

stocate la o dată ulterioară, după primirea unui certificat de ordin de divulgare sau de păstrare a probelor electronice. Datele ar trebui furnizate indiferent dacă sunt sau nu criptate.

- (20) Categoriile de date reglementate de prezentul regulament includ datele privind abonații, datele privind accesul, datele privind operațiile (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 prestatorilor de servicii să partajeze în mod voluntar datele care nu se referă la conținut cu autoritățile străine de aplicare a legii.
- (21) Este adecvat să se identifice datele privind accesul drept o categorie specifică de date utilizată în prezentul regulament. Datele privind accesul sunt solicitate pentru același obiectiv ca și datele privind abonații, cu alte cuvinte pentru a identifica utilizatorul subiacent, iar nivelul de interferență cu drepturile fundamentale este similar cu cel al datelor privind abonații. Datele privind accesul sunt de obicei înregistrate în cadrul unei înregistrări de evenimente (cu alte cuvinte, un log al serverului), pentru a indica începerea și încheierea unei sesiuni de acces a unui utilizator la un serviciu. Este adesea o adresă IP individuală (statică sau dinamică) sau un identificator pentru interfața de rețea utilizată în cursul sesiunii de acces. În cazul în care utilizatorul este necunoscut, este necesar adesea ca datele privind accesul să fie obținute înainte ca datele privind abonații referitoare la identificatorul respectiv să îi poată fi solicitate prestatorului de servicii.
- (22) Pe de altă parte, datele privind operațiile sunt solicitate în general pentru a obține informații referitoare la contactele utilizatorului și la locul în care se află acesta și pot fi utilizate pentru a stabili profilul unei persoane vizate. Acestea fiind spuse, datele privind accesul nu pot servi în sine la stabilirea unui scop similar, de exemplu nu dezvăluie nicio informație referitoare la interlocutorii aflați în legătură cu utilizatorul. Prin urmare, prezenta propunere introduce o nouă categorie de date, care trebuie să fie tratate în același mod ca și datele privind abonații, în cazul în care obiectivul obținerii acestor date este similar.
- (23) Toate categoriile de date conțin date cu caracter personal și, prin urmare, sunt acoperite de garanțiile acordate în temeiul acquis-ului Uniunii în materie de protecție a datelor, însă intensitatea impactului asupra drepturilor fundamentale variază, în special între datele privind abonații și datele privind accesul, pe de o parte, și între datele privind operațiile și datele referitoare la conținut, pe de altă parte. În timp ce datele privind abonații și datele privind accesul sunt utile pentru a obține primele indicii în cadrul unei anchete cu privire la identitatea unui suspect, datele privind operațiile și datele referitoare la conținut sunt cele mai relevante ca element probatoriu. Prin urmare, este esențial ca toate aceste categorii de date să fie reglementate de instrument. Din cauza gradului diferit de interferență cu drepturile fundamentale, sunt impuse condiții diferite pentru obținerea datelor privind abonații și a celor privind accesul, pe de o parte, și a datelor privind operațiile și a celor referitoare la conținut, pe de altă parte.
- (24) Ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice sunt măsuri de investigare care ar trebui să fie emise doar în cadrul unor proceduri penale specifice împotriva unor autori specifici, cunoscuți sau încă necunoscuți, ai unei infracțiuni concrete care a avut deja loc, în urma unei evaluări individuale a proporționalității și a necesității în fiecare caz în parte.

- (25) Prezentul regulament nu aduce atingere competențelor de investigare ale autorităților în cadrul procedurilor civile sau administrative, inclusiv atunci când astfel de proceduri pot duce la aplicarea unor sancțiuni.
- (26) Prezentul regulament ar trebui să se aplice prestatorilor de servicii care oferă servicii în Uniune, iar ordinele prevăzute în prezentul regulament pot fi emise doar pentru datele referitoare la serviciile oferite în Uniune. Serviciile oferite exclusiv în afara Uniunii nu intră în domeniul de aplicare al prezentului regulament, chiar dacă prestatorul de servicii este stabilit în Uniune.
- (27) Pentru a stabili dacă un prestator de servicii oferă sau nu servicii în Uniune, este necesară o evaluare din care să reiasă dacă prestatorul de servicii le permite unor persoane juridice sau fizice din unul sau mai multe state membre să utilizeze serviciile sale. Cu toate acestea, simpla accesibilitate a unei interfețe online, cum ar fi de exemplu accesibilitatea site-ului web al prestatorului de servicii sau al unui intermediar sau accesibilitatea unei adrese de e-mail și a altor date de contact în unul sau mai multe state membre, luate în considerare în mod separat, nu ar trebui să fie o condiție suficientă pentru aplicarea prezentului regulament.
- (28) O legătură substanțială cu Uniunea ar trebui, de asemenea, să fie relevantă pentru stabilirea sferei de aplicare a prezentului regulament. Ar trebui să se considere că există o astfel de legătură substanțială cu Uniunea în cazul în care prestatorul de servicii are un sediu în Uniune. În absența unui astfel de sediu, criteriul referitor la o legătură substanțială ar trebui să fie evaluat pe baza existenței unui număr semnificativ de utilizatori în unul sau mai multe state membre sau a orientării activităților către unul sau mai multe state membre. Orientarea activităților către unul sau mai multe state membre poate fi stabilită pe baza tuturor circumstanțelor relevante, inclusiv pe baza unor factori precum utilizarea unei limbi sau a unei monede folosite în general în statul membru respectiv sau posibilitatea de a comanda bunuri sau servicii. Orientarea activităților către un stat membru ar putea să reiasă, de asemenea, din disponibilitatea unei aplicații în magazinul de aplicații naționale relevante, din oferirea de publicitate locală sau de publicitate în limba folosită în statul membru respectiv sau din gestionarea relațiilor cu clienții, de exemplu prin furnizarea de servicii pentru clienți în limba folosită în general în statul membru respectiv. De asemenea, trebuie să se presupună existența unei legături substanțiale atunci când un prestator de servicii își direcționează activitățile spre unul sau mai multe state membre, astfel cum se prevede la articolul 17 alineatul (1) litera (c) din Regulamentul nr. 1215/2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială³⁶. Pe de altă parte, prestarea serviciului în vederea simplei respectări a interdicției de discriminare prevăzute în Regulamentul (UE) 2018/302³⁷ nu poate fi considerată, exclusiv pe baza acestui motiv, drept direcționare sau orientare a activităților către un anumit teritoriu din cadrul Uniunii.
- (29) Un ordin european de divulgare a probelor electronice ar trebui să fie emis doar în cazul în care acest lucru este necesar și proporțional. Evaluarea ar trebui să ia în

³⁶ [Regulamentul \(UE\) nr. 1215/2012](#) al Parlamentului European și al Consiliului din 12 decembrie 2012 privind competența judiciară, recunoașterea și executarea hotărârilor în materie civilă și comercială (JO L 351, 20.12.2012, p. 1).

³⁷ [Regulamentul \(UE\) 2018/302](#) al Parlamentului European și al Consiliului din 28 februarie 2018 privind prevenirea geoblocării nejustificate și a altor forme de discriminare bazate pe cetățenia sau naționalitatea, domiciliul sau sediul clienților pe piața internă și de modificare a Regulamentelor (CE) nr. 2006/2004 și (UE) 2017/2394, precum și a Directivei 2009/22/CE (JO L 601, 2.3.2018, p. 1).

considerare dacă ordinul se limitează la ceea ce este necesar pentru a atinge obiectivul legitim de obținere a datelor relevante și necesare care să servească drept probe doar în cazul respectiv.

- (30) Atunci când este emis un ordin european de divulgare sau de păstrare a probelor electronice, ar trebui să intervină întotdeauna o autoritate judiciară fie în procesul de emitere, fie în cel de validare a ordinului. Având în vedere caracterul mai sensibil al datelor privind operațiile și al celor referitoare la conținut, emiterea sau validarea ordinelor europene de divulgare pentru aceste categorii de date necesită un control jurisdicțional din partea unui judecător. În plus, întrucât datele privind abonații și cele privind accesul sunt mai puțin sensibile, ordinele europene de divulgare pentru aceste categorii de date pot fi emise sau validate de către procurori competenți.
- (31) Din același motiv, trebuie să se facă o distincție în ceea ce privește domeniul de aplicare material al prezentului regulament: ordinele de divulgare a datelor privind abonații și a celor privind accesul pot fi emise pentru orice infracțiune, în timp ce datele privind operațiile și cele referitoare la conținut ar trebui să facă obiectul unor cerințe mai stricte pentru a reflecta natura mai sensibilă a acestor date. Existența unui prag permite o abordare mai proporțională, împreună cu o serie de alte condiții și garanții *ex ante* și *ex post* prevăzute în propunere pentru a asigura respectarea proporționalității și a drepturilor persoanelor afectate. În același timp, pragul nu ar trebui să limiteze eficacitatea instrumentului și utilizarea sa de către practicieni. Faptul de a permite ca ordinele să fie emise pentru anchete legate de infracțiuni pentru care se prevede o limită superioară a pedepsei de cel puțin trei ani limitează domeniul de aplicare a instrumentului la infracțiuni mai grave, fără a afecta excesiv posibilitățile sale de utilizare de către practicieni. Sunt excluse astfel din domeniul de aplicare un număr semnificativ de infracțiuni care sunt considerate mai puțin grave de către statele membre, astfel cum reiese din aplicarea unei limite superioare a pedepsei mai reduse. De asemenea, această abordare are avantajul de a fi ușor de aplicat în practică.
- (32) Pentru anumite infracțiuni, probele sunt în mod normal disponibile exclusiv în format electronic, care este deosebit de fluid prin natura sa. Acest lucru este valabil pentru infracțiunile conexe mediului informatic, chiar și pentru cele care ar putea să nu fie considerate grave în sine, dar care pot provoca pagube extinse sau considerabile, inclusiv, în special, cazurile cu impact individual redus, dar cu volum ridicat și prejudiciu global. Pentru majoritatea cazurilor în care infracțiunea a fost săvârșită prin intermediul unui sistem informatic, aplicarea aceluiași prag ca și în cazul altor tipuri de infracțiuni ar conduce cel mai frecvent la impunitate. Acest lucru justifică aplicarea regulamentului și în cazul infracțiunilor pentru care limita pedepsei este inferioară pragului de 3 ani de închisoare. Infracțiunile legate de terorism, astfel cum sunt descrise în Directiva 2017/541/UE, nu necesită pragul maxim de minimum 3 ani.
- (33) În plus, este necesar să se prevadă că ordinul european de divulgare a probelor electronice nu poate fi emis decât dacă un ordin similar ar fi disponibil pentru aceeași infracțiune într-o situație internă comparabilă în statul emitent.
- (34) În cazurile în care datele solicitate sunt stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei societăți sau unei alte entități, care nu este persoană fizică, cel mai frecvent în cazul serviciilor de găzduire, ordinul european de divulgare a probelor electronice ar trebui utilizat doar atunci când măsurile de investigare adresate societății sau entității nu sunt adecvate, în special întrucât ar risca să periclitizeze ancheta. Acest aspect este relevant în special în ceea ce privește entitățile mai mari, cum ar fi organismele de drept public sau entitățile

guvernamentale, care recurg la serviciile prestatorilor de servicii pentru a furniza infrastructura sau serviciile lor IT corporative sau ambele. În astfel de situații, primul destinatar al unui ordin european de divulgare a probelor electronice ar trebui să fie societatea sau o altă entitate. Această societate sau altă entitate poate să nu fie un prestator de servicii care intră sub incidența prezentului regulament. Cu toate acestea, în cazurile în care nu este oportun ca ordinul să fie adresat entității respective, deoarece este suspectată de implicare în cauza respectivă sau există indicii referitoare la coluziunea cu obiectivul anchetei, autoritățile competente ar trebui să fie în măsură să se adreseze prestatorului de servicii care furnizează infrastructura în cauză pentru divulgarea datelor solicitate. Această dispoziție nu aduce atingere dreptului de a-i impune prestatorului de servicii să păstreze datele.

- (35) Imunitățile și privilegiile, care se pot referi la categorii de persoane (cum ar fi diplomații) sau la relații protejate în mod specific (cum ar fi privilegiul juridic profesional), sunt menționate în alte instrumente de recunoaștere reciprocă, cum ar fi ordinul european de anchetă. Sfera lor de aplicare și impactul lor diferă în funcție de dreptul național aplicabil care ar trebui luat în considerare la momentul emiterii ordinului, întrucât autoritatea emitentă poate să emită ordinul doar dacă un ordin similar ar fi disponibil într-o situație internă comparabilă. Pe lângă acest principiu de bază, imunitățile și privilegiile care protejează datele privind accesul, datele privind operațiile sau datele referitoare la conținut în statul membru al prestatorului de servicii ar trebui luate în considerare în măsura posibilului în statul emitent în același mod ca și când ar fi fost prevăzute în legislația națională al statului emitent. Acest lucru este relevant în special în cazul în care legislația statului membru în care prestatorul de servicii sau reprezentantul său legal primește ordinul prevede un grad mai mare de protecție decât legislația statului emitent. De asemenea, dispoziția asigură respectarea în cazurile în care divulgarea datelor ar putea afecta interesele fundamentale ale statului membru respectiv, cum ar fi securitatea și apărarea națională. Ca o garanție suplimentară, aceste aspecte ar trebui să fie luate în considerare nu doar atunci când este emis ordinul, ci și mai târziu, când se evaluează relevanța și la admisibilitatea datelor în cauză în etapa corespunzătoare a procedurii penale și în cazul în care are loc o procedură de executare, efectuată de autoritatea de executare.
- (36) Ordinul european de păstrare a probelor electronice poate fi emis pentru orice infracțiune. Obiectivul său este de a împiedica eliminarea, ștergerea sau modificarea datelor în situațiile în care poate dura mai mult timp obținerea divulgării acestor date, de exemplu întrucât vor fi utilizate canale de cooperare judiciară.
- (37) Ordinele europene de divulgare și de păstrare a probelor electronice ar trebui să se adreseze reprezentantului legal desemnat de către prestatorul de servicii. În absența unui reprezentant legal desemnat, ordinele pot fi adresate oricărui sediu al prestatorului de servicii în Uniune. Acesta poate fi cazul atunci când nu există nicio obligație juridică pentru furnizorul de servicii de a desemna un reprezentant legal. În cazul nerespectării ordinului de către reprezentantul legal, în situații de urgență, ordinul european de divulgare sau de păstrare a probelor electronice poate fi adresat și prestatorului de servicii în paralel cu continuarea executării ordinului inițial sau în locul acestei executări, în conformitate cu articolul 14. În cazul nerespectării ordinului de către reprezentantul legal, în alte situații decât cele de urgență, dar când există în mod evident riscul de pierdere a datelor, ordinul european de divulgare sau de păstrare a probelor electronice poate fi adresat, de asemenea, oricărui sediu al prestatorului de servicii în Uniune. Din cauza acestor diferite scenarii posibile, se utilizează termenul general „destinatar” în cadrul dispozițiilor. În cazul în care o obligație, cum ar fi cea

referitoare la confidențialitate, se aplică nu doar destinatarului, ci și prestatorului de servicii în cazul în care acesta nu este destinatarul, acest lucru este menționat în dispoziția respectivă.

- (38) Ordinele europene de divulgare și de păstrare a probelor electronice ar trebui transmise prestatorului de servicii prin intermediul unui certificat de ordin european de divulgare a probelor electronice (EPOC) sau al unui certificat de ordin european de păstrare a probelor electronice (EPOC-PR), care ar trebui traduse. Certificatele ar trebui să conțină aceleași informații obligatorii ca și ordinele, cu excepția motivelor pentru necesitatea și proporționalitatea măsurii sau a unor detalii suplimentare cu privire la caz pentru a evita punerea în pericol a anchetelor. Însă, întrucât fac parte din ordin ca atare, acestea îi permit persoanei suspectate să îl conteste ulterior în cursul procedurilor penale. Atunci când este necesar, un certificat trebuie să fie tradus în (una dintre) limba (limbile) oficială (oficiale) a (ale) statului membru al destinatarului sau într-o altă limbă oficială pe care prestatorul a declarat că o va accepta.
- (39) Autoritatea emitentă competentă ar trebui să transmită EPOC sau EPOC-PR direct destinatarului prin orice mijloace care permit o înregistrare scrisă, în condiții care să îi permită prestatorului de servicii să stabilească autenticitatea acestuia, cum ar fi prin scrisoare recomandată, e-mail și platforme securizate sau alte canale securizate, inclusiv cele puse la dispoziție de către prestatorul de servicii, în conformitate cu normele de protecție a datelor cu caracter personal.
- (40) Datele solicitate ar trebui să fie transmise autorităților cel târziu în termen de 10 zile de la primirea EPOC. Prestatorul ar trebui să respecte termene mai scurte în cazuri de urgență și în cazul în care autoritatea emitentă indică alte motive pentru neaplicarea termenului-limită de 10 zile. Pe lângă pericolul iminent de ștergere a datelor solicitate, astfel de motive ar putea include circumstanțe legate de o anchetă în curs, de exemplu în cazul în care datele solicitate sunt asociate altor măsuri de investigare urgente care nu pot fi puse în aplicare fără datele care lipsesc sau care sunt dependente în alt mod de acestea.
- (41) Pentru a permite prestatorilor de servicii să facă față unor probleme formale, este necesar să se instituie o procedură pentru comunicarea dintre prestatorul de servicii și autoritatea judiciară emitentă în cazurile în care EPOC ar putea fi incomplet, conține erori vădite sau nu conține informații suficiente pentru a executa ordinul. În plus, în cazul în care prestatorul de servicii nu oferă informațiile în mod exhaustiv sau la timp din orice alt motiv, de exemplu întrucât consideră că există un conflict cu o obligație în temeiul legislației unei țări terțe sau întrucât consideră că ordinul european de divulgare a probelor electronice nu a fost emis în conformitate cu condițiile prevăzute în prezentul regulament, acesta ar trebui să se adreseze autorităților emitente și să ofere justificările adecvate. Prin urmare, procedura de comunicare ar trebui să permită, în mare, corectarea sau reconsiderarea EPOC de către autoritatea emitentă într-un stadiu incipient. Pentru a garanta disponibilitatea datelor, prestatorul de servicii ar trebui să păstreze datele în cazul în care poate identifica datele solicitate.
- (42) Atunci când primește un certificat de ordin european de păstrare a probelor electronice („EPOC-PR”), prestatorul de servicii ar trebui să păstreze datele solicitate pentru o perioadă maximă de 60 de zile, cu excepția cazului în care autoritatea emitentă îl informează pe prestatorul de servicii că a demarat procedura de emitere a unei solicitări ulterioare de divulgare, caz în care datele ar trebui păstrate în continuare. Perioada de 60 de zile este calculată pentru a permite transmiterea unei cereri oficiale. Acest lucru presupune că au fost adoptate cel puțin unele măsuri oficiale, de exemplu,

trimiterea unei cereri de asistență juridică reciprocă pentru a fi tradusă. În urma primirii acestor informații, datele ar trebui să fie păstrate atât timp cât este necesar până în momentul în care datele sunt divulgate în cadrul unei cereri ulterioare de divulgare.

- (43) Prestatorii de servicii și reprezentanții lor legali ar trebui să asigure confidențialitatea și, atunci când li se solicită acest lucru de către autoritatea emitentă, să se abțină de la a informa persoana ale cărei date sunt solicitate pentru a proteja anchetarea infracțiunilor, în conformitate cu articolul 23 din Regulamentul (UE) 2016/679³⁸. Cu toate acestea, informațiile adresate utilizatorului reprezintă un element esențial pentru a permite efectuarea unui control jurisdicțional și introducerea de căi de atac judiciare și ar trebui furnizate de către autoritate în cazul în care prestatorului de servicii i s-a solicitat să nu informeze utilizatorul, în cazul în care nu există niciun risc de a se pune în pericol anchetele în curs, în conformitate cu măsurile naționale de transpunere a articolului 13 din Directiva (UE) 2016/680³⁹.
- (44) În cazul nerespectării ordinului de către destinatar, autoritatea emitentă poate transmite ordinul complet, inclusiv motivele privind necesitatea și proporționalitatea, însoțit de certificat, autorității competente din statul membru în care își are reședința sau sediul destinatarul certificatului. Acest stat membru ar trebui să îl execute în conformitate cu legislația sa națională. Statele membre ar trebui să prevadă impunerea unor sancțiuni pecuniare eficace, proporționale și disuasive în cazul încălcării obligațiilor stabilite în prezentul regulament.
- (45) Procedura de executare este o procedură prin care destinatarul se poate opune executării pe baza anumitor motive limitate. Autoritatea de executare poate refuza să recunoască și să execute ordinul pe baza aceluiași motive sau în cazul în care se aplică privilegii și imunități în temeiul legislației sale naționale sau divulgarea ar putea afecta interesele sale fundamentale, cum ar fi securitatea și apărarea națională. Autoritatea de executare ar trebui să se consulte autoritatea emitentă înainte de a refuza să recunoască sau să execute ordinul, pe baza acestor motive. În cazul nerespectării ordinului, autoritățile pot impune sancțiuni. Aceste sancțiuni ar trebui să fie proporționale ținând seama, de asemenea, de circumstanțe specifice cum ar fi nerespectarea repetată sau sistematică a ordinelor.
- (46) Fără a aduce atingere obligațiilor lor în materie de protecție a datelor, prestatorii de servicii nu ar trebui să fie considerați răspunzători în statele membre pentru prejudicii aduse utilizatorilor lor sau unor terți care rezultă exclusiv din respectarea cu bună-credință a unui EPOC sau a unui EPOC-PR.
- (47) Pe lângă persoanele ale căror date sunt solicitate, prestatorii de servicii și țările terțe pot fi afectate, la rândul lor, de măsura de investigare. Pentru a garanta respectarea intereselor suverane ale țărilor terțe, pentru a proteja persoanele în cauză și pentru a face față eventualelor obligațiilor contradictorii care le revin prestatorilor de servicii,

³⁸ [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) (JO L 119, 4.5.2016, p. 1).

³⁹ [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 (JO L 119, 4.5.2016, p. 89).

prezentul instrument prevede un mecanism specific de control jurisdicțional în cazul în care respectarea unui ordin european de divulgare a probelor electronice ar împiedica prestatorii de servicii să respecte o obligație legală ce rezultă din legislația unui stat terț.

- (48) În acest scop, ori de câte ori destinatarul consideră că ordinul european de divulgare a probelor electronice în cazul în speță ar duce la încălcarea unei obligații legale care decurge din legislația unei țări terțe, acesta ar trebui să informeze autoritatea emitentă prin intermediul unei obiecții motivate, utilizând formularele prevăzute. În acest caz, autoritatea emitentă ar trebui să reexamineze ordinul european de divulgare a probelor electronice ținând seama de obiecția motivată, luând în considerare aceleași criterii pe care ar trebui să le aibă în vedere instanța competentă. În cazul în care autoritatea decide să mențină ordinul, procedura ar trebui să fie înaintată instanței competente, astfel cum a fost notificată de către statul membru în cauză, care supune apoi ordinul controlului jurisdicțional.
- (49) În vederea stabilirii existenței unei obligații contradictorii în circumstanțele specifice ale cazului care face obiectul examinării, instanța competentă ar trebui să se bazeze, dacă este necesar, pe o expertiză externă adecvată, de exemplu în cazul în care controlul jurisdicțional ridică probleme de interpretare a legislației din țara terță în cauză. Acest demers ar putea include consultarea autorităților centrale din țara respectivă.
- (50) Expertiza în materie de interpretare ar putea fi furnizată, de asemenea, prin intermediul unor avize ale experților, în cazul în care acestea sunt disponibile. Informațiile și jurisprudența privind interpretarea legislației țărilor terțe și privind procedurile în materie de conflicte în statele membre ar trebui să fie puse la dispoziție pe o platformă centrală, cum ar fi proiectul SIRIUS și/sau Rețeaua Judiciară Europeană. Instanțele ar putea astfel să beneficieze de experiența și de expertiza acumulată de alte instanțe cu privire la aceleași aspecte sau la aspecte similare. Aceasta nu ar trebui să împiedice o nouă consultare a țării terțe, dacă este cazul.
- (51) În cazul în care există obligații contradictorii, instanța ar trebui să stabilească dacă dispozițiile contradictorii ale țării terțe interzic divulgarea datelor în cauză pe motiv că acest lucru este necesar pentru protecția fie a drepturilor fundamentale ale persoanelor în cauză, fie a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională. Atunci când efectuează această evaluare, instanța ar trebui să ia în considerare dacă legislația țării terțe, în loc să vizeze protejarea drepturilor fundamentale sau a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, 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. În cazul în care instanța concluzionează că dispozițiile contradictorii ale țării terțe interzic divulgarea datelor în cauză pe motiv că acest lucru este necesar pentru protecția fie a drepturilor fundamentale ale persoanelor în cauză, fie a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, aceasta ar trebui să consulte țara terță prin intermediul autorităților sale centrale, care sunt deja prezente în scopul asistenței juridice reciproce în cea mai mare parte a lumii. Aceasta ar trebui să stabilească un termen-limită până la care țara terță poate ridica obiecții cu privire la executarea ordinului european de divulgare a probelor electronice; în cazul în care autoritățile țării terțe nu răspund în termenul stabilit (sau prelungit), în ciuda unui mesaj de atenționare prin care sunt informate cu privire la consecințele lipsei unui răspuns din partea lor, instanța menține ordinul.

În cazul în care autoritățile țării terțe se opun divulgării, instanța ar trebui să revoce ordinul.

- (52) În toate celelalte cazuri de obligații contradictorii, care nu sunt legate de drepturile fundamentale ale persoanelor sau de interesele fundamentale ale țării terțe legate de securitatea sau apărarea națională, instanța ar trebui să adopte decizia cu privire la menținerea sau nu a ordinului european de divulgare a probelor electronice luând în considerare o serie de elemente care urmăresc să se stabilească soliditatea legăturii cu una dintre cele două jurisdicții implicate, interesele privind obținerea, respectiv împiedicarea divulgării datelor și posibilele consecințe pentru prestatorul de servicii ale obligației de se conforma ordinului. Un aspect important pentru infracțiunile conexe mediului informatic, locul în care a fost săvârșită infracțiunea se referă atât la locul (locurile) în care a fost întreprinsă acțiunea, cât și la locul (locurile) în care s-au materializat efectele infracțiunii.
- (53) Condițiile prevăzute la articolul 9 se aplică, de asemenea, în cazul unor obligații contradictorii care derivă din legislația unei țări terțe. În cursul acestei proceduri, datele ar trebui să fie păstrate. În cazul în care ordinul este revocat, poate fi emis un nou ordin de păstrare pentru a permite autorității emitente să solicite divulgarea datelor prin intermediul altor canale, cum ar fi asistența juridică reciprocă.
- (54) Este esențial ca toate persoanele ale căror date sunt solicitate în cursul anchetelor sau al procedurilor penale să aibă acces la o cale de atac eficientă, în conformitate cu articolul 47 din Carta drepturilor fundamentale a Uniunii Europene. În cazul persoanelor suspectate și acuzate, dreptul la o cale de atac eficientă ar trebui exercitat în cursul procedurilor penale. Acest lucru poate afecta admisibilitatea sau, după caz, importanța în cadrul procedurilor, a probelor obținute prin aceste mijloace. În plus, acestea beneficiază de toate garanțiile procedurale care le sunt aplicabile, cum ar fi dreptul la informare. Alte persoane, care nu sunt persoane suspectate sau acuzate, ar trebui să beneficieze, de asemenea, de dreptul la o cale de atac eficientă. Prin urmare, ar trebui prevăzută cel puțin posibilitatea de a contesta legalitatea unui ordin european de divulgare a probelor electronice, inclusiv necesitatea și proporționalitatea ordinului. Prezentul regulament nu ar trebui să limiteze motivele pentru contestarea legalității ordinului. Aceste căi de atac ar trebui exercitate în statul emitent, în conformitate cu legislația națională. Normele privind măsurile provizorii ar trebui să fie reglementate de legislația națională.
- (55) În plus, în cursul procedurii de executare și al exercitării căii de atac ulterioare, destinatarul poate să se opună executării unui ordin european de divulgare sau de păstrare a probelor electronice pentru un număr limitat de motive, inclusiv faptul că acesta nu a fost emis sau validat de o autoritate competentă sau faptul că acesta încalcă în mod vădit Carta drepturilor fundamentale a Uniunii Europene sau că este în mod vădit abuziv. De exemplu, un ordin care solicită divulgarea de date referitoare la conținut privind o categorie nedefinită de persoane dintr-o zonă geografică sau care nu are nicio legătură cu procedura penală efectivă ar ignora în mod evident condițiile pentru emiterea unui ordin european de divulgare a probelor electronice.
- (56) Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. În conformitate cu articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene și cu articolul 16 alineatul (1) din TFUE, orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. Atunci când pun în aplicare prezentul regulament, statele membre ar trebui să

asigure faptul că datele cu caracter personal sunt protejate și că pot fi prelucrate numai în conformitate cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/680.

- (57) Datele cu caracter personal obținute în temeiul prezentului regulament ar trebui prelucrate numai când acest lucru este necesar și proporțional în scopul prevenirii, anchetării, depistării sau urmăririi penale a infracțiunilor sau al aplicării sancțiunilor penale și al exercitării dreptului la apărare. În special, statele membre ar trebui să se asigure că se aplică politici adecvate de protecție a datelor în cazul transmiterii de date cu caracter personal din partea autorităților relevante către prestatorii de servicii în sensul prezentului regulament, inclusiv măsuri pentru a garanta securitatea datelor. Prestatorii de servicii ar trebui să asigure aceleași condiții pentru transmiterea de date cu caracter personal către autoritățile relevante. Numai persoanele autorizate ar trebui să aibă acces la informații care conțin date cu caracter personal, care poate fi obținut prin proceduri de autentificare. Ar trebui să fie luată în considerare utilizarea unor mecanisme de asigurare a autenticității, cum ar fi sistemele naționale de identificare electronică notificate sau serviciile de încredere, astfel cum sunt prevăzute în Regulamentul (UE) 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.
- (58) Comisia ar trebui să efectueze o evaluare a prezentului regulament care ar trebui să se bazeze pe cele cinci criterii, și anume eficiența, eficacitatea, relevanța, coerența și valoarea adăugată europeană și ar trebui să servească drept bază pentru evaluările impactului unor eventuale măsuri suplimentare. Ar trebui să fie colectate în mod regulat informații, pentru a servi la evaluarea prezentului regulament.
- (59) Utilizarea de formulare pretraduse și standardizate facilitează cooperarea și schimbul de informații dintre autoritățile judiciare și prestatorii de servicii, permițându-le să obțină și să transmită probe electronice mai rapid și mai eficient, îndeplinind în același timp cerințele necesare în materie de securitate într-un mod ușor de utilizat. Acestea reduc costurile de traducere și contribuie la un nivel ridicat de calitate. În mod similar, formularele de răspuns ar trebui să permită un schimb standardizat de informații, în special în cazul în care prestatorii de servicii nu sunt în măsură să se conformeze, întrucât contul respectiv nu există sau datele nu sunt disponibile. De asemenea, formularele ar trebui să faciliteze colectarea de statistici.
- (60) Pentru a răspunde în mod eficace unei posibile necesități de îmbunătățire în ceea ce privește conținutul și EPOC și EPOC-PR și al formularului care trebuie folosit pentru a furniza informații cu privire la imposibilitatea de a executa EPOC sau EPOC-PR, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui delegată Comisiei, în vederea modificării anexelor I, II și III la prezentul regulament. Este deosebit de important ca, în cadrul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare⁴⁰. În special, pentru a se asigura o participare egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

⁴⁰

JO L 123, 12.5.2016, p. 1.

- (61) Măsurile bazate pe prezentul regulament nu ar trebui să înlocuiască ordinele europene de anchetă în conformitate cu Directiva 2014/41/UE a Parlamentului European și a Consiliului⁴¹ în vederea obținerii de probe electronice. Autoritățile statelor membre ar trebui să aleagă instrumentul cel mai adaptat situației lor; acestea ar putea prefera să utilizeze ordinul european de anchetă atunci când solicită o serie de diferite tipuri de măsuri de investigare, inclusiv divulgarea de probe electronice din partea unui alt stat membru, fără însă a se limita la aceasta.
- (62) Din cauza evoluțiilor tehnologice, în câțiva ani ar putea prevala noi forme de instrumente de comunicare sau ar putea apărea lacune în ceea ce privește aplicarea prezentului regulament. Prin urmare, este important să se prevadă o reexaminare a aplicării sale.
- (63) Întrucât obiectivul prezentului regulament, și anume îmbunătățirea obținerii de probe electronice la nivel transfrontalier, nu poate fi realizat în mod satisfăcător de către statele membre, având în vedere natura sa transfrontalieră, însă poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri în conformitate cu principiul subsidiarității prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul menționat, prezentul regulament nu depășește ceea ce este necesar pentru îndeplinirea respectivelor obiective.
- (64) În conformitate cu articolul 3 din Protocolul privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, *[Regatul Unit/Irlanda și-a notificat dorința de a participa la adoptarea și aplicarea prezentului regulament] sau [fără a aduce atingere articolului 4 din protocol, Regatul Unit/Irlanda nu participă la adoptarea prezentului regulament și, prin urmare, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale]*.
- (65) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentului regulament și, prin urmare, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.
- (66) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului⁴² și a emis un aviz la data de (...) ⁴³,

⁴¹ [Directiva 2014/41/UE](#) din 3 aprilie 2014 privind ordinul european de anchetă în materie penală (JO L 130, 1.5.2014, p.1).

⁴² Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

⁴³ JO C , , p. .

Capitolul 1: Obiect, definiții și domeniu de aplicare

Articolul 1

Obiect

- (1) Prezentul regulament stabilește normele în temeiul cărora o autoritate a unui stat membru poate cere unui prestator de servicii care oferă servicii în Uniune să divulge sau să păstreze probe electronice, indiferent de locul în care se află datele. Prezentul regulament nu aduce atingere competențelor autorităților naționale de a obliga prestatorii de servicii stabiliți sau reprezentați pe teritoriul lor să se conformeze unor măsuri naționale similare.
- (2) Prezentul regulament nu are ca efect modificarea obligației de respectare a drepturilor fundamentale și a principiilor juridice astfel cum sunt consacrate la articolul 6 din TUE, inclusiv dreptul la apărare al persoanelor care fac obiectul unor proceduri penale, și nu aduce atingere obligațiilor care le revin autorităților de aplicare a legii sau autorităților judiciare în această privință.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

- (1) „ordin european de divulgare a probelor electronice” înseamnă o decizie cu caracter obligatoriu emisă de o autoritate emitentă dintr-un stat membru prin care un prestator de servicii ce oferă servicii în Uniune și este stabilit sau reprezentat într-un alt stat membru este obligat să divulge probe electronice;
- (2) „ordin european de păstrare a probelor electronice” înseamnă o decizie cu caracter obligatoriu emisă de o autoritate emitentă dintr-un stat membru prin care un prestator de servicii ce oferă servicii în Uniune și este stabilit sau reprezentat într-un alt stat membru este obligat să păstreze probe electronice, în vederea unei cereri ulterioare de divulgare;
- (3) „prestator de servicii” înseamnă orice persoană fizică sau juridică care prestează una sau mai multe dintre următoarele categorii de servicii:
 - (a) servicii de comunicații electronice, astfel cum sunt definite la articolul 2 alineatul (4) din [Directiva de instituire a Codului european al comunicațiilor electronice];
 - (b) servicii ale societății informaționale, astfel cum sunt definite la articolul 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului⁴⁴, pentru care stocarea datelor este o componentă esențială a serviciului furnizat utilizatorului, inclusiv rețelele de socializare, piețele online

⁴⁴ [Directiva \(UE\) 2015/1535](#) a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

care facilitează tranzacțiile între utilizatorii lor și alți furnizori de servicii de găzduire;

- (c) servicii legate de numele de domenii de internet și de numerotarea IP, cum ar fi furnizorii de adrese IP, registrele de nume de domenii, operatorii de registre de nume de domenii și serviciile conexe de protecție a vieții private în sectorul comunicațiilor electronice și servicii de proxy;
- (4) „oferirea de servicii în Uniune” înseamnă:
 - (a) a permite persoanelor juridice sau fizice din unul sau mai multe state membre să utilizeze serviciile enumerate la punctul 3 de mai sus; și
 - (b) a avea o legătură substanțială cu statul (statele) membru (membre) menționat(e) la litera (a);
- (5) „sediul” înseamnă 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;
- (6) „probe electronice” înseamnă probe stocate în format electronic de către un prestator de servicii sau în numele unui prestator de servicii în momentul primirii unui certificat de ordin de divulgare sau de păstrare a probelor electronice, constând în date stocate privind abonații, date privind accesul, date privind operațiile și date referitoare la conținut;
- (7) „date privind abonații” înseamnă orice date cu privire la:
 - (a) identitatea unui abonat sau client, cum ar fi numele furnizat, data nașterii, adresa poștală sau adresa geografică, datele privind facturarea și plata, telefon sau e-mail;
 - (b) tipul de serviciu și durata sa, inclusiv datele tehnice și datele de identificare a măsurilor tehnice conexe sau a interfețelor utilizate de către abonat sau client sau furnizate abonatului sau clientului, precum și date privind validarea utilizării serviciului, cu excepția parolei sau a altor mijloace de autentificare utilizate în locul unei parole care sunt furnizate de către un utilizator sau create la cererea unui utilizator;
- (8) „date privind accesul” înseamnă datele legate de începerea sau terminarea sesiunii de acces a unui utilizator la un serviciu, care sunt strict necesare exclusiv în scopul identificării utilizatorului serviciului, cum ar fi data și ora utilizării sau conectarea la serviciu și deconectarea, împreună cu adresa IP alocată de furnizorul de servicii de acces la internet utilizatorului unui serviciu, datele de identificare a interfeței utilizate și numele de utilizator. Acestea includ metadatele privind comunicațiile electronice, astfel cum sunt definite la articolul 4 alineatul (3) litera (g) din [Regulamentul privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice];
- (9) „date privind operațiile” înseamnă date legate de furnizarea unui serviciu oferit de un prestator de servicii care sunt utilizate pentru a oferi informații contextuale sau suplimentare cu privire la un astfel de serviciu și sunt generate sau prelucrate de un sistem informatic al prestatorului de servicii, cum ar fi originea și destinația unui mesaj sau ale oricărui alt tip de interacțiune, date privind localizarea dispozitivului, data, ora, durata, dimensiunea, ruta, formatul, protocolul utilizat și de tipul de compresie, cu excepția cazului în care aceste date constituie date privind accesul.

Acestea includ metadatele privind comunicațiile electronice, astfel cum sunt definite la articolul 4 alineatul (3) litera (g) din [Regulamentul privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice];

- (10) „date referitoare la conținut” înseamnă orice date stocate în format digital, cum ar fi mesajele scrise, mesajele vocale, înregistrările video, imaginile și sunetele, altele decât datele privind abonatii, datele privind accesul și datele privind operațiile;
- (11) „sistem informatic” înseamnă sistem informatic astfel cum este definit la articolul 2 litera (a) din Directiva 2013/40/UE a Parlamentului European și a Consiliului⁴⁵;
- (12) „stat emitent” înseamnă statul membru în care este emis ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice;
- (13) „stat de executare” înseamnă statul membru în care își are reședința sau sediul destinatarul ordinului european de divulgare a probelor electronice sau al ordinului european de păstrare a probelor electronice și căruia i se transmite, în vederea executării, ordinul european de divulgare a probelor electronice și certificatul de ordin european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice și certificatul de ordin european de păstrare a probelor electronice;
- (14) „autoritate de executare” înseamnă autoritatea competentă din statul de executare căreia autoritatea emitentă îi transmite, în vederea executării, ordinul european de divulgare a probelor electronice și certificatul de ordin european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice și certificatul de ordin european de păstrare a probelor electronice;
- (15) „cazuri de urgență” înseamnă situații în care există o amenințare iminentă la adresa vieții sau a integrității fizice a unei persoane sau la adresa unei infrastructuri critice, astfel cum este definită la articolul 2 litera (a) din Directiva 2008/114/CE a Consiliului⁴⁶.

Articolul 3 *Domeniul de aplicare*

- (1) Prezentul regulament se aplică prestatorilor de servicii care oferă servicii în Uniune.
- (2) Ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice pot fi emise doar pentru proceduri penale, atât în faza de urmărire penală, cât și în faza de judecată. De asemenea, ordinele pot fi emise în proceduri referitoare la o infracțiune pentru care o persoană juridică poate răspunde penal sau poate fi sancționată în statul emitent.
- (3) Ordinele prevăzute în prezentul regulament pot fi emise doar pentru datele referitoare la servicii oferite în Uniune, astfel cum sunt definite la articolul 2 punctul (3).

⁴⁵ [Directiva 2013/40/UE](#) a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

⁴⁶ [Directiva 2008/114/CE a Consiliului](#) din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (JO L 345, 23.12.2008, p. 75).

Capitolul 2: Ordinul european de divulgare a probelor electronice, ordinul european de păstrare a probelor electronice și certificatele aferente

Articolul 4 Autoritatea emitentă

- (1) Un ordin european de divulgare a probelor electronice care vizează date privind abonații și date privind accesul poate fi emis de către:
 - (a) un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror competent în cazul vizat sau
 - (b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitate de autoritate de investigație în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern. Un astfel de ordin european de divulgare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de divulgare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror din statul emitent.
- (2) Un ordin european de divulgare a probelor electronice care vizează date privind operațiile și date referitoare la conținut poate fi emis doar de către:
 - (a) un judecător, o instanță judecătorească sau un judecător de instrucție competent în cazul vizat sau
 - (b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitate de autoritate de investigație în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern. Un astfel de ordin european de divulgare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de divulgare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească sau un judecător de instrucție din statul emitent.
- (3) Un ordin european de păstrare a probelor electronice poate fi emis de către:
 - (a) un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror competent în cazul vizat sau
 - (b) orice altă autoritate competentă, astfel cum este definită de către statul emitent, care acționează, în cazul respectiv, în calitate de autoritate de investigație în cadrul procedurilor penale și care are competența să dispună strângerea de probe în conformitate cu dreptul intern. Un astfel de ordin european de păstrare a probelor electronice este validat, după examinarea conformității sale cu condițiile pentru emiterea unui ordin european de păstrare a probelor electronice în temeiul prezentului regulament, de către un judecător, o instanță judecătorească, un judecător de instrucție sau un procuror din statul emitent.
- (4) În cazul în care ordinul a fost validat de către o autoritate judiciară în temeiul alineatelor (1) litera (b), (2) litera (b) și (3) litera (b), autoritatea respectivă poate fi considerată, de asemenea, drept autoritate emitentă în scopul transmiterii

certificatului de ordin european de divulgare a probelor electronice și a certificatului de ordin european de păstrare a probelor electronice.

Articolul 5

Condițiile pentru emiterea unui ordin european de divulgare a probelor electronice

- (1) O autoritate emitentă poate emite un ordin european de divulgare a probelor electronice doar în cazul în care sunt îndeplinite condițiile prevăzute în prezentul articol.
- (2) Ordinul european de divulgare a probelor electronice este necesar și proporțional în scopul procedurilor menționate la articolul 3 alineatul (2) și poate fi emis doar dacă o măsură similară este disponibilă pentru aceeași infracțiune într-o situație internă asemănătoare în statul emitent.
- (3) Ordinele europene de divulgare a probelor electronice care vizează date privind abonații și date privind accesul pot fi emise pentru toate infracțiunile.
- (4) Ordinele europene de divulgare a probelor electronice care vizează date privind operațiunile sau date referitoare la conținut pot fi emise doar
 - (a) pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin 3 ani sau
 - (b) pentru următoarele infracțiuni, dacă sunt în întregime sau parțial săvârșite prin intermediul unui sistem informatic:
 - infracțiunile definite la articolele 3, 4 și 5 din Decizia-cadru 2001/413/JAI a Consiliului⁴⁷;
 - infracțiunile definite la articolele 3-7 din Directiva 2011/92/UE a Parlamentului European și a Consiliului⁴⁸;
 - infracțiunile definite la articolele 3-8 din Directiva 2013/40/UE a Parlamentului European și a Consiliului;
 - (c) pentru infracțiunile definite la articolele 3-12 și 14 din Directiva (UE) 2017/541 a Parlamentului European și a Consiliului⁴⁹.
- (5) Ordinul european de divulgare a probelor electronice include următoarele informații:
 - (a) autoritatea emitentă și, după caz, autoritatea de validare;
 - (b) destinatarul ordinului european de divulgare a probelor electronice, astfel cum se menționează la articolul 7;
 - (c) persoanele ale căror date sunt solicitate, cu excepția cazului în care unicul scop al ordinului este de a identifica o persoană;

⁴⁷ [Decizia-cadru 2001/413/JAI a Consiliului](#) din 28 mai 2001 de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul (JO L 149, 2.6.2001, p. 1).

⁴⁸ [Directiva 2011/92/UE](#) a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului (JO L 335, 17.12.2011, p. 1).

⁴⁹ [Directiva \(UE\) 2017/541](#) a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

- (d) categoria de date solicitate (date privind abonații, date privind accesul, date privind operațiile sau date referitoare la conținut);
 - (e) după caz, perioada la care se referă cererea de divulgare;
 - (f) dispozițiile de drept penal aplicabile ale statului emitent;
 - (g) în cazul unei urgențe sau al unei cereri de divulgare rapidă, motivele care o justifică;
 - (h) în cazurile în care datele solicitate sunt stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei societăți sau unei alte entități, care nu este persoană fizică, o confirmare că ordinul este emis în conformitate cu alineatul (6);
 - (i) justificarea necesității și a proporționalității măsurii.
- (6) În cazurile în care datele solicitate sunt stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei societăți sau unei alte entități, care nu este persoană fizică, ordinul european de divulgare a probelor electronice nu poate fi adresat decât prestatorului de servicii atunci când măsurile de investigare adresate societății sau entității nu sunt adecvate, în special întrucât ar putea periclita ancheta.
- (7) În cazul în care autoritatea emitentă are motive să considere că datele privind operațiile sau datele referitoare la conținut solicitate sunt protejate de imunitățile și privilegiile acordate în temeiul legislației statului membru în care își are reședința sau sediul destinatarul ordinului sau că divulgarea poate afecta interesele fundamentale ale statului membru, cum ar fi securitatea și apărarea națională, autoritatea emitentă trebuie să solicite clarificări înainte de a emite ordinul european de divulgare a probelor electronice, inclusiv prin consultarea autorităților competente ale statului membru în cauză, fie direct, fie prin intermediul Eurojust sau al Rețelei Judiciare Europene. În cazul în care autoritatea emitentă constată că datele privind accesul, datele privind operațiile sau datele referitoare la conținut solicitate sunt protejate prin astfel de imunități și privilegii sau că divulgarea lor ar afecta interesele fundamentale ale celui alt stat membru, aceasta nu emite ordinul european de divulgare a probelor electronice.

Articolul 6

Condițiile pentru emiterea unui ordin european de păstrare a probelor electronice

- (1) O autoritate emitentă poate emite un ordin european de păstrare a probelor electronice doar în cazul în care sunt îndeplinite condițiile prevăzute în prezentul articol.
- (2) Atunci când acest lucru este necesar și proporțional pentru a împiedica eliminarea, ștergerea sau modificarea datelor în vederea unei solicitări ulterioare de divulgare a acestor date prin intermediul asistenței juridice reciproce, poate fi emis un ordin european de anchetă sau un ordin european de divulgare a probelor electronice. Ordinele europene de păstrare a probelor electronice pot fi emise pentru toate infracțiunile.
- (3) Ordinul european de păstrare a probelor electronice include următoarele informații:
 - (a) autoritatea emitentă și, după caz, autoritatea de validare;

- (b) destinatarul ordinului european de păstrare a probelor electronice, astfel cum se menționează la articolul 7;
- (c) persoanele ale căror date sunt păstrate, cu excepția cazului în care unicul scop al ordinului este de a identifica o persoană;
- (d) categoria de date care trebuie păstrate (date privind abonații, date privind accesul, date privind operațiunile sau date referitoare la conținut);
- (e) după caz, perioada la care se referă cererea de păstrare;
- (f) dispozițiile de drept penal aplicabile ale statului emitent;
- (g) justificarea necesității și a proporționalității măsurii.

Articolul 7

Destinatarul unui ordin european de divulgare a probelor electronice și al unui ordin european de păstrare a probelor electronice

- (1) Ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice se adresează în mod direct unui reprezentant legal desemnat de către prestatorul de servicii, în scopul de a aduna probe în cadrul procedurilor penale.
- (2) În cazul în care nu a fost desemnat niciun reprezentant legal în mod specific, ordinul european de divulgare a probelor electronice și ordinul european de păstrare a probelor electronice pot fi adresate oricărui sediu al prestatorului de servicii în Uniune.
- (3) În cazul în care reprezentantul legal nu respectă un certificat ordin european de divulgare a probelor electronice într-un caz de urgență în temeiul articolului 9 alineatul (2), certificatul poate fi adresat oricărui sediu al prestatorului de servicii în Uniune.
- (4) În cazul în care reprezentantul legal nu respectă obligațiile care îi revin în temeiul articolului 9 sau 10 și autoritatea emitentă consideră că există un risc grav de pierdere a datelor, ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice poate fi adresat oricărui sediu al prestatorului de servicii în Uniune.

Articolul 8

Certificatul de ordin european de divulgare a probelor electronice și de ordin european de păstrare a probelor electronice

- (1) Un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice se transmite destinatarului astfel cum este definit la articolul 7 prin intermediul unui certificat de ordin european de divulgare a probelor electronice (*European Production Order Certificate* - EPOC) sau al unui certificat de ordin european de păstrare a probelor electronice (*European Preservation Order Certificate* - EPOC-PR).

Autoritatea emitentă sau autoritatea de validare completează EPOC prevăzut în anexa I sau EPOC-PR prevăzut în anexa II, îl semnează și îi certifică conținutul ca fiind exact și corect.

- (2) EPOC sau EPOC-PR este transmis direct prin orice mijloace care permit o înregistrare scrisă și în condiții care să îi permită destinatarului să stabilească autenticitatea acestuia.
- În cazul în care prestatorii de servicii, statele membre sau organismele Uniunii au instituit platforme specializate sau alte canale securizate pentru tratarea cererilor de date de către autoritățile de aplicare a legii și de către autoritățile judiciare, autoritatea emitentă poate alege, de asemenea, să transmită certificatul prin intermediul acestor canale.
- (3) EPOC conține informațiile menționate la articolul 5 alineatul (5) literele (a) - (h), inclusiv informații suficiente care să îi permită destinatarului să identifice și să contacteze autoritatea emitentă. Nu se includ justificarea necesității și a proporționalității măsurii sau detalii suplimentare cu privire la anchetă.
- (4) EPOC-PR conține informațiile menționate la articolul 6 alineatul (3) literele (a) - (f), inclusiv informații suficiente care să îi permită destinatarului să identifice și să contacteze autoritatea emitentă. Nu se includ justificarea necesității și a proporționalității măsurii sau detalii suplimentare cu privire la anchetă.
- (5) Dacă este necesar, EPOC sau EPOC-PR se traduce într-o limbă oficială a Uniunii acceptată de către destinatar. În cazul în care nicio limbă nu a fost specificată, EPOC sau EPOC-PR se traduce într-una dintre limbile oficiale ale statului membru în care își are reședința sau sediul reprezentantul legal.

Articolul 9 *Executarea unui EPOC*

- (1) După primirea unui EPOC, destinatarul se asigură că datele solicitate sunt transmise direct autorității emitente sau autorităților de aplicare a legii astfel cum se specifică în EPOC cel târziu în termen de 10 zile de la primirea EPOC, cu excepția cazului în care autoritatea emitentă indică motivele pentru care este necesară o divulgare mai rapidă.
- (2) În cazuri de urgență, destinatarul transmite datele solicitate fără întârzieri nejustificate, cel târziu în termen de 6 ore de la primirea unui EPOC.
- (3) În cazul în care destinatarul nu își poate respecta obligația întrucât EPOC este incomplet, conține erori vădite sau nu conține suficiente informații pentru executarea acestuia, destinatarul informează autoritatea emitentă menționată în EPOC fără întârzieri nejustificate și solicită clarificări, utilizând formularul prevăzut în anexa III. Acesta informează autoritatea emitentă dacă a fost posibilă identificarea și păstrarea, astfel cum se prevede la alineatul (6). Autoritatea emitentă reacționează cu promptitudine în termen de cel mult 5 zile. Termenele prevăzute la alineatele (1) și (2) nu se aplică până când nu se oferă clarificările necesare.
- (4) În cazul în care destinatarul nu își poate respecta obligația din motive de forță majoră sau de imposibilitate *de facto* care nu poate fi atribuită destinatarului sau prestatorului de servicii, în cazul în care acesta este diferit de destinatar, în special deoarece persoana ale cărei date sunt solicitate nu este clientul acestuia sau deoarece datele au fost șterse înainte de primirea EPOC, destinatarul informează autoritatea emitentă menționată în EPOC fără întârzieri nejustificate, explicând motivele prin intermediul formularului prevăzut în anexa III. Dacă sunt îndeplinite condițiile relevante, autoritatea emitentă reține EPOC.

- (5) În toate cazurile în care destinatarul nu furnizează informațiile solicitate, nu le furnizează în mod exhaustiv sau nu le furnizează în termenul stabilit, din alte motive, acesta informează autoritatea emitentă fără întârzieri nejustificate și cel târziu în termenele prevăzute la alineatele (1) și (2) cu privire la motivele sale, utilizând formularul prevăzut în anexa III. Autoritatea emitentă revizuieste ordinul ținând seama de informațiile furnizate de prestatorul de servicii și, dacă este necesar, stabilește un nou termen pentru divulgarea datelor de către prestatorul de servicii.
- În cazul în care destinatarul consideră că EPOC nu poate fi executat întrucât, exclusiv pe baza informațiilor conținute în EPOC, reiese că acest document încalcă în mod vădit Carta drepturilor fundamentale a Uniunii Europene sau că este în mod vădit abuziv, destinatarul trimite formularul prevăzut în anexa III și autorității de executare competente din statul membru al destinatarului. În astfel de cazuri, autoritatea de executare competentă poate solicita clarificări din partea autorității emitente cu privire la ordinul european de divulgare a probelor electronice, fie direct, fie prin intermediul Eurojust sau al Rețelei Judiciare Europene.
- (6) Destinatarul păstrează datele solicitate, dacă nu le divulgă imediat, cu excepția cazului în care informațiile prevăzute în EPOC nu îi permit să identifice datele solicitate, situație în care acesta solicită clarificări în conformitate cu alineatul (3). Destinatarul păstrează în continuare datele până în momentul divulgării lor, indiferent dacă această divulgare are loc pe baza ordinului european de divulgare a probelor electronice clarificat și a certificatului aferent sau prin intermediul altor canale, cum ar fi asistența juridică reciprocă. În cazul în care divulgarea și păstrarea datelor nu mai sunt necesare, autoritatea emitentă și, după caz, în temeiul articolului 14 alineatul (8), autoritatea de executare informează destinatarul fără întârzieri nejustificate.

Articolul 10

Executarea unui EPOC-PR

- (1) După primirea unui EPOC-PR, destinatarul păstrează datele solicitate, fără întârzieri nejustificate. Păstrarea încetează după 60 de zile, cu excepția cazului în care autoritatea emitentă confirmă că a fost lansată o cerere ulterioară de divulgare.
- (2) În cazul în care autoritatea emitentă confirmă în termenul prevăzut la alineatul (1) că a fost lansată o cerere ulterioară de divulgare, destinatarul păstrează datele atâta timp cât este necesar pentru a divulga datele, odată transmisă cererea ulterioară de divulgare.
- (3) În cazul în care păstrarea datelor nu mai este necesară, autoritatea emitentă informează destinatarul fără întârzieri nejustificate.
- (4) În cazul în care destinatarul nu își poate respecta obligația întrucât certificatul este incomplet, conține erori vădite sau nu conține suficiente informații pentru executarea EPOC-PR, destinatarul informează autoritatea emitentă menționată în EPOC-PR fără întârzieri nejustificate și solicită clarificări, utilizând formularul prevăzut în anexa III. Autoritatea emitentă reacționează cu promptitudine în termen de cel mult 5 zile. Destinatarul, la rândul său, se asigură că pot fi primite clarificările necesare pentru a-și îndeplini obligația prevăzută la alineatul (1).
- (5) În cazul în care destinatarul nu își poate respecta obligația din motive de forță majoră sau de imposibilitate *de facto* care nu poate fi atribuită destinatarului sau prestatorului de servicii, în cazul în care acesta este diferit de destinatar, în special

deoarece persoana ale cărei date sunt solicitate nu este clientul acestuia sau deoarece datele au fost șterse înainte de primirea ordinului, destinatarul contactează autoritatea emitentă menționată în EPOC-PR fără întârzieri nejustificate, explicând motivele prin intermediul formularului prevăzut în anexa III. Dacă sunt îndeplinite aceste condiții, autoritatea emitentă retrage EPOC-PR.

- (6) În toate cazurile în care destinatarul nu păstrează informațiile solicitate, din alte motive enumerate în formularul din anexa III, acesta informează autoritatea emitentă fără întârzieri nejustificate cu privire la motivele sale, utilizând formularul prevăzut în anexa III. Autoritatea emitentă revizuiește ordinul ținând seama de justificările oferite de prestatorul de servicii.

Articolul 11

Confidențialitate și informații destinate utilizatorilor

- (1) Destinatarii și prestatorii de servicii, în cazul în care aceștia sunt diferiți de destinatari, iau măsurile necesare pentru a asigura confidențialitatea EPOC sau EPOC-PR și a datelor divulgate sau păstrate și, în cazul în care acest lucru este solicitat de către autoritatea emitentă, se abțin de la a informa persoana ale cărei date sunt solicitate, pentru a nu obstrucționa procedurile penale relevante.
- (2) În cazul în care autoritatea emitentă a solicitat destinatarului să se abțină de la a informa persoana ale cărei date sunt solicitate, autoritatea emitentă informează persoana ale cărei date sunt solicitate prin EPOC fără întârzieri nejustificate cu privire la divulgarea datelor. Această informare poate fi amânată atât cât este necesar și proporțional pentru a evita obstrucționarea procedurilor penale relevante.
- (3) Atunci când informează persoana, autoritatea emitentă include informații cu privire la căile de atac disponibile, astfel cum se prevede la articolul 17.

Articolul 12

Rambursarea cheltuielilor

Prestatorul de servicii poate solicita rambursarea cheltuielilor sale de către statul emitent, dacă acest lucru este prevăzut în dreptul intern al statului emitent pentru ordinele naționale în situații similare, în conformitate cu aceste dispoziții de drept intern.

Capitolul 3: Sancțiuni și executare

Articolul 13

Sancțiuni

Fără a aduce atingere legislațiilor naționale care prevăd impunerea de sancțiuni penale, statele membre stabilesc normele privind sancțiunile pecuniare aplicabile în caz de nerespectare a obligațiilor ce decurg în temeiul articolelor 9, 10 și 11 din prezentul regulament și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile pecuniare prevăzute trebuie să fie eficiente, proporționale și disuasive. Statele membre informează fără întârziere Comisia despre sancțiunile și măsurile respective, precum și, în cel mai scurt termen, despre orice modificare ulterioară care le afectează.

Articolul 14
Procedura de executare

- (1) În cazul în care destinatarul nu se conformează unui EPOC în termenul stabilit sau unui EPOC-PR, fără a oferi motive acceptate de autoritatea emitentă, aceasta din urmă poate transmite autorității competente din statul de executare ordinul european de divulgare a probelor electronice însoțit de EPOC sau ordinul european de păstrare a probelor electronice însoțit de EPOC-PR, precum și formularul prevăzut în anexa III completat de către destinatar și orice alt document relevant în vederea executării sale prin orice mijloace care permit o înregistrare scrisă, în condiții care să îi permită autorității de executare să stabilească autenticitatea acestuia. În acest scop, autoritatea emitentă traduce ordinul, formularul și orice alte documente însoțitoare într-una dintre limbile oficiale ale statului membru respectiv și informează destinatarul cu privire la transfer.
- (2) În momentul primirii, autoritatea de executare recunoaște fără formalități suplimentare un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice transmis în conformitate cu alineatul (1) și ia măsurile necesare pentru executarea acestuia, cu excepția cazului în care autoritatea de executare consideră că se aplică unul dintre motivele prevăzute la alineatele (4) sau (5) sau că datele în cauză sunt protejate de o imunitate sau de un privilegiu în temeiul dreptului său intern sau divulgarea lor îi poate afecta interesele sale fundamentale, cum ar fi securitatea și apărarea națională. Autoritatea de executare ia decizia de a recunoaște ordinul fără întârzieri nejustificate și cel târziu în termen de 5 zile lucrătoare de la primirea ordinului.
- (3) În cazul în care autoritatea de executare recunoaște ordinul, aceasta impune în mod formal destinatarului să se conformeze obligației relevante, informând destinatarul cu privire la posibilitatea de a se opune executării invocând motivele enumerate la alineatele (4) sau (5), precum și cu privire la sancțiunile aplicabile în caz de neconformare și stabilește un termen-limită pentru conformare sau pentru opoziție.
- (4) Destinatarul poate să se opună executării ordinului european de divulgare a probelor electronice doar invocând următoarele motive:
 - (a) ordinul european de divulgare a probelor electronice nu a fost emis sau validat de o autoritate emitentă astfel cum se prevede la articolul 4;
 - (b) ordinul european de divulgare a probelor electronice nu a fost emis pentru o infracțiune prevăzută la articolul 5 alineatul (4);
 - (c) destinatarul nu a putut să se conformeze EPOC din cauza unei imposibilități *de facto* sau din motive de forță majoră sau deoarece EPOC conține erori vădite;
 - (d) ordinul european de divulgare a probelor electronice nu vizează date stocate de către prestatorul de servicii sau în numele acestuia în momentul primirii EPOC;
 - (e) serviciul nu este reglementat de prezentul regulament;
 - (f) exclusiv pe baza informațiilor conținute în EPOC, reiese că acest document încalcă în mod vădit Carta drepturilor fundamentale a Uniunii Europene sau că este în mod vădit abuziv.
- (5) Destinatarul poate să se opună executării ordinului european de păstrare a probelor electronice doar invocând următoarele motive:

- (a) ordinul european de păstrare a probelor electronice nu a fost emis sau validat de o autoritate emitentă astfel cum se prevede la articolul 4;
 - (b) prestatorul de servicii nu a putut să se conformeze EPOC-PR din cauza unei imposibilității *de facto* sau din motive de forță majoră sau deoarece EPOC-PR conține erori vădite;
 - (c) ordinul european de păstrare a probelor electronice nu vizează date stocate de către prestatorul de servicii sau în numele acestuia în momentul primirii EPOC-PR;
 - (d) serviciul nu intră în domeniul de aplicare al prezentului regulament;
 - (e) exclusiv pe baza informațiilor conținute în EPOC-PR, reiese că acest document încalcă în mod vădit Carta drepturilor fundamentale a Uniunii Europene sau că este în mod vădit abuziv.
- (6) În cazul unei obiecții formulate de destinatar, autoritatea de executare decide dacă va executa sau nu ordinul pe baza informațiilor furnizate de către destinatar și, dacă este necesar, pe baza informațiilor suplimentare obținute de la autoritatea emitentă în conformitate cu alineatul (7).
- (7) Înainte de a decide să nu recunoască sau să nu execute ordinul în conformitate cu alineatele (2) și (6), autoritatea de executare se consultă cu autoritatea emitentă prin orice mijloace adecvate. După caz, aceasta solicită informații suplimentare din partea autorității emitente. Autoritatea emitentă răspunde la orice cerere de acest tip în termen de 5 zile lucrătoare.
- (8) Toate deciziile sunt notificate imediat autorității emitente și destinatarului prin orice mijloace care permit o înregistrare scrisă.
- (9) În cazul în care autoritatea de executare obține datele de la destinatar, aceasta le transmite autorității emitente în termen de 2 zile lucrătoare, cu excepția cazului în care datele respective sunt protejate de o imunitate sau de un privilegiu în temeiul dreptului său intern sau îi afectează interesele sale fundamentale, cum ar fi securitatea și apărarea națională. În acest caz, autoritatea de executare informează autoritatea emitentă cu privire la motivele pentru care nu transmite datele.
- (10) În cazul în care destinatarul nu se conformează obligațiilor care îi revin în temeiul unui ordin recunoscut al cărui caracter executoriu a fost confirmat de către autoritatea de executare, autoritatea respectivă impune o sancțiune pecuniară în conformitate cu dreptul său intern. Este disponibilă o cale de atac eficientă împotriva deciziei de aplicare a unei amenzi.

Capitolul 4: Căi de atac

Articolul 15

Procedura de control jurisdicțional în cazul unor obligații contradictorii bazate pe drepturile fundamentale sau pe interesele fundamentale ale unei țări terțe

- (1) În cazul în care destinatarul consideră că respectarea ordinului european de divulgare a probelor electronice ar intra în conflict cu legislația aplicabilă a unei țări terțe care interzice divulgarea datelor în cauză pe motiv că acest lucru este necesar pentru protecția fie a drepturilor fundamentale ale persoanelor în cauză, fie a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, acesta

informează autoritatea emitentă cu privire la motivele sale de a nu executa ordinul european de divulgare a probelor electronice, în conformitate cu procedura menționată la articolul 9 alineatul (5).

- (2) Obiecția motivată include toate detaliile relevante cu privire la legislația țării terțe, la aplicabilitatea sa în cazul vizat și la natura obligației contradictorii. Ea nu poate fi întemeiată pe faptul că nu există dispoziții similare privind condițiile, formalitățile și procedurile de emitere a unui ordin de divulgare în legislația aplicabilă a țării terțe și nici pe circumstanța unică în care datele ar fi stocate într-o țară terță.
- (3) Autoritatea emitentă revizuiește ordinul european de divulgare a probelor electronice pe baza obiecției motivate. În cazul în care autoritatea emitentă intenționează să mențină ordinul european de divulgare a probelor electronice, aceasta solicită un control jurisdicțional din partea instanței competente din statul său membru. Execuția ordinului este suspendată până la finalizarea controlului jurisdicțional.

Instanța competentă evaluează mai întâi dacă există un conflict, examinând:

- (a) dacă, pe baza circumstanțelor specifice ale cazului respectiv, se aplică legislația țării terțe și, în caz afirmativ,
 - (b) dacă legislația țării terțe, aplicată circumstanțelor specifice ale cazului respectiv, interzice divulgarea datelor în cauză.
- (4) Atunci când efectuează această evaluare, instanța ar trebui să ia în considerare dacă legislația țării terțe, în loc să vizeze protejarea drepturilor fundamentale sau a intereselor fundamentale ale țării terțe legate de securitatea sau apărarea națională, încearcă în mod evident să protejeze alte interese sau are drept obiectiv protejarea unor activități ilegale împotriva solicitărilor de aplicare a legii în contextul anchetelor penale.
 - (5) În cazul în care instanța competentă consideră că nu există niciun conflict relevant în sensul alineatelor (1) și (4), aceasta menține ordinul. În cazul în care instanța competentă stabilește existența unui conflict relevant în sensul alineatelor (1) și (4), aceasta transmite toate informațiile factuale și legale relevante în ceea ce privește cauza, inclusiv evaluarea sa, autorităților centrale din țara terță respectivă, prin intermediul autorității sale centrale naționale, stabilind un termen de 15 zile pentru obținerea unui răspuns din partea autorităților respective. La cererea motivată a autorității centrale din țara terță, termenul poate fi prelungit cu 30 de zile.
 - (6) În cazul în care, în termenul stabilit, autoritatea centrală din țara terță informează instanța competentă că se opune executării ordinului european de divulgare a probelor electronice în această cauză, instanța competentă revocă ordinul și informează autoritatea emitentă și destinatarul. Dacă nu se primește nicio obiecție în termenul stabilit (sau prelungit), instanța competentă trimite un mesaj de atenționare prin care acordă autorității centrale din țara terță încă 5 zile pentru a răspunde și prin care o informează cu privire la consecințele lipsei unui răspuns din partea sa. În cazul în care nu se primește nicio obiecție în acest termen suplimentar, instanța competentă menține ordinul.
 - (7) În cazul în care instanța competentă stabilește că ordinul trebuie menținut, aceasta informează autoritatea emitentă și destinatarul, care execută ordinul.

Articolul 16

Procedura de control jurisdicțional în cazul unor obligații contradictorii bazate pe alte motive

- (1) În cazul în care destinatarul consideră că respectarea ordinului european de divulgare a probelor electronice ar intra în conflict cu legislația aplicabilă a unei țări terțe care interzice divulgarea datelor în cauză din alte motive decât cele menționate la articolul 15, acesta informează autoritatea emitentă cu privire la motivele sale de a nu executa ordinul european de divulgare a probelor electronice, în conformitate cu procedura menționată la articolul 9 alineatul (5).
- (2) Obiecția motivată trebuie să includă toate detaliile relevante cu privire la legislația țării terțe, la aplicabilitatea sa în cazul vizat și la natura obligației contradictorii. Ea nu poate fi întemeiată pe faptul că nu există dispoziții similare privind condițiile, formalitățile și procedurile de emitere a unui ordin de divulgare în legislația aplicabilă a țării terțe și nici pe circumstanța unică în care datele ar fi stocate într-o țară terță.
- (3) Autoritatea emitentă revizuieste ordinul european de divulgare a probelor electronice pe baza obiecției motivate. În cazul în care autoritatea emitentă intenționează să mențină ordinul european de divulgare a probelor electronice, aceasta solicită un control jurisdicțional din partea instanței competente din statul său membru. Execuția ordinului este suspendată până la finalizarea controlului jurisdicțional.
- (4) Instanța competentă evaluează mai întâi dacă există un conflict, examinând:
 - (a) dacă, pe baza circumstanțelor specifice ale cazului respectiv, se aplică legislația țării terțe și, în caz afirmativ,
 - (b) dacă legislația țării terțe, aplicată circumstanțelor specifice ale cazului respectiv, interzice divulgarea datelor în cauză.
- (5) În cazul în care instanța competentă consideră că nu există niciun conflict relevant în sensul alineatelor (1) și (4), aceasta menține ordinul. În cazul în care instanța competentă stabilește că legislația țării terțe, atunci când se aplică circumstanțelor specifice ale cauzei supuse examinării, interzice divulgarea datelor în cauză, instanța competentă decide menținerea sau retragerea ordinului, în special pe baza următorilor factori:
 - (a) interesul protejat de legislația relevantă a țării terțe, inclusiv interesul țării terțe în ceea ce privește împiedicarea divulgării datelor;
 - (b) gradul de legătură dintre cauza penală pentru care a fost emis ordinul și cele două jurisdicții, astfel cum reiese din analiza, printre altele, a următorilor factori:

localizarea, cetățenia și reședința persoanei ale cărei date sunt solicitate și/sau ale victimei (victimelor);

locul în care a fost săvârșită infracțiunea în cauză;
 - (c) gradul de legătură dintre prestatorul de servicii și țara terță în cauză; în acest context, locul de stocare a datelor în sine nu este suficient pentru stabilirea unei legături substanțiale;
 - (d) interesele statului care desfășoară ancheta în obținerea probelor în cauză, pe baza gravității infracțiunii și a importanței obținerii de probe în mod rapid;

- (e) posibilele consecințe pentru destinatar sau pentru prestatorul de servicii ale respectării ordinului european de divulgare a probelor electronice, inclusiv sancțiunile care ar putea fi aplicate.
- (6) În cazul în care instanța competentă decide să revoce ordinul, aceasta informează autoritatea emitentă și destinatarul. În cazul în care instanța competentă stabilește că ordinul trebuie menținut, aceasta informează autoritatea emitentă și destinatarul, care execută ordinul.

Articolul 17 *Căi de atac eficiente*

- (1) Persoanele suspectate și acuzate ale căror date au fost obținute prin intermediul unui ordin european de divulgare a probelor electronice au dreptul la căi de atac eficiente împotriva ordinului european de divulgare a probelor electronice în cursul procedurilor penale pentru care a fost emis ordinul, fără a aduce atingere căilor de atac disponibile în temeiul Directivei (UE) 2016/680 și al Regulamentului (UE) 2016/679.
- (2) În cazul în care persoana ale cărei date au fost obținute nu este o persoană suspectată sau acuzată în cadrul procedurilor penale pentru care a fost emis ordinul, aceasta are dreptul la căi de atac eficiente împotriva unui ordin european de divulgare a probelor electronice în statul emitent, fără a aduce atingere căilor de atac disponibile în temeiul Directivei (UE) 2016/680 și al Regulamentului (UE) 2016/679.
- (3) Dreptul la o cale de atac eficientă se exercită în fața unei instanțe din statul emitent în conformitate cu legislația națională din acest stat și include posibilitatea de a contesta legalitatea măsurii în cauză, inclusiv necesitatea și proporționalitatea acesteia.
- (4) Fără a aduce atingere articolului 11, autoritatea emitentă ia măsurile corespunzătoare pentru a garanta faptul că sunt furnizate informații cu privire la posibilitățile de a recurge la căi de atac în temeiul dreptului național și că acestea pot fi exercitate în mod eficient.
- (5) În acest caz se aplică aceleași termene-limită și celelalte condiții ca în cazul recurgerii la o cale de atac în cauze interne similare, într-un mod care să garanteze exercitarea eficientă a acestor căi de atac pentru persoanele în cauză.
- (6) Fără a aduce atingere normelor procedurale interne, statele membre asigură faptul că, în procedurile penale din statul emitent, se respectă dreptul la apărare și echitatea procedurilor în cadrul evaluării probelor obținute prin intermediul ordinului european de divulgare a probelor electronice.

Articolul 18 *Respectarea privilegiilor și a imunităților în temeiul legislației statului de executare*

În cazul în care datele privind operațiile sau datele referitoare la conținut obținute prin intermediul ordinului european de divulgare a probelor electronice sunt protejate de imunități sau privilegii acordate în temeiul legislației statului membru al destinatarului sau acestea afectează interesele fundamentale ale statului membru, cum ar fi securitatea și apărarea națională, instanța din statul emitent se asigură, în cursul procedurilor penale pentru care a fost emis ordinul, că aceste motive sunt luate în considerare în același mod ca și când ar fi fost prevăzute în dreptul său național atunci când evaluează relevanța și admisibilitatea probelor în

cauză. Instanța poate consulta autoritățile din statul membru relevant, Rețeaua Judiciară Europeană în materie penală sau Eurojust.

Capitolul 5: Dispoziții finale

Articolul 19

Monitorizarea și raportarea

- (1) Până la *[data aplicării prezentului regulament]* cel târziu, Comisia stabilește un program detaliat de monitorizare a realizărilor, a rezultatelor și a impactului prezentului regulament. Programul de monitorizare stabilește mijloacele care vor fi utilizate și intervalele care vor fi aplicate pentru colectarea de date și alte probe necesare. Acesta precizează măsurile care trebuie luate de Comisie și, respectiv, de statele membre pentru colectarea și analizarea datelor și a altor probe.
- (2) În orice caz, statele membre colectează date de la autoritățile relevante și realizează statistici cuprinzătoare. Datele colectate sunt trimise Comisiei în fiecare an până la data de 31 martie pentru anul calendaristic precedent și includ:
 - (a) numărul de EPOC și EPOC-PR emise în funcție de tipul de date solicitate, în funcție de prestatorii de servicii destinatari și în funcție de situație (cazuri de urgență sau nu);
 - (b) numărul de EPOC executate și neexecutate în funcție de tipul de date solicitate, în funcție de prestatorii de servicii destinatari și în funcție de situație (cazuri de urgență sau nu);
 - (c) pentru EPOC executate, durata medie de obținere a datelor solicitate din momentul în care a fost emis EPOC până în momentul obținerii datelor, în funcție de tipul de date solicitate, în funcție de prestatorii de servicii destinatari și în funcție de situație (cazuri de urgență sau nu);
 - (d) numărul de ordine europene de divulgare a probelor electronice transmise și primite în vederea executării în statul de executare, în funcție de tipul de date solicitate, în funcție de prestatorii de servicii destinatari și în funcție de situație (cazuri de urgență sau nu) și numărul de ordine executate;
 - (e) numărul de căi de atac împotriva ordinelor europene de divulgare a probelor electronice în statul emitent și în statul de executare în funcție de tipul de date solicitate.

Articolul 20

Modificarea certificatelor și a formularelor

Comisia adoptă acte delegate în conformitate cu articolul 21 de modificare a anexelor I, II și III, pentru a aborda în mod eficient o eventuală nevoie de îmbunătățire în ceea ce privește conținutul formularelor EPOC și EPOC-PR și al formularelor care trebuie utilizate pentru a furniza informații cu privire la imposibilitatea de a executa EPOC sau EPOC-PR.

Articolul 21

Exercitarea delegării

- (1) Se conferă Comisiei competența de a adopta acte delegate în condițiile prevăzute la prezentul articol.

- (2) Delegarea competenței menționate la articolul 20 se acordă pe durată nedeterminată începând din *[data aplicării prezentului regulament]*.
- (3) Delegarea de competențe menționată la articolul 20 poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte în ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară menționată în decizie. Decizia nu aduce atingere valabilității actelor delegate care sunt deja în vigoare.
- (4) Înainte de adoptarea unui act delegat, Comisia îi consultă pe experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016⁵⁰.
- (5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.
- (6) Un act delegat adoptat în temeiul articolului 20 intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea actului respectiv către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 22

Notificări

- (1) Până la *[data aplicării prezentului regulament]*, fiecare stat membru notifică Comisiei următoarele:
 - (a) autoritățile care, în conformitate cu dreptul său intern, sunt competente în temeiul articolului 4 să emită și/sau să valideze ordine europene de divulgare a probelor electronice și ordine europene de păstrare a probelor electronice;
 - (b) autoritatea de executare sau autoritățile competente să execute ordine europene de divulgare a probelor electronice și ordine europene de păstrare a probelor electronice în numele unui alt stat membru;
 - (c) instanțele competente să soluționeze obiecții motivate de către destinatari în conformitate cu articolele 15 și 16.
- (2) Comisia pune informațiile primite în conformitate cu prezentul articol la dispoziția publicului, fie pe un site web specific, fie pe site-ul web al Rețelei Judiciare Europene menționat la articolul 9 din Decizia 2008/976/JAI a Consiliului⁵¹.

Articolul 23

Relația cu ordinele europene de anchetă

Autoritățile statelor membre pot continua să emită ordine europene de anchetă în conformitate cu Directiva 2014/41/UE pentru colectarea de probe care ar intra, de asemenea, sub incidența prezentului regulament.

⁵⁰ JO L 123, 12.5.2016, p. 13.

⁵¹ Decizia 2008/976/JAI a Consiliului din 16 decembrie 2008 privind Rețeaua Judiciară Europeană (JO L 348, 24.12.2008, p. 130).

Articolul 24

Evaluare

Până la [5 ani de la data aplicării prezentului regulament] cel târziu, Comisia efectuează o evaluare a regulamentului și prezintă un raport Parlamentului European și Consiliului cu privire la funcționarea prezentului regulament, care include o evaluare a necesității de a extinde domeniul său de aplicare. Dacă este cazul, raportul este însoțit de propuneri legislative. Evaluarea este efectuată în conformitate cu Orientările Comisiei privind o mai bună legiferare. Statele membre furnizează Comisiei informațiile necesare pentru întocmirea raportului.

Articolul 25

Intrarea în vigoare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Se aplică de la [6 luni de la intrarea sa în vigoare].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.

Adoptat la Bruxelles,

*Pentru Parlamentul European,
Președintele*

*Pentru Consiliu,
Președintele*