Consiliul
Uniunii Europene

Bruxelles, 30 noiembrie 2018
(OR. en)

15020/18

Dosar interinstituțional:
2018/0108(COD)

JAI 1236
COPEN 428
CYBER 304
DROIPEN 192
JAIEX 160
ENFOPOL 596
DAPIX 366
EJUSTICE 163
MI 917
TELECOM 442
DATAPROTECT 263
CODEC 2180

NOTĂ

Sursă:	Președinția
Destinatar:	Consiliul
Nr. doc. ant.:	14351/1/18 REV1
Nr. doc. Csie:	8110/18
Subiect:	Regulamentul Parlamentului European și al Consiliului privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală - abordare generală

INTRODUCERE

1. La 17 aprilie 2018, Comisia a adoptat și a transmis Consiliului și Parlamentului European propunerea sus-menționată, al cărei temei juridic îl constituie articolul 82 alineatul (1) din TFUE. Propunerea urmărește crearea unor ordine europene de divulgare și de păstrare a probelor electronice pentru a se putea obține sau păstra astfel de probe într-o jurisdicție străină, fără implicarea autorităților competente din jurisdicția respectivă. Ordinele vizează în mod specific accesul transfrontalier la probe electronice, încercând să adapteze mecanismele de cooperare judiciară la nevoile care însoțesc combaterea criminalității în era digitală.

2. Propunere de regulament creează posibilitatea de a solicita orice categorie de date stocate. Cu toate acestea, propunerea prevede un anumit prag pentru datele referitoare la traficul pe internet și cele referitoare la conținut [spre deosebire de datele privind abonații și de cele privind accesul], care pot fi solicitate numai pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin trei ani pentru anumite infracțiuni dependente de mediul informatic, facilitate de calculator sau legate de terorism.

3. Propunerea prevede un termen-limită obligatoriu de zece zile pentru executarea ordinului european de divulgare a probelor electronice, dar în cazuri de urgență (amenințare iminentă la adresa vieții sau a integrității fizice a unei persoane sau la adresa unei infrastructuri critice) termenul este de șase ore. În ceea ce privește ordinul european de păstrare a probelor electronice, autoritatea competentă are la dispoziție 60 de zile pentru a confirma că a demarat procedura de emitere a unei solicitări ulterioare de divulgare a datelor (inclusiv prin asistența judiciară reciprocă). În cazul nerespectării unui ordin, se pot impune sancțiuni prestatorului de servicii.

4. Ordinele trebuie adresate unui prestator de servicii care oferă servicii în Uniune sau reprezentantului legal desemnat de prestatorul de servicii, situat într-un alt stat membru, în scopul colectării de probe electronice, în conformitate cu propunerea de directivă. Proiectul de regulament utilizează drept criterii tipul de servicii furnizate (servicii de comunicații electronice, societatea informațională, servicii de găzduire, numerotarea IP, servicii de protecție a vieții private și servicii de proxy), desemnând, totodată, anumite tipuri de prestatori de servicii (registre de nume de domenii de internet sau operatori de astfel de registre).

5. La 18 octombrie 2018, Consiliul European[1] a solicitat identificarea unei soluții pentru a se asigura accesul transfrontalier rapid și eficient la probele electronice, pentru a se lupta în mod eficace împotriva terorismului și a criminalității grave și organizate, atât în cadrul UE, cât și la nivel internațional. Acesta a subliniat faptul că ar trebui să se convină asupra propunerilor Comisiei privind probele electronice până la sfârșitul legislaturii actuale.

6. În Parlamentul European, dna Birgit Sippel (LIBE, S&D) a fost numită raportor la 24 mai 2018. Comisia LIBE a discutat propunerea la 11 iunie 2018 și a organizat mai multe reuniuni și audieri, inclusiv o audiere publică la 27 noiembrie 2018. Nu a fost stabilit un calendar pentru adoptarea raportului.

7. Comitetul Economic și Social European și-a adoptat avizul[2] la 12 iulie 2018.

---

1 EUCO 13/18, punctul 9.
2 Documentul 11533/18.

II. LUCRĂRILE DIN CADRUL CONSILIULUI

8. Comisia a prezentat această propunere Grupului de lucru COPEN la 27 aprilie 2018, prezentarea fiind urmată de o examinare articol cu articol a propunerii de regulament și de un schimb de opinii cu privire la evaluarea de impact în cadrul grupului de lucru, la 5-6 mai 2018. În general, atât evaluarea de impact, cât și propunerea au fost primite favorabil de către delegații.

9. Discuțiile s-au concentrat în principal pe conceptul propus de Comisie, și anume de a transmite un ordin european de divulgare a probelor electronice direct prestatorului de servicii sau reprezentantului său legal, fără implicarea statului membru unde se află aceștia (adică, statul de executare), pe definiția sintagmei „prestator de servicii”, pe chestiunea imunităților și privilegiilor, pe procedura de control jurisdicțional în cazul unor obligații contradictorii, precum și pe sancțiunile pentru nerespectarea obligațiilor în temeiul regulamentului.

10. Examinarea propunerii de către grupul de lucru s-a desfășurat în timpul președințiilor bulgară și austriacă. Au fost organizate douăsprezece întâlniri care au avut drept rezultat cinci versiuni revizuite consecutive. Discuțiile s-au încheiat la 20 noiembrie 2018, în vederea transmiterii textului de compromis care figurează în anexa la prezenta notă, spre adoptare cu titlul de abordare generală cu privire la propunere, în cadrul următoarei reuniuni a Consiliului JAI din 6 și 7 decembrie 2018.

11. Rezultatul discuțiilor din cadrul reuniunilor grupului de lucru, contribuțiile scrise primite din partea delegațiilor, precum și rezervele statelor membre cu privire la text, sunt reflectate în textul de compromis revizuit al Președinției, care figurează în anexă. Considerentele au fost adaptate pentru a reflecta modificările aduse dispozițiilor de fond. Toate modificările față de propunerea Comisiei sunt scoase în evidență prin **caractere aldine** (pentru textul nou) și prin [...] (pentru textul eliminat).

III. CONCLUZIE

12. Textul, astfel cum figurează în anexă, reflectă eforturile depuse de Președinție și de statele membre pentru a se ajunge la un compromis.

13. La 28 noiembrie 2018, Comitetul Reprezentanților Permanenți a ajuns la un acord cu privire la textul de compromis al Președinției, astfel cum figurează în anexa la prezenta notă, cu o singură modificare, și anume eliminarea rezervei delegației SI în nota de subsol 27.

14. Consiliul este invitat, prin urmare, să ajungă la o abordare generală cu privire la acest text, care va constitui baza pentru negocierile cu Parlamentul European în cadrul procedurii legislative ordinare (articolul 294 din TFUE).

ANEXĂ

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală[3]

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 parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[4],

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 1516 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 Țările de Jos, Finlanda, Republica Cehă și Letonia au formulat o rezervă cu privire la întregul text de compromis. În ceea ce privește Țările de Jos, această rezervă se referă, printre altele, la articolele 5, 6, 7a, 11 alineatul (3), 12a, 12b, 14 și 17.

4 JO C , , p. .

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

(5) În comunicarea comună din 13 septembrie 2017 privind reziliența, prevenirea și apărarea[5], 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[6] din 3 octombrie 2017, 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.

---

5 JOIN(2017) 450 final.

6 2017/2068(INI).

(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 **sistematică** [...], **în fiecare caz**, a 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 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.

(**12a**) **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 Consiliului[7]. În orice caz, ar trebui ca ordinul european de divulgare a probelor electronice să nu fie eliberat în cazul în care statul membru emitent dispune de indicii conform cărora acest lucru ar contraveni principiului *non bis in idem*.**

[7] 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).

(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/UE[8], 2012/13/UE[9], 2013/48/UE[10], 2016/343[11], 2016/800[12] și 2016/1919[13] ale Parlamentului European și ale Consiliului.

(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.

---

8 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).

9 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).

10 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).

11 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).

12 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).

13 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).

(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 telefonia VOIP, mesageria instantanee și serviciile de e-mail. **Prezentul regulament ar trebui să se aplice totodată și altor** [...] **prestatori** [...] de servicii ale societății informaționale **în sensul Directivei (UE) 2015/1535** [...] **care** nu se califică drept [...] **prestatori** de servicii de comunicații electronice, **dar care oferă utilizatorilor lor fie capacitatea de a comunica între ei, fie servicii care pot fi utilizate pentru a stoca sau prelucra date în numele acestora. Acest lucru ar trebui să fie conform cu termenii utilizați în Convenția de la Budapesta privind criminalitatea informatică. Prelucrarea datelor trebuie înțeleasă în sens tehnic, drept crearea sau manipularea de date, cu alte cuvinte operații tehnice prin care se produc sau se modifică date cu ajutorul capacității de procesare a computerelor. Categoriile de prestatori de servicii incluse aici sunt, de exemplu,** piețele online [...] **care oferă** consumatorilor [...] **și** întreprinderilor **capacitatea de a comunica unii cu alții** și alte servicii de găzduire, inclusiv în cazul în care serviciul este furnizat prin intermediul tehnologiei de tip *cloud computing*, **precum și platforme online de jocuri și platforme online de jocuri de noroc. În cazurile în care un prestator de servicii ale societății informaționale nu oferă utilizatorilor săi capacitatea de a comunica între ei, ci doar cu prestatorul de servicii, sau nu oferă capacitatea de a prelucra sau de a stoca date ori în cazurile în care capacitatea de a stoca/prelucra date nu este o componentă esențială a serviciului pus la dispoziția utilizatorilor, cum ar fi serviciile juridice, de arhitectură, de inginerie și de contabilitate prestate online la distanță, acesta nu ar intra în domeniul de aplicare al definiției, chiar dacă serviciile respective corespund definiției serviciilor societății informaționale prevăzute în 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, nu este nevoie ca prestatorii de servicii să fie stabiliți 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 a unității 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.

(24a) Întrucât procedurile care vizează acordarea de asistență juridică reciprocă pot fi considerate drept proceduri penale în conformitate cu dreptul intern aplicabil în statele membre, ar trebui să se clarifice faptul că ordinul european de divulgare a probelor electronice sau ordinul european de păstrare a probelor electronice nu ar trebui emis în scopul furnizării de asistență juridică reciprocă altui stat membru sau unei țări terțe. În astfel de cazuri, cererea de acordare a asistenței juridice reciproce ar trebui adresată statului membru sau țării terțe care poate furniza asistența juridică reciprocă în temeiul dreptului său intern. Cu toate acestea, în cazul în care autoritatea emitentă a obținut deja probe electronice în temeiul prezentului regulament pentru propriile proceduri sau anchete penale, iar ulterior datele respective fac obiectul transferului sau transmiterii, ar trebui să se aplice condițiile referitoare la principiul specialității.

(24b) Prezentul regulament ar trebui să se aplice procedurilor penale inițiate de autoritatea emitentă în scopul localizării unei persoane condamnate care s-a sustras justiției, în scopul executării unei pedepse sau a unei măsuri de siguranță privative de libertate. Cu toate acestea, în cazul în care sentința sau măsura de siguranță privativă de libertate a fost pronunțată/luată *in absentia*, nu ar trebui să fie posibil să se emită un ordin european de divulgare a probelor electronice sau un ordin european de păstrare a probelor electronice, întrucât dreptul intern al statelor membre privind hotărârile judecătorești pronunțate *in absentia* variază considerabil pe teritoriul Uniunii Europene.

(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 [...] baza**t** [...] **pe criterii faptice specifice, precum** existența unui număr semnificativ de utilizatori în unul sau mai multe state membre sau orientarea 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 comercială[14]. Pe de altă parte, prestarea serviciului în vederea simplei respectări a interdicției de discriminare prevăzute în Regulamentul (UE) 2018/302[15] 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 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, **ținându-se seama în mod corespunzător de impactul măsurii asupra drepturilor fundamentale ale persoanei ale cărei date sunt solicitate.**

---

14 Regulamentul (UE) 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).

15 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).

(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 trei 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.

(33a) În cazurile în care un ordin este emis pentru a se obține categorii de date diferite, autoritatea emitentă trebuie să se asigure că condițiile și procedurile, cum ar fi notificarea statului de executare, sunt îndeplinite pentru toate categoriile de date respective.

(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 pericliteze 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.

(34a) În cazul în care datele sunt stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei autorități publice, doar autoritățile din același stat membru ar trebui să aibă capacitatea de a emite un ordin european de divulgare sau de păstrare a probelor electronice, deoarece astfel de date pot fi considerate drept deosebit de sensibile. Prin autoritate publică ar trebui să se înțeleagă orice autoritate care, în temeiul dreptului său intern aplicabil, este împuternicită să guverneze sau să asigure administrarea unei anumite părți sau a unui anumit aspect al vieții publice, cum ar fi subdiviziuni ale ramurilor judiciară, legislativă sau executivă ale unui stat, provincii sau municipalități.

(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 **sau dreptul jurnaliștilor de a nu-și divulga sursele de informare)**, 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. [...] **Măsura în care un al doilea cadru legislativ trebuie luat în considerare ar trebui să depindă de intensitatea legăturii dintre persoana ale cărei date sunt solicitate și statul emitent. Atunci când persoana își are reședința pe teritoriul statului emitent, există o legătură puternică cu statul emitent. Prin urmare, cadrul legislativ aplicabil pentru evaluarea** imunităților și privilegiilor **ar trebui să fie, exclusiv, cel al statului emitent. Același principiu se aplică normelor pentru stabilirea și limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă, precum și intereselor fundamentale ale statului de executare. Până la formularea unei solicitări de date referitoare la conținut sau de date privind operațiile, autorităților dețin deja indicii, de regulă, legate de locul de reședință al persoanei în cauză, pe baza demersurilor anterioare de investigații. Mai mult, datele statistice indică faptul că în marea majoritate a cazurilor, persoana își are reședința în statul emitent. În cazurile în care situația este diferită, de exemplu pentru că persoana ale cărei date sunt solicitate a luat măsuri pentru a ascunde locul în care se află, ar trebui să se aplice același principiu.**

(35a) **I**munitățile și privilegiile, **precum și normele privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă,** care protejează [...] datele privind operațiile sau referitoare la conținut în [...] statul [...] **de executare** ar trebui, **prin urmare,** să fie luate în considerare [...] **în cazul în care autoritatea emitentă are motive întemeiate să considere că persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul său.** [...] Acest lucru este relevant în special în cazul în care legislația statului membru **respectiv** [...] 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. [...] **A**ceste aspecte ar trebui să fie luate în considerare nu doar atunci când ordinul este emis, ci și mai târziu, de către autoritatea de executare,[...] în cazul în care are loc o procedură de executare.

(35b) În cazul în care autoritatea emitentă urmărește să obțină date privind operațiile și are motive întemeiate să considere că persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul său și că datele solicitate sunt protejate de imunitățile și privilegiile acordate în temeiul legislației statului de executare sau de norme ale statului membru respectiv privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă ori că divulgarea lor poate afecta interesele fundamentale ale statului membru respectiv, cum ar fi securitatea și apărarea națională, autoritatea emitentă ar trebui să solicite clarificări, inclusiv prin recurgerea la consultări adecvate.

(35c) În cazurile în care ordinul european de divulgare a probelor electronice vizează date referitoare la conținut, iar autoritatea emitentă are motive întemeiate să considere că persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul său, statul de executare este notificat și are posibilitatea de a informa autoritatea emitentă cât mai curând posibil, de preferință în termen de 10 zile, despre probleme care ar putea conduce la retragerea sau modificarea ordinului, ca de pildă imunitățile și privilegiile persoanei ale cărei date sunt solicitate sau norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă. Spre deosebire de datele care nu se referă la conținut, cele referitoare la conținut sunt deosebit de sensibile, întrucât este posibil ca persoanele să își dezvăluie gândurile, precum și amănunte delicate despre viața lor privată. Acest fapt justifică aplicarea unui tratament diferit, precum și implicarea autorităților statului de executare încă din primele etape ale procedurii. În astfel de cazuri, statul membru emitent ar trebui să furnizeze o copie a certificatului statului de executare în același moment în care certificatul este furnizat prestatorului de servicii. Pentru a facilita o verificare rapidă, autoritatea emitentă ar trebui să aleagă una dintre limbile acceptate de către statul de executare în cazul în care este necesară o traducere a certificatului, chiar și atunci când prestatorul de servicii a semnalat că este dispus să accepte și certificate redactate în alte limbi decât una dintre limbile oficiale ale statului de executare. În eventualitatea în care […] autoritatea notificată semnalează probleme, aceasta ar trebui să pună la dispoziția autorității emitente toate informațiile relevante referitoare la imunitățile și privilegiile acordate persoanei în temeiul dreptului său intern sau referitoare la norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă ori informații din care să reiasă că ordinul afectează interesele fundamentale ale statului membru în cauză, cum ar fi securitatea și apărarea națională.

(35d) În cazurile în care, în momentul emiterii ordinului european de divulgare a probelor electronice, persoana are mai mult de un loc de reședință, iar unul dintre acestea este situat pe teritoriul statului emitent, sau în cazurile în care locul de reședință al persoanei nu poate fi stabilit prin eforturi rezonabile și proporționate, procedurile de mai sus nu se aplică. Cu toate acestea, o vizită scurtă, o vacanță sau un sejur similar în statul emitent nu sunt suficiente pentru a stabili existența unui drept de reședință în acel stat membru, în absența oricărei alte legături strânse.

(35e) Pentru a face posibilă o procedură rapidă, momentul potrivit pentru a se determina dacă este necesară notificarea autorităților statului de executare ar trebui să fie momentul în care ordinul este emis sau validat. Orice schimbare ulterioară a locului de reședință nu ar trebui să aibă niciun impact asupra procedurii. În cazul în care autoritatea emitentă nu are motive întemeiate să considere că persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul său la momentul emiterii sau validării ordinului, iar mai târziu se dovedește că, într-adevăr, persoana respectivă nu își avea reședința pe teritoriul statului membru emitent, nu ar mai trebui să fie necesară nicio verificare sau notificare ulterioară. Cu toate acestea, persoana vizată își poate invoca drepturile, precum și norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă pe întreaga durată a procedurii penale, iar celălalt stat membru poate invoca, la rândul său, interesele sale fundamentale, precum securitatea și apărarea națională, în orice moment în timpul desfășurării procedurii penale. Mai mult, aceste considerente ar putea fi invocate și în timpul procedurii de executare.

(35f) În cazul în care datele sunt protejate de privilegii sau imunități ori de norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă în temeiul dreptului intern al statului de executare sau în cazul în care divulgarea datelor ar putea afecta interesele fundamentale ale statului membru respectiv, statul membru emitent ar trebui să se asigure că aceste considerente sunt luate în considerare ca și când ar fi fost prevăzute de propriul drept intern, pentru ca ele să aibă efect. Dacă, de exemplu, astfel de privilegii sau imunități nu sunt acordate în temeiul dreptului intern al statului membru emitent, protecția ar trebui adaptată, în măsura posibilului, astfel încât să aproximeze privilegiul sau imunitatea echivalentă cea mai asemănătoare în temeiul dreptului intern al statului emitent, luându-se în considerare obiectivele și interesele urmărite de protecția specifică și efectele produse de aceasta. Consecințele juridice generate de propriul drept intern pentru astfel de situații similare ar trebui să se aplice. Pentru a stabili modul în care aceste considerente să fie luate în considerare ca și când ar fi fost prevăzute de dreptul său intern, autoritatea emitentă poate contacta autoritatea notificată pentru informații suplimentare asupra naturii și a efectelor protecției, fie direct, fie prin Rețeaua judiciară în materie penală sau prin intermediul Eurojustului. În timp ce statul membru de executare poate ridica orice tip de obiecții în baza acestor considerente, persoana ale cărei date sunt solicitate nu poate invoca decât propriile drepturi, cum ar fi privilegiile sau imunitățile, și nu poate ridica obiecții în baza unui interes fundamental al statului de executare.

(35g) În cazul în care un privilegiu sau o imunitate interzic utilizarea datelor, însă aceste drepturi ar putea fi retrase, iar autoritatea emitentă intenționează să utilizeze datele obținute drept probe sau nu retrage ordinul chiar dacă datele nu au fost obținute, cu toate acestea, statul membru emitent ar trebui să aibă posibilitatea de a solicita autorității competente să introducă o cerere de retragere a privilegiului sau de ridicare a imunității.

(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.

(36a) Pentru a asigura protecția deplină a drepturilor fundamentale, validarea ordinului european de divulgare a probelor electronice sau a ordinului european de păstrare a probelor electronice de către autoritățile judiciare ar trebui, în principiu, să fie obținută înainte de emiterea ordinului. Atunci când se caută să se obțină date privind abonații și date privind accesul, se pot face excepții de la acest principiu numai în situații excepționale, în care autoritatea emitentă stabilește în mod valabil că este vorba despre un caz de urgență și în care nu este posibilă obținerea în prealabil în timp util a validării din partea autorității judiciare, în special atunci când autoritatea de validare nu poate fi contactată pentru a se obține validarea, iar amenințarea este atât de iminentă încât trebuie să se acționeze imediat. Cu toate acestea, acest lucru se aplică numai în cazul în care această procedură este prevăzută într-un caz intern similar în temeiul dreptului intern.

(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. **În cazurile în care ordinul european de divulgare sau de păstrare a probelor electronice este adresat prestatorului de servicii ca urmare a nerespectării ordinului de către reprezentantul legal, aceasta poate să fie executat și împotriva prestatorului de servicii.**

(38) Ordinele europene de divulgare și de păstrare a probelor electronice ar trebui transmise **destinatarului** 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 de executare** sau într-o altă limbă oficială pe care prestatorul a declarat că o va accepta.

(39) Autoritatea emitentă competentă **sau autoritatea competentă pentru transmitere** ar trebui să transmită EPOC sau EPOC-PR direct destinatarului **într-un mod sigur și fiabil**, 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 trebuie transmise autorităților **într-un mod sigur și fiabil, care să permită să se stabilească autenticitatea expeditorului și integritatea datelor**, cel târziu în termen de 10 de 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 [...] 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 [...] **ordinului european de divulgare a probelor electronice** 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.

(41a) Destinatarul nu ar trebui să fie obligat să respecte ordinul în cazul unei imposibilități *de facto*, care nu a fost creată de destinatar sau de prestatorul de servicii, dacă acesta este diferit de destinatar, în momentul primirii ordinului. Imposibilitatea *de facto* ar trebui prezumată în cazul în care persoana ale cărei date au fost solicitate nu este client al prestatorului de servicii sau nu poate fi identificată ca atare chiar și după transmiterea unei solicitări de informații suplimentare către autoritatea emitentă ori în cazul în care datele au fost șterse în mod legal înainte de primirea ordinului.

(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. **Mai mult, ei ar trebui** [...] 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) 2016/679[16], [...] **cu excepția situației în care autoritatea emitentă îi solicită să informeze persoana. În aceste cazuri, autoritatea emitentă ar trebui, de asemenea, să furnizeze prestatorului de servicii informațiile necesare despre căile de atac aplicabile, astfel încât acestea să poată fi incluse în informațiile transmise persoanei în cauză. În toate situațiile**, 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 **nu** i s-a solicitat să [...] informeze utilizatorul, **de îndată ce** [...] 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) 2016/680[17]. **Autoritatea emitentă se poate abține de la informarea persoanei ale cărei date privind abonații și cele privind accesul au fost solicitate, în cazul în care este necesar și proporționat pentru a proteja drepturile fundamentale și interesele legitime ale unei alte persoane și mai ales în cazul în care aceste drepturi și interese sunt mai presus de interesul pe care îl are persoana ale cărei date au fost solicitate de a fi informată. O astfel de situație ar putea surveni atunci când ordinul vizează date privind abonații sau date privind accesul aparținând unei terțe persoane, având în vedere prezumția de nevinovăție a persoanei suspectate. În cazul în care identitatea persoanei în cauză nu este cunoscută de autoritatea emitentă, ar trebui efectuate investigații pentru a se stabili identitatea acestei persoane numai în măsura în care acest lucru pare necesar și proporționat în raport cu caracterul invaziv al măsurii și cu efortul asociat stabilirii identității respective.**

(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.

---

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 (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

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 (JO L 119, 4.5.2016, p. 89).

(45) Procedura de executare este o procedură prin care destinatarul poate [...] **invoca motive formale împotriva** executării în baza anumitor motive limitate. Autoritatea de executare poate refuza să recunoască și să execute ordinul pe baza acelorași motive [...] **și, în plus, în cazul în care acestea trebuie avute în vedere în temeiul prezentului regulament**, dacă se aplică imunități și privilegii în temeiul dreptului său intern, **precum și norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă** ori dacă 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.

(45a) Atunci când, într-un caz individual anume, autoritățile competente stabilesc sancțiunile pecuniare corespunzătoare, acestea ar trebui să ia în considerare toate circumstanțele relevante, cum ar fi natura, gravitatea și durata încălcării, dacă aceasta a fost comisă intenționat sau din neglijență, dacă prestatorul de servicii a mai fost tras la răspundere pentru încălcări anterioare similare, precum și capacitatea financiară a prestatorului de servicii considerat răspunzător. În circumstanțe excepționale, respectiva evaluare poate determina autoritatea de executare să decidă să se abțină de la impunerea oricărei sancțiuni pecuniare. Ar trebui acordată o atenție deosebită, în acest sens, microîntreprinderilor care nu respectă un ordin într-un caz de urgență din cauza lipsei de resurse de personal în afara programului normal de lucru, în cazul în care datele sunt transmise fără întârzieri nejustificate.

(46) [...] **P**restatorii de servicii nu ar trebui să fie considerați răspunzători în statele membre pentru prejudicii aduse utilizatorilor lor sau unor terți, care rezultă [...] din respectarea cu bună-credință a unui EPOC sau a unui EPOC-PR. **Răspunderea asigurării legalității ordinului, în special sub aspectul caracterului necesar și proporționat al acestuia, ar trebui să revină autorității emitente.**

(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, 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 **poate** [...] să se bazeze, dacă este necesar, pe o consultanță specializată externă adecvată, de exemplu [...] cu privire la interpretarea 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 **legislației** țării terțe **se aplică și, în caz afirmativ, dacă acestea** interzic divulgarea datelor în cauză [...]. În cazul în care instanța concluzionează că dispozițiile contradictorii ale țării terțe interzic divulgarea datelor în cauză, [...] [...] [...] instanța ar trebui să decidă dacă să se mențină sau nu ordinul european de divulgare a probelor electronice luând în considerare o serie de elemente care urmăresc să stabilească soliditatea legăturii cu oricare 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. **În momentul efectuării evaluării, ar trebui acordată o importanță și o greutate deosebite protecției drepturilor fundamentale prin dispozițiile țării terțe, precum și altor interese fundamentale, cum ar fi interesele în materie de securitate națională ale țării terțe, precum și gradului de legătură a cauzei penale cu oricare dintre cele două jurisdicții.**

(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 ***putea fi*** exercitat[...] **ori de câte ori datele obținute sunt utilizate în cursul** procedurilor penale **împotriva acestora**. 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, **ale căror date au fost solicitate, dar** 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 cursul procedurii de executare, autoritatea de executare **poate refuza recunoașterea și executarea unui ordin european de divulgare sau de păstrare a probelor electronice dintr-un număr limitat de motive**. […]

(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.

(56a) Transmiterea și transferul, precum și utilizarea probelor electronice obținute prin intermediul unui ordin european de divulgare a probelor electronice în cadrul altor proceduri penale și pentru un alt scop decât cel pentru care a fost emis ordinul ar trebui să fie restricționate, în special la infracțiunile pentru care autoritatea emitentă ar fi putut, de asemenea, emite un ordin european de divulgare a probelor electronice. În plus, utilizarea, transmiterea sau transferul de probe electronice ar trebui să fie posibile numai în cazul în care datele sunt necesare pentru a preîntâmpina o amenințare imediată și gravă la adresa securității publice a statului membru respectiv sau a țării terțe respective, precum și la adresa intereselor lor esențiale. Mai mult, transferul internațional de probe electronice este supus condițiilor stabilite în capitolul V din Directiva (UE) 2016/680. În cazurile în care datele cu caracter personal obținute sunt utilizate în scopul preîntâmpinării unei amenințări imediate și grave la adresa securității publice a statului membru respectiv sau a țării terțe respective, precum și la adresa intereselor lor esențiale, iar existența unei astfel de amenințări ar putea să nu conducă la lansarea unor anchete penale, ar trebui să se aplice Regulamentul (UE) 2016/679.

(56b) Atunci când se face o declarație referitoare la regimul lingvistic, statele membre sunt încurajate să includă cel puțin o limbă în plus față de limba oficială (limbile oficiale).

(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 cursul 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 legiferare[18]. În special, pentru a asigura participarea 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

(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 Consiliului[19] în vederea obținerii de probe electronice. Autoritățile statelor membre ar trebui să aleagă instrumentul cel mai adaptat [...] **cazului în speță**; 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 enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestor obiective.

[18] JO L 123, 12.5.2016, p. 1.

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

(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, [...] Irlanda și-a notificat dorința de a participa la adoptarea și aplicarea prezentului regulament [...] fără a aduce atingere articolului 4 din protocol, Regatul Unit [...] nu participă la adoptarea prezentului regulament și 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 Consiliului[20] și a emis un aviz la data de (…)[21],

---

[20] 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).

[21] JO C , , p. .

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul 1: Obiect, definiții și domeniu de aplicare

Articolul 1
Obiectul

(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, **cu excepția serviciilor financiare menționate la articolul 2 alineatul (2) litera (b) din Directiva 2006/123/CE**:

   (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 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;

(c) **alte** servicii ale societății informaționale, astfel cum sunt definite la articolul 1 punctul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului[22], **care presupun:**

– **capacitatea utilizatorilor de a comunica între ei;** sau

– de a procesa ori stoca date în numele utilizatorilor beneficiari ai serviciului [...][23]

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, **în baza unor criterii faptice specifice**, cu statul sau statele membre menționate la litera (a);

5. „sediu” **sau „a-și avea sediul”** înseamnă [...] exercitarea efectivă a unei activități economice pentru o perioadă nedeterminată prin intermediul unei infrastructuri stabile de unde este exercitată activitatea de prestare de servicii [...] sau 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;

---

22 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).

23 Finlanda, Letonia și Luxemburgul au exprimat o rezervă, fiind de părere că autoritățile publice nu ar trebui să fie obligate să respecte un ordin de divulgare sau de păstrare a probelor electronice (Finlanda) și că definiția este încă prea vagă și lipsită de securitate juridică (Luxemburg); privind necesitatea de a examina mai în detaliu definiția, mai ales în legătură cu propunerea de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul colectării de probe în cadrul procedurilor penale (Letonia).

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 ([...]**c**) 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 ([...]**c**) 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 abonații, 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 Consiliului[24];

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;

[24] 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).

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 transmit, **dacă este necesar**, 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 Consiliului[25].

Articolul 3
Domeniul de aplicare

(1) Prezentul regulament se aplică prestatorilor de servicii care oferă servicii în Uniune.

(1a) Regulamentul nu se aplică procedurilor inițiate de autoritatea emitentă cu scopul de a oferi asistență juridică reciprocă unui alt stat membru sau unei țări terțe.

(2) Ordinele europene de divulgare a probelor electronice și ordinele [...] europene de **păstrare** a probelor electronice pot fi emise doar pentru proceduri penale [...] **și pentru executarea unei pedepse sau a unei măsuri de siguranță privative de libertate care nu a fost pronunțată/luată *in absentia* în cazul în care persoana condamnată s-a sustras justiției**.[...] 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[26].

(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).

---

25 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).

26 Republica Cehă, Finlanda, Letonia și Germania au formulat o rezervă cu privire la extinderea domeniului de aplicare în ceea ce privește persoanele condamnate care s-au sustras justiției; inclusiv pentru dispozițiile paralele de la articolul 5 alineatul (3) și de la articolul 6 alineatul (2).

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.

(5) În cazurile de urgență a căror existență a fost stabilită în mod valabil, autoritățile menționate la alineatul 1 litera (b) și la alineatul (3) litera (b) pot emite respectivul ordin de divulgare a datelor privind abonații și a celor privind accesul fără o validare prealabilă dacă validarea nu poate fi obținută la timp și dacă aceste autorități ar putea emite ordinul fără validare într-un caz similar la nivel național. Autoritatea emitentă solicită validarea ex-post, fără întârzieri nejustificate, cel târziu în termen de 48 de ore. În cazul în care validarea ex-post nu este acordată, autoritatea emitentă retrage imediat ordinul și, în conformitate cu dreptul său intern, fie șterge datele care au fost obținute, fie se asigură că datele nu se utilizează drept probe[27].

(6) Fiecare stat membru poate desemna una sau mai multe autorități centrale responsabile de transmiterea administrativă a certificatelor, a ordinelor și a notificărilor, de primirea datelor și a notificărilor, precum și de transmiterea altor tipuri de corespondență oficială referitoare la certificate sau la ordine.

[27] Grecia și Luxemburgul au formulat o rezervă cu privire la posibilitatea de validare ex-post.

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 **și pentru executarea unei pedepse sau a unei măsuri de siguranță privative de libertate cu o durată de cel puțin patru luni**.

(4) Ordinele europene de divulgare a probelor electronice care vizează date privind operațiile sau date referitoare la conținut pot fi emise doar[28]:

(a) pentru infracțiuni care se pedepsesc în statul emitent cu o pedeapsă cu închisoarea a cărei limită superioară este de cel puțin trei ani[29] 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 Consiliului[30];

– infracțiunile definite la articolele 3-7 din Directiva 2011/92/UE a Parlamentului European și a Consiliului[31];

– infracțiunile definite la articolele 3-8 din Directiva 2013/40/UE a Parlamentului European și a Consiliului;

---

28 Finlanda și Slovenia ar prefera o abordare de tip listă.

29 Ciprul a formulat o rezervă cu privire la condițiile de emitere a unui ordin european de divulgare a probelor electronice pentru infracțiunile care se pedepsesc cu o pedeapsă cu o durată mai mică de cinci ani;

30 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).

31 Directiva 2011/93/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).

(c) pentru infracțiunile definite la articolele 3-12 și 14 din Directiva (UE) 2017/541 a Parlamentului European și a Consiliului[32].

(d) pentru executarea unei pedepse sau a unei măsuri de siguranță privative de libertate cu o durată de cel puțin patru luni impuse pentru infracțiunile prevăzute la literele (a), (b) și (c) ale prezentului alineat;

(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) **utilizatorul, cu excepția cazului în care unicul scop al ordinului este de a identifica utilizatorul, sau orice alt identificator unic, cum ar fi numele de utilizator, numărul de identificare sau denumirea contului, pentru a stabili datele care sunt solicitate** [...];

(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.

---

[32] 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).

(6a) **Un ordin european de divulgare a probelor electronice prin care se solicită date stocate sau prelucrate ca parte a unei infrastructuri furnizate de un prestator de servicii unei autorități publice nu poate fi emis decât dacă autoritatea publică pentru care sunt stocate sau prelucrate datele se află în statul emitent.**

(7) [...] **În cazurile în care ordinul se referă la date privind operațiile și autoritatea emitentă** are [...] **motive întemeiate** să considere că [...]

(a) **persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul statului emitent și că**

(b) datele solicitate sunt protejate prin imunitățile și privilegiile acordate în temeiul legislației [...] statului **de executare** [...] sau **fac obiectul, în statul membru respectiv, normelor privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă** sau că divulgarea lor poate afecta interesele fundamentale ale statului **de executare** [...], cum ar fi securitatea și apărarea națională, autoritatea emitentă [...] solicită clarificări **referitoare la circumstanțele menționate la litera (b)** înainte de a emite ordinul european de divulgare a probelor electronice, inclusiv prin consultarea autorităților competente ale statului **de executare** [...] [...], fie direct, fie prin intermediul Eurojustului sau al Rețelei judiciare europene. În cazul în care autoritatea emitentă constată că datele solicitate [...] privind operațiile [...] **sunt** protejate prin astfel de imunități și privilegii **sau prin norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă** sau că divulgarea lor ar afecta interesele fundamentale ale celuilalt stat membru, **cum ar fi securitatea și apărarea națională**, aceasta **ține seama de circumstanțele respective ca și cum ar fi fost prevăzute în dreptul său intern și** nu emite ordinul european de divulgare a probelor electronice **sau îl adaptează, atunci când este necesar, pentru a da efect respectivelor motive**[33].

(8) **Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a statului de executare, autoritatea emitentă poate solicita autorității de executare să contacteze autoritatea competentă pentru a-i solicita să își exercite această competență fără întârziere. Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a unui alt stat membru sau a unei țări terțe sau de o organizație internațională, autoritatea emitentă poate solicita autorității în cauză să își exercite această competență.**

---

[33] Germania și Republica Cehă pledează pentru adăugarea datelor referitoare la conținut. În plus, Germania a solicitat includerea unei clauze privind drepturile fundamentale atât la prezenta dispoziție, cât și la articolul 12a. Ungaria a formulat o rezervă de fond motivată de logica dispoziției: în opinia acestei delegații, în cazul în care există motive întemeiate de a se considera că refuzul este previzibil, ar trebui să fie posibilă o consultare prealabilă în general, inclusiv pentru dispozițiile paralele de la articolul 5 alineatul (7), articolul 7a, articolul 9 alineatul (5), articolul 12a și articolul 14.

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. **Articolul 5 alineatul (6a) se aplică *mutatis mutandis*.**

(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 **și pentru executarea unei pedepse sau a unei măsuri de siguranță privative de libertate cu o durată de cel puțin patru luni**.

(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) [...] **utilizatorul,** cu excepția cazului în care unicul scop al ordinului este de a identifica [...] **utilizatorul, sau orice alt identificator unic, cum ar fi numele de utilizator, numărul de identificare sau denumirea contului, pentru a stabili datele care sunt solicitate;**

(d) categoria de date care trebuie păstrate (date privind abonații, date privind accesul, date privind operațiile 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 [...], 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 de ordin european de divulgare a probelor electronice într-un caz de urgență în temeiul articolului 9 alineatul (2), **ordinul european de divulgare a probelor electronice** [...] 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 7a
Notificarea[34]

(1) În cazurile în care ordinul european de divulgare a probelor electronice vizează date referitoare la conținut, iar autoritatea emitentă are motive întemeiate să considere că persoana ale cărei date sunt solicitate nu își are reședința pe propriul său teritoriu, autoritatea emitentă transmite o copie a EPOC autorității competente din statul de executare, în același timp cu transmiterea EPOC destinatarului în conformitate cu articolul 7.

(2) **Autoritatea notificată poate informa cât de curând posibil autoritatea emitentă în legătură cu orice circumstanță în temeiul articolului 5 alineatul (7) litera (b) și depune eforturi pentru a face acest lucru în termen de 10 zile. Autoritatea emitentă ține seama de circumstanțele respective ca și cum ar fi fost prevăzute în dreptul său intern și retrage sau adaptează ordinul, atunci când este necesar, pentru a da efect respectivelor motive, dacă datele nu au fost deja furnizate. În caz de retragere, autoritatea emitentă informează imediat destinatarul.**

(3) Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a statului de executare, autoritatea emitentă poate solicita autorității notificate să contacteze autoritatea competentă pentru a-i solicita să își exercite această competență fără întârziere. Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a unui alt stat membru sau a unei țări terțe sau de o organizație internațională, autoritatea emitentă poate solicita autorității în cauză să își exercite această competență.

(4) Notificarea nu are efect suspensiv asupra obligațiilor destinatarului în temeiul prezentului regulament.

---

34 Republica Cehă, Finlanda, Germania, Grecia, Ungaria și Letonia au formulat o rezervă cu privire la procedura de notificare, pledând pentru o procedură care să aibă un efect mai important și care să includă și datele privind operațiile și o clauză privind drepturile fundamentale, și anume o clauză care să prevadă motivele de refuz de care autoritatea care primește notificarea să se poată prevala; de asemenea, ar trebui inversată norma privind situațiile care ar putea fi considerate drept „caz la nivel național”; în cele din urmă, Germania pledează pentru transmiterea ordinului, și nu a certificatului, în timp ce Republica Cehă este de părere că ar trebui transmise atât ordinul, cât și certificatul.
Belgia, Bulgaria, Estonia, Franța, Irlanda, Italia, Polonia, Portugalia și Spania au formulat o rezervă cu privire la procedura de notificare și dispozițiile legate de introducerea unei proceduri de notificare, în special articolul 5 alineatul (7), articolele 9, 12a și 14, precum și considerentele conexe, precizând că ar fi preferabilă propunerea Comisiei, care nu conține notificarea; Belgia, Luxemburgul, Irlanda, Slovenia și Polonia ar prefera, dacă nu se poate renunța la notificare, o notificare a statului membru în care își are reședința persoana ale cărei date sunt solicitate.

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 se [...] transmit de către **autoritatea emitentă sau din partea acesteia într-un mod sigur și fiabil, care să permită** [...] destinatarului să **realizeze o înregistrare scrisă și să** stabilească [...] autenticitatea [...] **certificatului**.

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, **într-un mod sigur și fiabil, care să permită stabilirea autenticității și integrității**, 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[35].

(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 cinci 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 [...] dintr-o imposibilitate *de facto* **cauzată de circumstanțe necreate de destinatar sau de prestatorul de servicii în momentul primirii ordinului** [...], destinatarul contactează autoritatea emitentă menționată în EPOC fără întârzieri nejustificate, explicând motivele prin intermediul formularului prevăzut în anexa III. […]

35 Germania propune, cel puțin, să se adauge un considerent nou prin care să se solicite Comisiei și statelor membre să depună eforturi pentru a institui cât de curând posibil canale electronice de comunicare, securizate, care să permită stabilirea autenticității și a integrității.

(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 revizuiește 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.

[…][36]

(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.

[36] Ungaria a formulat o rezervă în legătură cu eliminarea.

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 cinci zile. La rândul său, destinatarul 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 [...] dintr-o imposibilitate *de facto* **cauzată de circumstanțe necreate de destinatar sau de prestatorul de servicii în momentul primirii ordinului** [...], **destinatarul** [...] **informează** autoritatea emitentă menționată în EPOC-PR fără întârzieri nejustificate, explicând motivele prin intermediul formularului prevăzut în anexa III. […]

(6) În toate cazurile în care destinatarul nu păstrează informațiile solicitate, din alte motive [...], 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[37]

(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 [...] se abțin de la a informa persoana ale cărei date sunt solicitate, pentru **a evita** [...] să obstrucționeze procedurile penale relevante. **Ei nu informează persoana ale cărei date** [...] **sunt solicitate decât în cazul în care acest lucru este solicitat în mod explicit de autoritatea emitentă. În acest caz, autoritatea emitentă îi furnizează destinatarului sau prestatorului de servicii, dacă este diferit de destinatar, și informații în temeiul alineatului 4 de la prezentul articol.**

(2) În cazul în care autoritatea emitentă **nu** a solicitat [...] **prestatorului de servicii să** informeze [...] persoana ale cărei date **au fost** [...] solicitate **în conformitate cu alineatul (1)**, autoritatea emitentă informează această [...] persoană [...]. [...] **Autoritatea emitentă poate amâna informarea persoanei ale cărei date sunt solicitate atât timp cât amânarea constituie o măsură necesară și proporționată** [...] pentru a se evita obstrucționarea [...] procedurilor penale [...].

(3) **Autoritatea emitentă se poate abține de la informarea persoanei ale cărei date privind abonații și cele privind accesul au fost solicitate, în cazul în care este necesar și proporționat pentru a proteja drepturile fundamentale și interesele legitime ale unei alte persoane și mai ales în cazul în care aceste drepturi și interese sunt mai presus de interesul pe care îl are persoana ale cărei date au fost solicitate de a fi informată.** […]

(4) Se includ și informații despre căile de atac disponibile în temeiul articolului 17.

---

37 Finlanda și Germania au formulat rezerve, fiind de părere că sunt necesare mai multe detalii (dispoziții privind limba, ajutorul juridic, informații detaliate despre căile de atac etc.); în plus, Germania afirmă că ar trebui informate persoanele în cauză (și nu doar persoana ale cărei date sunt solicitate).

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. **Statele membre informează Comisia cu privire la normele de rambursare, iar aceasta le publică.**

Articolul **12a** […]
[…] **Limitări ale utilizării datelor obținute**

(1) [...] **În cazul în care persoana ale cărei date sunt solicitate nu își are reședința pe teritoriul statului emitent și** datele privind operațiile sau datele privind conținutul **au fost** obținute prin ordinul european de divulgare a probelor electronice, **iar autoritatea emitentă primește informații care arată că respectivele date** [...] **sunt** protejate prin imunități sau privilegii acordate în temeiul legislației [...] **statului de executare** [...] sau **fac obiectul, în statul de executare, unor norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă** sau [...] **dacă, potrivit acelui stat membru**, **divulgarea respectivelor date ar aduce atingere intereselor sale fundamentale** precum securitatea și apărarea națională, [...] **autoritățile competente** din statul emitent se asigură, în cursul procedurilor penale [...], că aceste motive sunt luate în considerare ca și cum ar fi fost prevăzute în dreptul lor intern [...]. [...] **Autoritățile competente** pot consulta autoritățile din statul membru relevant, Rețeaua judiciară europeană în materie penală sau Eurojustul.

(2) **Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a statului de executare, autoritatea competentă din statul emitent poate solicita autorității de executare sau autorității notificate să contacteze autoritatea competentă a statului de executare pentru a-i solicita să își exercite această competență fără întârziere. Atunci când ridicarea privilegiului sau a imunității depinde de o autoritate a unui alt stat membru sau a unei țări terțe sau de o organizație internațională, autoritatea competentă din statul emitent poate solicita autorității în cauză să își exercite această competență.**

Articolul 12b
Principiul specialității

(1) Probele electronice nu se utilizează în scopul altor proceduri decât cele pentru care au fost obținute în conformitate cu prezentul regulament, cu excepția:

(a) scopului procedurilor pentru care s-ar fi putut emite un ordin european de divulgare a probelor electronice în conformitate cu articolul 5 alineatele (3) și (4); sau

(b) obiectivului de prevenire a unei amenințări imediate și grave pentru ordinea publică a statului emitent sau pentru interesele fundamentale ale acestuia.

(2) Probele electronice obținute în conformitate cu prezentul regulament pot fi transmise unui alt stat membru numai:

(a) în scopul procedurilor pentru care s-ar fi putut emite un ordin european de divulgare a probelor electronice în conformitate cu articolul 5 alineatele (3) și (4); sau

(b) pentru prevenirea unei amenințări imediate și grave pentru ordinea publică a statului membru respectiv sau pentru interesele fundamentale ale acestuia.

(3) **Probele electronice obținute în conformitate cu prezentul regulament pot fi transferate unei țări terțe sau unei organizații internaționale numai în conformitate cu condițiile prevăzute la alineatul (2) literele (a) și (b) ale prezentului articol și la capitolul V din Directiva (UE) 2016/680.**

Capitolul 3: Sancțiuni și executare

Articolul 13
Sancțiuni[38]

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 **alineatul (1)** din prezentul regulament și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Statele membre notifică normele respective Comisiei fără întârziere și îi comunică acesteia, fără întârziere, orice modificări ulterioare privind aceste norme.

Statele membre se asigură că sancțiunile pecuniare prevăzute [...] **sunt** eficace, proporționale și cu efect de descurajare.

Statele membre se asigură că se pot impune sancțiuni pecuniare de până la 2 % din cifra de afaceri anuală totală la nivel mondial a prestatorului de servicii aferentă exercițiului financiar precedent.

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 alt document însoțitor într-una dintre [...] limbile [...] **acceptate de** statul membru respectiv și informează destinatarul cu privire la transfer.

(2) În momentul primirii, autoritatea de executare recunoaște fără formalități suplimentare **și ia măsurile necesare pentru executarea**

(a) unui ordin european de divulgare a probelor electronice**, cu excepția cazului în care autoritatea de executare consideră că se aplică unul din motivele prevăzute la alineatul (4)**, sau

(b) **unui** ordin european de păstrare a probelor electronice, [...] cu excepția cazului în care autoritatea de executare consideră că se aplică unul din motivele prevăzute la alineatul [...] (5) [...].

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.

---

38 Finlanda, Germania și Letonia au formulat o rezervă cu privire la armonizarea sancțiunilor.

(2a) Articolul 5 alineatul (8) se aplică *mutatis mutandis*.

(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 alineatul [...] (4) **literele (a)-(e) sau la alineatul** (5), precum și cu privire la sancțiunile aplicabile în caz de neconformare și stabilește un termen-limită pentru conformare sau pentru opoziție.

(4) [...] **Recunoașterea sau** executarea ordinului european de divulgare a probelor electronice **nu pot fi refuzate decât** pe baza următoarelor 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 imposibilității *de facto* [...] 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) [...] **se aplică unul din motivele menționate la articolul 12a alineatul (1)**[39].

(5) [...] **Recunoașterea sau** executarea ordinului european de păstrare a probelor electronice **nu pot fi refuzate decât** pe baza următoarelor 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 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) […]

---

39 Republica Cehă, Finlanda, Ungaria, Germania și Letonia au formulat o rezervă cu privire la eliminarea articolului 14 alineatul (4) litera (f) și a alineatului (5), litera (e), susținând că eliminarea nu ar putea fi sprijinită decât dacă s-ar adăuga, la articolul 5, la articolul 7a alineatul (2) și la articolul 12a alineatul (1), o clauză privind drepturile fundamentale, precum și privind respectarea normelor constituționale naționale.

(6) În cazul unei obiecții formulate de destinatar **în temeiul alineatului (4) literele (a)-(e) și al alineatului (5)**, 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 printr-o imunitate sau printr-un privilegiu în temeiul dreptului său intern **sau prin norme privind determinarea sau limitarea răspunderii penale legate de libertatea presei și de libertatea de exprimare în alte mijloace de informare în masă** 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 16
Procedura de control jurisdicțional în cazul unor obligații contradictorii […]

(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 [...], 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 alineatele (5) **și (6)**.

(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. **Ea se depune în termen de cel mult 10 zile de la data la care EPOC i-a fost transmis destinatarului. Termenele se calculează în conformitate cu dreptul intern al autorității emitente.**

(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.

(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 în speță, interzice divulgarea datelor în cauză, instanța competentă decide dacă să mențină sau **să revoce** [...] ordinul. **Această evaluare se bazează** mai ales pe [...] următorii factori, **o importanță deosebită fiind acordată factorilor menționați la literele (a) și (b)**:

(a) interesul protejat de legislația relevantă a țării terțe, inclusiv **drepturile fundamentale și alte interese care împiedică divulgarea datelor** [...]**, în special interesele de securitate națională ale țării terțe;**

(b) gradul de legătură dintre cauza penală pentru care a fost emis ordinul și cele două jurisdicții, astfel cum reiese din analizarea, 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.

(5b) **Instanța judecătorească poate solicita informații din partea autorității competente a țării terțe ținând seama de Directiva 2016/680, mai ales de capitolul V din aceasta, și în măsura în care o astfel de transmitere nu obstrucționează procedurile penale relevante.**

(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[40]

(1) **Fără a aduce atingere altor căi de atac disponibile în conformitate cu dreptul intern, orice** [...] persoană [...] ale cărei date au fost **solicitate** [...] 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 cazul în care persoana respectivă este o persoană suspectată** [...] **sau acuzată, aceasta are dreptul la căi de atac eficiente** în cursul procedurilor penale [...] în cadrul cărora [...] sunt folosite datele. **Aceste căi de atac** nu aduc 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.

[40] Germania a formulat o rezervă, afirmând că fiecare persoană vizată de un ordin ar trebui să aibă dreptul la o cale de atac, și nu doar persoana ale cărei date au fost solicitate; de asemenea, căile de atac ar trebui să fie accesibile și în cadrul unei proceduri penale inițiate împotriva ordinelor de păstrare a probelor electronice.

(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
[…]

[…]

Capitolul 5: Dispoziții finale

Articolul 18a
Regimul lingvistic

Fiecare stat membru indică dacă, în cazul executării, va accepta ca EPOC sau EPOC-PR și/sau un ordin european de divulgare a probelor electronice și un ordin european de păstrare a probelor electronice să fie transmise în altă limbă sau în alte limbi decât limba sau limbile oficiale ale acestuia și, în caz afirmativ, în care anume.

Articolul 19
Monitorizare și raportare

(1) Până cel târziu la *[data aplicării prezentului regulament],* 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**, în măsura posibilului**:

(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**, validare ex-post**);

(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;

(f) **numărul de cazuri în care nu s-a acordat validarea ex-post.**

(3) Prestatorii de servicii pot colecta, păstra și publica statistici. Dacă astfel de date au fost colectate, ele pot fi trimise Comisiei până la 31 martie pentru anul calendaristic precedent și pot include, în măsura în care este posibil:

(a) numărul de EPOC și de EPOC-PR primite, în funcție de tipul de date solicitate, de stat membru și de situație (cazuri de urgență sau nu);

(b) numărul de EPOC executate și neexecutate, în funcție de tipul de date solicitate, de stat membru și de situație (cazuri de urgență sau nu);

(c) pentru EPOC executate, durata medie de obținere a datelor solicitate din momentul în care a fost primit EPOC până în momentul furnizării, în funcție de tipul de date solicitate, de stat membru și de situație (cazuri de urgență sau nu);

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) Competența de a adopta acte delegate este conferită Comisiei 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 din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere 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 2016[41].

(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.

[41] JO L 123, 12.5.2016, p. 13.

Articolul 22
Notificări

(1) Până la [*data aplicării prezentului regulament*], fiecare stat membru notifică Comisiei următoarele:

(a) autoritățile care, în conformitate cu dreptul lor intern, sunt competente în temeiul articolului 4 să emită [...], să valideze, **să transmită și/sau să primească** ordine europene de divulgare a probelor electronice și ordine europene de păstrare a probelor electronice **sau notificări despre acestea**;

(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 articolul [...] 16;

(d) **limbile acceptate pentru transmiterea EPOC sau a EPOC-PR și/sau a unui ordin european de divulgare a probelor electronice și a unui ordin european de păstrare a probelor electronice, în cazul executării în conformitate cu articolul 18a.**

(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 Consiliului[42].

Articolul 23
Relația cu […] ***alte instrumente, acorduri și înțelegeri***

Prezentul regulament nu aduce atingere altor instrumente, acorduri și înțelegeri ale UE și internaționale privind [...] colectarea de probe care ar intra, de asemenea, sub incidența prezentului regulament.

[42] 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 [*cinci 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 *[[...] **24** de 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 Strasbourg,

Pentru Parlamentul European *Pentru Consiliu*

Președintele *Președintele*