DOI: https://www.doi.org/10.31178/AUBD-FJ.2026.2.8

Forum Juridic nr. 1 / 2026

ANALELE UNIVERSITĂȚII DIN BUCUREȘTI - SERIA DREPT

Ordinul european de divulgare și de păstrare a probelor electronice. Regulamentul (UE) 2023/1543 și limitele asimilării ordinelor europene cu procedeele probatorii din Codul de procedură penală. Observații pe marginea proiectului de lege nr. L272/2026

Conf. univ. dr. Radu Slăvoiu[1]
Universitatea „Nicolae Titulescu" din București – Facultatea de Drept
Lect. univ. dr. George Zlati[2]
Universitatea „1 Decembrie 1918" Alba Iulia – Facultatea de Drept și Științe Sociale

Rezumat: *Articolul analizează ordinele europene de divulgare și de păstrare a probelor electronice, reglementate prin Regulamentul (UE) 2023/1543, aplicabil de la 18 august 2026, și proiectul de lege L272/2026 privind punerea lui în aplicare în dreptul intern. Sunt examinate chestiuni pe care Regulamentul le lasă deschise, de la elementul de extraneitate până la regimul cheii criptografice aflate în controlul furnizorului. Cea mai mare relevanță practică o are necorespondența dintre clasificarea datelor din Regulament și cea din dreptul intern, unde datele solicitate exclusiv în scopul identificării utilizatorului, tratate ca fiind puțin intruzive, sunt date de trafic. Concluzia autorilor este că definirea ordinului european prin actul procesual intern transferă asupra unui instrument al dreptului Uniunii limitele procedeelor probatorii naționale, de unde poate rezulta o tensiune cu condiția cauzei interne similare și un risc de nelegalitate care se manifestă abia ex post.*

Cuvinte cheie: *probe electronice; ordin european de divulgare; ordin european de păstrare; Regulamentul (UE) 2023/1543; proiectul de lege L272/2026; cauză internă similară; date de trafic; procedee probatorii.*

European Production Orders and European Preservation Orders for Electronic Evidence Regulation (EU) 2023/1543 and the Limits of Classifying European Orders under the Evidence-Gathering Procedures of the Romanian Code of Criminal Procedure. Comments on Draft Law No. L272/2026

Abstract: *The article examines the European Production Orders and European Preservation Orders for electronic evidence, governed by Regulation (EU) 2023/1543, applicable from 18 August 2026, and draft law L272/2026 on its implementation in Romanian law. It addresses questions the Regulation leaves open, from the cross-border element to the regime of the encryption key held by the provider. The most practically relevant issue is the inconsistency between the data categories of the Regulation and those of Romanian law, where data requested for the sole purpose of identifying the user, treated as barely intrusive, are traffic data. The authors conclude that defining the European order through the domestic*

[1] E-mail: radu.slavoiu@univnt.ro.
[2] E-mail: george.zlati@uab.ro.

procedural act transfers the limits of national evidence-gathering procedures onto an instrument of Union law, from which a tension with the condition of a similar domestic case may follow, along with a risk of illegality that surfaces only ex post.

Keywords: *electronic evidence; European Production Order; European Preservation Order; Regulation (EU) 2023/1543; draft law L272/2026; similar domestic case; traffic data; evidence-gathering procedures.*

I. INTRODUCERE

Începând cu data de 18 august 2026 se aplică Regulamentul (UE) 2023/1543 privind ordinele europene de divulgare a probelor electronice și ordinele europene de păstrare a probelor electronice[3] în cadrul procedurilor penale și pentru executarea pedepselor privative de libertate în urma unor proceduri penale [art. 34 alin. (2) din Regulament].

Punerea în aplicare a Regulamentului la nivel național face obiectul unui proiect de Lege adoptat de Senat, înregistrat cu nr. L272/2026[4] (în continuare, proiectul de Lege) și aflat în dezbatere la Camera Deputaților. Precizăm *ab initio* că Regulamentul privind probele electronice [în continuare, Regulamentul] este parte a unui pachet legislativ, alături de Directiva (UE) 2023/1544[5], cu termen de transpunere la 18 februarie 2026 [art. 7 alin. (1) din Directivă]. Din datele existente la acest moment, rezultă că termenul nu a fost însă respectat de majoritatea statelor membre[6].

Directiva operează, de altfel, cu două termene distincte:

a) Termenul pentru transpunerea Directivei, scadent la 18 februarie 2026;

b) Termenul pentru furnizorii de servicii, art. 3 alin. (6) prevăzând că cei care ofereau servicii în Uniune la 18 februarie 2026 au obligația pozitivă de a-și desemna un sediu sau de a numi reprezentanți legali până la 18 august 2026, iar cei care încep să ofere servicii ulterior, în termen de șase luni de la data la care încep să le ofere.

---

[3] Traducerea în limba română a Regulamentului ridică ea însăși o problemă la nivel terminologic. Astfel, versiunea în limba engleză folosește „European Production Order", în timp ce versiunea în limba română se raportează la noțiunea de „ordin de divulgare", deși „divulgare" este echivalentul rezervat în dreptul Uniunii pentru „disclosure", așa cum rezultă din cel de al doilea Protocol adițional la Convenția privind criminalitatea informatică. De asemenea, „European Preservation Order" a fost tradus ca fiind „ordin de păstrare", deși art. 154 C.pr.pen. reglementează „conservarea datelor informatice", iar chiar considerentul (9) al versiunii în limba română a Regulamentului se raportează la „conservarea și divulgarea probelor electronice", aceasta fiind de altfel singura trimitere la termenul de „conservare".

[4] Proiectul de lege este înregistrat la Senat cu nr. L272/2026, a se vedea în acest sens https://www.senat.ro/legis/lista.aspx?nr_cls=L272&an_cls=2026. Analiza din prezentul articol are în vedere forma adoptată de Senat în ședința din 8 iunie 2026, disponibilă la https://www.senat.ro/legis/PDF/2026/26L272FS.PDF, aflată în dezbatere la Camera Deputaților.

[5] Directiva (UE) 2023/1544 a Parlamentului European și a Consiliului din 12 iulie 2023 de stabilire a unor norme armonizate privind desemnarea sediilor desemnate și numirea reprezentanților legali în scopul obținerii de probe electronice în cadrul procedurilor penale.

[6] Potrivit evidenței măsurilor naționale de transpunere comunicate Comisiei, au notificat asemenea măsuri zece state membre: Cehia, Danemarca, Germania, Estonia, Croația, Italia, Lituania, Slovacia, Finlanda și Suedia (https://eur-lex.europa.eu/legal-content/RO/NIM/?uri=CELEX:32023L1544, consultat la 30 iulie 2026). România nu figurează printre acestea, proiectul de lege de transpunere, distinct de cel analizat aici, fiind adoptat de Guvern la 4 mai 2026 (https://gov.ro/ro/guvernul/sedinte-guvern/informatie-de-presa-privind-actele-normative-adoptate-in-edinta-extraordinara-a-guvernului-romaniei-din-4-mai-2026).

Regulamentul are în vedere cadrul normativ aplicabil cu privire la emiterea ordinelor de divulgare [în eng., production order] și de păstrare [în eng., preservation order], adică ce date pot fi obținute ori conservate, de la cine (persoana vizată de ordin), de către cine (emitentul ordinului) și în ce condiții (în funcție de natura datelor). În schimb, Directiva reglementează obligația pozitivă a furnizorilor de servicii care oferă servicii în Uniune de a desemna un sediu ori de a numi un reprezentant legal[7] căruia ordinele să îi fie adresate, împreună cu regimul sancționator aplicabil pentru neîndeplinirea acestor obligații pozitive.[8]

Ordinul se transmite direct destinatarului, fără intermedierea vreunei autorități din statul membru în care acesta se află. Autoritatea emitentă nu îl trimite, așadar, unui procuror ori unei instanțe din acel stat spre a fi retransmis, ci se adresează nemijlocit sediului desemnat sau reprezentantului legal [art. 7 alin. (1) din Regulament]. Ceea ce ajunge la destinatar nu este însă ordinul însuși, ci un certificat, respectiv EPOC în cazul ordinului de divulgare și EPOC-PR în cazul ordinului de păstrare, completat și semnat de autoritatea emitentă sau, după caz, de autoritatea de validare, pe formularul din anexa I ori din anexa II [art. 9 alin. (1) din Regulament].

Certificatul nu reproduce conținutul ordinului, ci doar preia o parte a informațiilor. Autoritatea de executare din statul destinatarului este notificată din oficiu doar atunci când notificarea este obligatorie, adică în cazul ordinului de divulgare a datelor privind traficul, cu excepția celor solicitate exclusiv în scopul identificării utilizatorului, și a datelor referitoare la conținut, ipoteză în care EPOC îi este transmis în același timp cu transmiterea către destinatar [art. 8 alin. (1) din Regulament], notificarea având, în afara cazurilor de urgență, efect suspensiv asupra obligațiilor destinatarului [art. 8 alin. (4)].

Destinatarul, adică sediul desemnat sau reprezentantul legal, nu există decât prin transpunerea Directivei, iar statul care impune obligația nu este neapărat cel în care destinatarul se situează geografic. Potrivit art. 3 alin. (1), obligația este asigurată de statul membru în care furnizorul este stabilit, atunci când acesta are personalitate juridică și este stabilit în Uniune [lit. a)], respectiv de fiecare stat membru pe teritoriul căruia furnizorul oferă servicii, atunci când el nu este stabilit în Uniune ori este stabilit într-un stat membru care nu participă la instrumentele prevăzute la art. 1 alin. (2) [lit. b) și c)]. În aceste din urmă ipoteze, numirea se face într-un stat membru, ales de furnizor dintre cele în care își oferă serviciile [art. 3 alin. (2) lit. a)]. În lipsa transpunerii, Regulamentul rămâne aplicabil, însă fără destinatar căruia certificatul să îi fie comunicat, fără autoritatea centrală prevăzută la art. 6 din Directivă, care primește notificările furnizorilor potrivit art. 4 alin. (1) din aceasta, și fără sancțiunea despre care face vorbire art. 5 din Directivă.

Fiind de aplicare directă, Regulamentul nu se transpune în dreptul intern, însă aceasta nu înseamnă automat și că își poate găsi aplicabilitatea în absența oricărei intervenții a

[7] Directiva definește cele două noțiuni la art. 2. „Sediu desemnat” înseamnă „un sediu cu personalitate juridică desemnat în scris de un furnizor de servicii stabilit într-un stat membru care participă la un instrument juridic menționat la articolul 1 alineatul (2)” [pct. 5], iar „reprezentant legal” înseamnă „o persoană fizică sau juridică numită în scris de un furnizor de servicii care nu este stabilit într-un stat membru care participă” la un asemenea instrument [pct. 6]. Criteriul de distincție este, așadar, stabilirea sau nestabilirea furnizorului într-un stat membru care participă la un instrument juridic menționat la art. 1 alin. (2) din Directivă, nu în Uniune.

[8] Prin art. 5, Directiva creează obligații pozitive în sarcina statelor membre de a adopta normele privind sancțiunile aplicabile în cazul nerespectării dispozițiilor naționale adoptate în temeiul art. 3 și 4, sancțiuni care „trebuie să fie efective, proporționale și cu efect de descurajare”. Statele membre aveau obligația de a notifica aceste norme Comisiei până la 18 februarie 2026 și au obligația de a o informa anual cu privire la furnizorii care nu au respectat normele, la acțiunile de asigurare a respectării acestora și la sancțiunile aplicate.

legiuitorului național. Regulamentul obligă el însuși statele membre să stabilească normele privind sancțiunile pecuniare aplicabile în caz de încălcare a art. 10, art. 11 și a art. 13 alin. (4) [art. 15 alin. (1)], precum și să desemneze, potrivit dreptului lor intern, autoritățile competente să emită, să valideze ori să transmită ordinele, pe cele competente să primească notificările și să execute ordinele și pe cele competente să soluționeze obiecțiile motivate, notificându-le Comisiei până la 18 august 2025 [art. 31 alin. (1) lit. a)-c)].

În acest context, proiectul de Lege prezintă interes tocmai pentru că urmărește asimilarea, sub aspect procesual penal, a ordinelor de păstrare și de divulgare unor procedee probatorii reglementate deja în Codul de procedură penală, clarificând astfel modalitatea în care Regulamentul urmează să își găsească aplicabilitatea practică în dreptul intern.

Adoptarea unei asemenea legi poate însă genera și consecințe neprevăzute, cum ar fi crearea unui cadru normativ paralel și incompatibil, sau cel puțin incoerent, în raport cu prevederile Regulamentului. De altfel, aceasta este principala noastră îngrijorare în momentul de față, existând riscul ca proiectul de Lege să genereze o posibilă confuzie legată de extinderea procedeelor probatorii reglementate în Codul de procedură penală la orice cauză penală.

Prezenta analiză este departe de a fi una exhaustivă. Ceea ce ne propunem este o analiză evaluare critică, dar punctuală, a prevederilor Regulamentului și a proiectului de Lege privind punerea acestuia în aplicare în dreptul intern, cu evidențierea unor aspecte pe care le apreciem ca fiind problematice și care ar putea genera controverse sau probleme de interpretare ori/și de aplicabilitate în viitor.

II. POSIBILE CONTROVERSE DIN PERSPECTIVA REGULAMENTULUI

Înainte de a examina proiectul de Lege, apreciem ca fiind necesară o trecere în revistă a principalelor chestiuni de interpretare pe care le ridică Regulamentul însuși.

II.1. Sfera de aplicabilitate a Regulamentului

Prima chestiune care trebuie lămurită este aceea a situațiilor în care ordinele europene pot fi folosite. Regulamentul nu instituie un procedeu probatoriu de drept comun, ci un mecanism de cooperare, fiind așadar esențială identificarea unui element de extraneitate. Potrivit art. 1 alin. (1), Regulamentul stabilește normele în temeiul cărora o autoritate a unui stat membru poate cere „unui furnizor de servicii care oferă servicii în Uniune și care este stabilit în alt stat membru sau, dacă nu este stabilit, este reprezentat de un reprezentant legal în alt stat membru” să divulge ori să păstreze probe electronice. Definițiile celor două ordine reiau condiția extraneității, arătând că ordinul este adresat sediului desemnat sau reprezentantului legal „atunci când sediul desemnat respectiv sau reprezentantul legal respectiv se află într-un alt stat membru care are obligații în temeiul prezentului regulament” [art. 3 pct. 1 și 2].

Rezultă așadar că un ordin european nu poate fi emis de o autoritate română către un sediu desemnat ori un reprezentant legal aflat în România. Un asemenea act nu ar fi un ordin european, ci o solicitare națională guvernată exclusiv de Codul de procedură penală.

Această concluzie este confirmată de art. 1 alin. (1) din Regulament, ce precizează că actul „nu aduce atingere competențelor autorităților naționale de a se adresa furnizorilor de servicii stabiliți sau reprezentați pe teritoriul lor pentru a se asigura că aceștia respectă

măsurile naționale similare celor menționate în primul paragraf". Directiva statuează în același sens în considerentul (9), potrivit căruia statele membre pot continua să se adreseze furnizorilor stabiliți pe teritoriul lor „pentru situații pur interne", cu mențiunea că, procedând astfel, ele „nu ar trebui să eludeze principiile" care stau la baza ei ori a Regulamentului.

Din această delimitare decurg mai multe consecințe practice. În primul rând, un furnizor din afara Uniunii poate deveni destinatar al ordinului doar dacă și-a numit reprezentantul legal în alt stat membru decât cel emitent, iar locul numirii, ales de furnizor în limitele considerentului (13) al Directivei, ajunge să decidă regimul procedural aplicabil. De asemenea, Regulamentul nu se aplică nici procedurilor inițiate cu scopul de a acorda asistență judiciară unui alt stat membru sau unei țări terțe [art. 2 alin. (4)], deci nu poate servi ca instrument de retransmitere. Cea mai importantă consecință pentru analiza proiectului de Lege este însă aceea că orice interpretare care ar transforma ordinele europene într-un procedeu probatoriu utilizabil într-o situație pur internă este contrară art. 1 alin. (1) și art. 3 pct. 1 și 2 din Regulament.

Delimitarea nu trebuie confundată cu o a doua condiție, distinctă, pe care Regulamentul o impune, anume aceea ca ordinul să poată fi emis „în aceleași condiții într-o cauză internă similară" [art. 5 alin. (2) și art. 6 alin. (3)]. Prima privește domeniul de aplicare, anume în ce măsură mecanismul de cooperare judiciară prevăzut în Regulament își poate găsi aplicabilitatea. A doua privește condițiile de emitere, adică dacă dreptul statului emitent cunoaște la nivel intern un procedeu probatoriu echivalent, disponibil în aceleași condiții.

Într-o asemenea optică, ar trebui concluzionat că Regulamentul nu instituie un regim mai permisiv decât dreptul intern. Interpretând o sintagmă identică regăsită în cuprinsul art. 6 alin. (1) lit. b) din Directiva 2014/41/UE, CJUE a reținut că prin termenii „în aceleași condiții" și „într-o cauză internă similară" se condiționează „stabilirea condițiilor precise necesare pentru emiterea unui ordin european de anchetă exclusiv de dreptul statului emitent", iar autoritatea emitentă „trebuie să condiționeze un ordin european de anchetă de respectarea tuturor condițiilor prevăzute de dreptul propriului său stat membru pentru o cauză internă similară", scopul cerinței fiind acela de a „evita o eludare a normelor și a garanțiilor prevăzute de dreptul statului emitent"[9]. Precizarea a fost făcută, ce-i drept, într-o cauză privind transmiterea unor mijloace de probă aflate deja în posesia autorităților statului de executare, ipoteză în care Curtea a statuat că nu se cere identitatea condițiilor de fond cu cele aplicabile strângerii acelorași probe în statul emitent (pct. 96). Raționamentul se aplică *mutatis mutandis* ordinelor întemeiate pe Regulament, prin care datele nu sunt preluate de la o autoritate străină, ci sunt obținute în mod nemijlocit de la furnizorul unui serviciu.

II.2. Cine este furnizor de servicii și ce înseamnă „un număr semnificativ de utilizatori"

Anterior Regulamentului, autoritatea judiciară care avea nevoie de date deținute de un furnizor stabilit într-o altă jurisdicție depindea fie de cooperarea voluntară a acestuia, fie de instrumentele clasice de cooperare judiciară în materie penală, iar acestea din urmă se dovedeau ineficiente îndeosebi în ipoteza în care furnizorul care deținea date relevante pentru soluționarea cauzei avea sediul în afara Uniunii. Regulamentul își propune să rezolve

[9] CJUE, hotărârea din 30 aprilie 2024, M.N. (EncroChat), C-670/22, pct. 92, 93, 96 și 97.

acest obstacol în ceea ce privește cooperarea în materie penală, stabilind obligații pozitive în sarcina furnizorilor care prestează servicii în Uniune.

Regulamentul definește furnizorul de servicii prin trei categorii [art. 3 pct. 3]:

i. Serviciile de comunicații electronice, astfel cum sunt definite la art. 2 pct. 4 din Directiva (UE) 2018/1972, între care telefonia fixă și mobilă și accesul la internet, precum și, potrivit considerentului (27), telefonia VoIP, mesageria instantanee și serviciile de e-mail. Intră aici, în România, furnizorii de rețele și de servicii de comunicații electronice precum Orange România, Vodafone România sau Digi România, sau serviciile de mesagerie și de poștă electronică de tipul WhatsApp, Telegram, Signal ori Gmail.

ii. Serviciile legate de numele de domenii de internet și de numerotarea IP, precum registrele și operatorii de registre de nume de domenii, furnizorii de servicii de protecție a vieții private și de servicii de proxy ori registrele regionale de internet [considerentul (28)]. Este cazul RoTLD, registrul domeniilor .ro, ori al RIPE NCC, registrul regional de internet pentru Europa.

iii. Alte servicii ale societății informaționale care fie le permit utilizatorilor să comunice între ei, fie fac posibilă stocarea ori prelucrarea datelor în numele acestora, „cu condiția ca stocarea datelor să fie o componentă definitorie a serviciului furnizat utilizatorului", precum piețele online, adică platformele de comerț electronic care, în termenii considerentului (27), „oferă consumatorilor și întreprinderilor posibilitatea de a comunica unii cu alții", serviciile de găzduire, inclusiv cele furnizate prin tehnologia de tip cloud, ori platformele online de jocuri și de jocuri de noroc [considerentul (27)].

Exemplificativ, piețele online de tipul eMAG Marketplace sau OLX și furnizorii europeni de găzduire și de servicii cloud precum OVHcloud ori Hetzner. Rețelele sociale și platformele de partajare de conținut, precum Facebook, Instagram, YouTube sau TikTok, se încadrează la lit. c), fiind servicii ale societății informaționale care le permit utilizatorilor să comunice între ei, prin mesaje directe, comentarii și grupuri, și care fac totodată posibilă stocarea datelor în numele acestora, stocarea conținutului încărcat de utilizator fiind pentru asemenea platforme, în termenii aceluiași considerent, „o parte esențială" a serviciului.

Ar trebui totuși precizat că un serviciu de mesagerie precum WhatsApp, Telegram ori Signal este, în componenta sa de comunicare interpersonală, serviciu de comunicații electronice, deci se încadrează la art. 3 pct. 3 lit. a), soluție confirmată de considerentul (27), care include expres mesageria instantanee. Aceleași platforme oferă însă și funcții care nu presupun un schimb direct de informații între un număr finit de persoane, ai căror destinatari să fie stabiliți de cei care inițiază sau participă la comunicare, precum canalele publice, grupurile deschise ori conținutul de tip status sau story. În privința acestora, calificarea drept serviciu de comunicații interpersonale devine discutabilă, iar serviciul poate fi privit ca serviciu al societății informaționale în sensul lit. c). Cu toate acestea, apreciem că un asemenea cumul este posibil, art. 3 pct. 3 definind furnizorul de servicii ca fiind persoana care furnizează „una sau mai multe dintre următoarele categorii de servicii".

Serviciile financiare sunt excluse expres din sfera de aplicabilitate a Regulamentului, prin trimitere la art. 2 alin. (2) lit. b) din Directiva 2006/123/CE. Sub acest aspect, se va pune problema în ce măsură furnizorii de servicii de criptoactive (Binance, Coinbase, Kraken etc.) intră sau nu sub incidența prevederilor Regulamentului[10].

[10] A se vedea și art. 3 alin. (1) pct. 15 din Regulamentul (UE) 2023/1114, serviciile relevante pentru o platformă centralizată fiind operarea unei platforme de tranzacționare, schimbul de criptoactive contra fonduri și schimbul

Împrejurarea că furnizorul este stabilit în afara Uniunii nu îl scoate de sub incidența Regulamentului. Ceea ce prezintă relevanță este oferirea de servicii în Uniune, noțiune care presupune o legătură substanțială cu un stat membru, existentă fie atunci când furnizorul are un sediu în Uniune, fie, în lipsa acestuia, atunci când există „un număr semnificativ de utilizatori" în unul sau mai multe state membre ori o direcționare a activităților către acestea [art. 3 pct. 4 lit. b)].

Se observă că acest criteriu nu se raportează la un prag numeric, fiind astfel discutabil ce se înțelege prin „semnificativ"[11]. De asemenea, nu există vreun mecanism de verificare a îndeplinirii acestei condiții, aprecierea rămânând la latitudinea furnizorului serviciului în cauză. În orice caz, în măsura în care un furnizor din afara UE, dar care oferă servicii către utilizatori din UE, nu își îndeplinește obligația de a numi un reprezentant legal într-un stat membru care participă la instrumentele juridice relevante, prevăzută la art. 3 alin. (1) lit. b) din Directivă, se pune problema care dintre autoritățile competente desemnate la nivelul statelor membre poate aplica sancțiuni.

Răspunsul la această din urmă problemă poate rezulta din considerentul (21) al Directivei. Astfel, autoritățile centrale despre care acesta face vorbire sunt cele pe care fiecare stat membru le desemnează potrivit art. 6 din Directivă și le comunică Comisiei. Rolul acestora este acela de a coordona între ele aplicarea Directivei, în special măsurile de asigurare a respectării normelor de către furnizori. Ele nu se confundă cu autoritățile centrale la care se referă art. 4 alin. (6) din Regulament. Or, potrivit aceluiași considerent (21), obligația de cooperare a acestor autorități, menită să evite conflictele pozitive sau negative de competență, „nu ar trebui să aducă atingere dreptului fiecărui stat membru de a impune sancțiuni furnizorilor de servicii care nu își respectă obligațiile ce le revin în temeiul prezentei directive". Fiecare stat membru poate, așadar, să acționeze, coordonarea urmând să se realizeze prin autoritățile centrale. Eficacitatea rămâne însă discutabilă, de vreme ce, potrivit considerentului (18) al aceleiași directive, sancțiunile nu pot duce „la o interdicție, permanentă sau temporară, a furnizării de servicii".

Discuția poate deveni cu atât mai controversată în privința conturilor de tip *sockpuppet*[12] și a celor generate de o manieră automatizată, întrucât baza de utilizatori pe care se întemeiază competența poate fi creată artificial, încât un furnizor din afara Uniunii ajunge să intre sub incidența Regulamentului din cauza unor conturi fictive create pe propria platformă. Strict ipotetic, nu ar fi exclusă posibilitatea ca o autoritate interesată să se folosească de acest mod de operare tocmai pentru a atrage o entitate juridică din afara Uniunii în sfera de aplicabilitate a Regulamentului. Ipoteza nu este pur teoretică, fiindcă niciun mecanism nu verifică baza de utilizatori, iar art. 3 pct. 4 lit. b) nu impune ca utilizatorii să fie

---

de criptoactive contra altor criptoactive [art. 3 alin. (1) pct. 16 lit. (b)-(d), coroborat cu pct. 18-20]. Dreptul intern preia această definiție, cu excluderea consultanței privind criptoactivele, prin art. 2 lit. t[2]) din Legea nr. 129/2019 (publicată în M. Of., Partea I, nr. 589 din 18 iulie 2019), în forma dată de O.U.G. nr. 10/2025 (publicată în M. Of., Partea I, nr. 225 din 13 martie 2025), iar art. 2 lit. g) pct. 8 din aceeași lege include „furnizori de servicii de criptoactive" în categoria instituțiilor financiare, deci printre entitățile raportoare.

[11] Potrivit doctrinei (*R. Amato*, Bridging borders, streamlining justice, balancing interests. The e-Evidence package journey: from a troubled origin story to an uncertain future, în Rivista italiana di informatica e diritto, nr. 1/2025, p. 399), opțiunea de a defini o „bază semnificativă de utilizatori" a fost avută în vedere în evaluarea de impact, dar a fost abandonată din cauza dificultăților de stabilire și de aplicare a unui prag determinat, precum și a riscului de a crea portițe exploatabile.

[12] Termenul desemnează un cont fictiv, creat pentru a simula un utilizator independent.

reali (o analiză la nivel cantitativ și calitativ), ci doar să existe (o analiză strict la nivel cantitativ).

II.3. Serviciile bazate pe sisteme de inteligență artificială și noțiunea de stocare

Un serviciu construit pe un sistem de inteligență artificială de uz general[13], precum cele de tip LLM (ChatGPT, Claude, Gemini, Mistral etc.), poate stoca prompturi și răspunsuri[14] care privesc redactarea unor mesaje tip *phishing*, scrierea unui cod malițios (e.g. malware) ori planificarea unei conduite infracționale (e.g. fraudă investițională), adică exact tipul de date (de conținut) ce ar putea prezenta un interes deosebit pentru organele judiciare.

În opinia noastră, aceste servicii nu sunt servicii de comunicații interpersonale, fiindcă o asemenea calificare presupune un schimb interpersonal și interactiv de informații între utilizatori finali[15], pe când aici schimbul are loc între utilizator și modelul AI, nu între doi utilizatori. Ele se încadrează, prin urmare, în categoria serviciilor societății informaționale. Tot considerentul (27) arată însă că un furnizor de asemenea servicii care „nu oferă utilizatorilor săi capacitatea de a comunica între ei, ci numai cu furnizorul de servicii" rămâne în afara definiției atunci când stocarea datelor nu este o componentă definitorie, adică „o parte esențială", a serviciului. Cum un serviciu conversațional construit pe un model de limbaj se află tocmai în această ipoteză, condiția stocării devine esențială pentru stabilirea sferei de aplicabilitate a Regulamentului.

Or, raportat la această calificare, o posibilă controversă vizează condiția stocării acestor date referitoare la conținut. Astfel, cele două ipoteze ale art. 3 pct. 3 lit. c) sunt alternative: serviciul intră sub incidența Regulamentului fie dacă le permite utilizatorilor să comunice între ei [pct. (i)], fie dacă face posibilă stocarea datelor în numele lor, însă numai „cu condiția ca stocarea datelor să fie o componentă definitorie a serviciului furnizat utilizatorului" [pct. (ii)], sintagmă pe care considerentul (27) o explică prin „o parte esențială" a serviciului.

Unii furnizori de asemenea servicii stochează conversațiile pe server (cloud) între sesiuni[16], iar datele rămân accesibile ori de câte ori utilizatorul se autentifică în contul-client.

---

[13] Sistemul de IA de uz general este definit la art. 3 pct. 66 din Regulamentul (UE) 2024/1689 ca „un sistem de IA care se bazează pe un model de IA de uz general și care are capabilitatea de a deservi o varietate de scopuri, atât pentru utilizare directă, cât și pentru integrarea în alte sisteme de IA".

[14] Prin prompt se înțelege instrucțiunea sau întrebarea formulată de utilizator în limbaj natural și transmisă modelului (input), pe baza căreia acesta generează răspunsul (output). Noțiunea acoperă atât textul propriu-zis, cât și, în cazul modelelor multimodale, fișierele care îl însoțesc, precum imagini, documente ori înregistrări audio. Din perspectiva Regulamentului, promptul și răspunsul generat sunt date în format digital care nu constituie nici date privind abonații, nici date privind traficul, astfel încât se încadrează, prin eliminare, în categoria datelor referitoare la conținut [art. 3 pct. 12].

[15] Serviciul de comunicații interpersonale este definit la art. 2 pct. 5 din Directiva (UE) 2018/1972 ca „un serviciu furnizat de regulă contra cost care permite schimbul direct de informații într-un mod interpersonal și interactiv prin intermediul rețelelor de comunicații electronice între un număr finit de persoane, în cadrul căruia persoanele care inițiază sau participă la comunicare își stabilesc destinatarul (destinatarii) și care nu include serviciile care permit comunicarea interpersonală și interactivă doar ca un simplu element auxiliar minor care este legat în mod intrinsec de un alt serviciu". Norma internă de transpunere este art. 4 alin. (1) pct. 9^1 din O.U.G. nr. 111/2011 (publicată în M. Of., Partea I, nr. 925 din 27 decembrie 2011), introdus prin Legea nr. 198/2022 (publicată în M. Of., Partea I, nr. 681 din 7 iulie 2022).

[16] Noțiunea este folosită chiar de Regulament: datele privind traficul includ datele „legate de începerea și terminarea unei sesiuni de acces al utilizatorului, cum ar fi data și ora utilizării, conectarea la serviciu și

Alți furnizori oferă însă conversații temporare, *incognito* sau secrete, care nu apar în istoricul accesibil în contul-client și, de regulă, nu sunt folosite pentru antrenarea modelului, dar pot rămâne accesibile furnizorului pentru o perioadă limitată, de regulă între 72 de ore și 30 de zile[17], în scopul prevenirii abuzurilor (e.g. folosirea modelului pentru înlesnirea unor conduite infracționale).

Întrebarea este dacă stocarea trebuie să fie persistentă ori dacă este suficient să discutăm despre o stocare temporară. În orice caz, s-ar putea argumenta că stocarea este una persistentă inclusiv în ipoteza în care perioada de retenție este de 72 de ore.

Regulamentul se limitează însă la datele stocate de furnizor sau în numele acestuia în momentul primirii certificatului, ceea ce rezultă din chiar definiția probelor electronice [art. 3 pct. 8], precum și din motivele de refuz al executării prevăzute la art. 16 alin. (4) lit. d) și alin. (5) lit. c). Considerentul (19) confirmă această soluție și întărește teza potrivit căreia Regulamentul nu autorizează interceptarea datelor și nici obținerea datelor stocate ulterior acestui moment.

II.4. O clasificare a datelor diferită de cea din materia reținerii datelor

Regulamentul are în vedere patru categorii de date: datele privind abonații [art. 3 pct. 9], datele solicitate exclusiv în scopul identificării utilizatorului [art. 3 pct. 10], datele privind traficul [art. 3 pct. 11] și datele referitoare la conținut [art. 3 pct. 12].

Această clasificare nu se suprapune perfect peste cea cu care operează legislația națională, iar diferențele nu sunt doar de ordin terminologic. Clasificarea din materia reținerii datelor a fost concepută pentru a delimita ce anume trebuie păstrat, în mod general și prealabil, de către furnizorii de comunicații electronice, obligație instituită în dreptul intern prin Legea nr. 82/2012, declarată neconstituțională prin Decizia Curții Constituționale nr. 440/2014[18].

Definițiile cu care dreptul intern operează și astăzi se regăsesc însă în Legea nr. 506/2004, care distinge, în acest scop, între datele de trafic, datele de identificare a echipamentului și datele de localizare [art. 2 alin. (1) lit. b), b[1]) și c)][19].

---

deconectarea de la acesta" [art. 3 pct. 11], iar considerentul (32) arată că înregistrarea de evenimente, numită și log al serverului, „indică începerea și încheierea unei sesiuni de acces a unui utilizator la un serviciu". O sesiune desemnează, prin urmare, intervalul dintre autentificarea utilizatorului și încheierea accesului, iar disponibilitatea datelor între sesiuni înseamnă că acestea rămân stocate și după închiderea sesiunii, fiind regăsite la o autentificare ulterioară.

[17] Exemplificativ, OpenAI precizează că discuțiile temporare nu apar în istoric și nu sunt folosite pentru antrenarea modelelor, fiind însă păstrate până la 30 de zile din motive de siguranță (https://help.openai.com/en/articles/8914046-temporary-chat-faq). De asemenea, Anthropic prevede pentru discuțiile incognito că nu sunt salvate nici în istoricul conversațiilor, nici în memoria modelului, cu o retenție implicită de 30 de zile (https://support.claude.com/en/articles/12260368). Nu în ultimul rând, Google indică pentru discuțiile temporare din Gemini că nu apar în activitatea contului și nu sunt folosite pentru antrenare, fiind păstrate 72 de ore (https://support.google.com/gemini/answer/13594961).

[18] Decizia nr. 440 din 8 iulie 2014, publicată în M. Of., Partea I, nr. 653 din 4 septembrie 2014.

[19] Comparația trebuie extinsă la cele două procedee probatorii din Codul de procedură penală, care operează, la rândul lor, cu noțiuni diferite. Art. 152 C.pr.pen. privește „datele de trafic și localizare" prelucrate de furnizorii de rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului, preluând astfel clasificarea din Legea nr. 506/2004 (publicată în M. Of., Partea I, nr. 1.101 din 25 noiembrie 2004). Art. 154 C.pr.pen. privește, în schimb, „datele informatice, inclusiv datele referitoare la traficul

Regulamentul nu instituie o obligație generală și prealabilă de păstrare, ci, din contră, prevede că nu ar trebui să aibă ca efect păstrarea generală și nediferențiată a datelor [considerentul (19)]. Categoriile de date prevăzute în Regulament prezintă o cu totul altă relevanță. Cum intensitatea ingerinței în drepturile fundamentale diferă de la o categorie de date la alta, Regulamentul le supune unor garanții și unor condiții de emitere diferite [considerentul (34)]. Astfel, în funcție de natura datelor, Regulamentul stabilește cine emite ordinul, pentru ce infracțiuni poate fi emis și dacă autoritatea de executare este sau nu notificată[20].

Comparația dintre cele două clasificări relevă cel puțin trei necorelări. Prima privește datele solicitate exclusiv în scopul identificării utilizatorului, prin care Regulamentul înțelege „adrese IP și, după caz, porturile sursă[21] și marca temporală relevante, și anume data și ora, sau echivalentele tehnice ale identificatorilor respectivi și informațiile conexe".

Regulamentul le tratează ca fiind puțin intruzive, întrucât ordinul poate fi emis de procuror, pentru orice infracțiune, fără notificarea autorității de executare [art. 4 alin. (1), art. 5 alin. (3) și art. 8 alin. (1)]. Regimul favorabil nu decurge însă din natura datelor, ci exclusiv din scopul pentru care ele sunt solicitate. Considerentul (32) recunoaște expres că „în anumite circumstanțe, adresele IP pot fi considerate date privind traficul" și că „numerele de acces și informațiile conexe sunt considerate date privind traficul în unele state membre", precizând că regimul datelor privind abonații li se aplică doar atunci când sunt cerute „exclusiv în scopul identificării utilizatorului" într-o cauză penală, iar considerentul (33) confirmă soluția *a contrario*, cerând ca aceleași date, atunci când nu sunt solicitate în acest scop, „să fie tratate ca date privind traficul și să fie solicitate în cadrul aceluiași regim ca cel al datelor referitoare la conținut".

În dreptul intern, aceleași date sunt date de trafic, iar obținerea lor de la un furnizor de comunicații electronice constituie o metodă specială de supraveghere sau cercetare [art. 138 alin. (1) lit. j) C.pr.pen.] și se poate realiza doar cu autorizarea prealabilă a judecătorului

---

informațional", stocate prin intermediul unui sistem informatic, iar potrivit alin. (7^1) regimul se aplică și datelor aflate „în posesia sau sub controlul altor persoane".

[20] Astfel, ordinul care are ca obiect date privind abonații sau date solicitate exclusiv în scopul identificării utilizatorului poate fi emis de procuror, pentru orice infracțiune, fără notificarea autorității de executare [art. 4 alin. (1), art. 5 alin. (3) și art. 8 alin. (1)]. În schimb, ordinul care are ca obiect date privind traficul sau date referitoare la conținut poate fi emis numai pentru infracțiuni a căror pedeapsă privativă de libertate are maximul special de cel puțin trei ani [lit. a)], pentru infracțiunile definite la art. 3-8 din Directiva (UE) 2019/713, la art. 3-7 din Directiva 2011/93/UE și la art. 3-8 din Directiva 2013/40/UE, dacă sunt săvârșite, în întregime sau parțial, prin intermediul unui sistem informatic [lit. b)], precum și pentru infracțiunile definite la art. 3-12 și la art. 14 din Directiva (UE) 2017/541 privind combaterea terorismului [lit. c)], precum și, potrivit lit. d), pentru executarea unei pedepse privative de libertate sau a unei măsuri privative de libertate de cel puțin patru luni, dispusă în urma unei proceduri penale printr-o hotărâre care nu a fost pronunțată în lipsă, în cazurile în care persoana condamnată s-a sustras justiției, pentru infracțiunile menționate la lit. a)-c), și presupune notificarea autorității de executare [art. 5 alin. (4) și art. 8 alin. (1)]. Notificarea nu este însă invariabilă. Potrivit art. 8 alin. (2), ea nu se aplică dacă, la momentul emiterii ordinului, autoritatea emitentă are motive întemeiate să considere că infracțiunea a fost săvârșită, este săvârșită sau este probabil să fie săvârșită în statul emitent și că persoana ale cărei date sunt solicitate își are reședința în statul emitent. În aceste cazuri, informațiile prevăzute la art. 5 alin. (5) lit. i) și j) nu ajung nici la autoritatea de executare, de vreme ce al doilea paragraf al art. 9 alin. (2) le transmite numai atunci când notificarea este obligatorie.

[21] Adresa IP publică nu identifică *per se* abonatul atunci când furnizorul recurge la translatarea adreselor. În rețelele mobile, în particular, aceeași adresă IPv4 publică este folosită simultan de un număr mare de abonați, prin mecanisme de tip CGNAT, astfel încât identificarea presupune tripleta formată din adresa IP, portul sursă și marca temporală, singura care permite furnizorului să regăsească în jurnalele proprii sesiunea corespunzătoare.

de drepturi și libertăți, pentru infracțiunile prevăzute la art. 152 alin. (1) lit. a) C.pr.pen. Mai mult, art. 170 alin. (2) lit. b) C.pr.pen. exclude expres din obiectul său datele prevăzute la art. 138 alin. (1) lit. j).

A doua necorelare privește datele referitoare la conținut, definite prin excludere, ca fiind orice date în format digital care nu sunt date privind abonații sau date privind traficul. O asemenea abordare atrage în această categorie date care nu sunt nici conținut al unei comunicări, nici probă în sens propriu, precum *device fingerprint*[22] sau cele de tip *user-agent*[23]. Încadrarea nu este însă automată, fiindcă art. 3 pct. 11 definește datele privind traficul suficient de larg încât să acopere orice date „legate de furnizarea unui serviciu oferit de un furnizor de servicii, care servesc la a oferi informații contextuale sau suplimentare cu privire la un astfel de serviciu și sunt generate sau prelucrate de un sistem informatic al furnizorului de servicii".

A treia necorelare privește chiar sfera furnizorilor de servicii. Clasificarea din dreptul intern, întemeiată pe Legea nr. 506/2004 și preluată de art. 152 C.pr.pen., vizează sectorul comunicațiilor electronice, pe când cea a Regulamentului vizează datele în general, indiferent de natura furnizorului care le deține. Pentru un serviciu de stocare în *cloud*, pentru o platformă de colaborare sau pentru un serviciu de tip LLM, dreptul intern nu oferă o categorie corespondentă pentru datele referitoare la conținut, ci doar procedee probatorii generale, precum comunicarea de date informatice în temeiul art. 170 alin. (2) lit. a) C.pr.pen. Acest text privește însă „orice persoană fizică sau juridică de pe teritoriul României", încât el poate servi drept reper pentru cauza internă similară, dar nu poate fi folosit el însuși pentru a obține date de la un furnizor stabilit în alt stat membru, ipoteză pentru care Regulamentul a fost, de altfel, conceput[24].

II.5. Parola stocată în bazele de date ale furnizorilor sub forma unei valori hash

Modul în care operează definiția prin excludere a datelor referitoare la conținut prezintă o importanță aparte în cazul parolei stocate în baza de date a furnizorului sub forma unei valori hash (MD5, SHA1, SHA256 etc.).

Datele privind abonații exclud expres „parolele sau alte mijloace de autentificare utilizate în locul unei parole care sunt furnizate de către un utilizator sau create la cererea unui utilizator" [art. 3 pct. 9 lit. b)], iar o parolă nu se încadrează nici în categoria datelor

[22] Amprenta dispozitivului [în eng., device fingerprint] desemnează combinația de atribute pe care terminalul le expune serviciului la fiecare conexiune, precum rezoluția ecranului, fusul orar, limba, fonturile instalate, versiunea sistemului de operare și a aplicației client ori particularitățile de randare grafică. Niciunul dintre aceste atribute nu identifică singur utilizatorul, însă combinația lor este suficient de rară încât să permită recunoașterea aceluiași terminal între sesiuni, chiar în lipsa autentificării sau a modulelor de tip cookie.

[23] Agentul utilizator (user-agent) este câmpul prin care aplicația client, de regulă browserul, își declară la fiecare cerere tipul, versiunea și sistemul de operare pe care rulează. Valoarea nu este verificată de server și poate fi modificată de utilizator, ceea ce îi limitează forța probantă luată izolat, dar rămâne un element de corelare între sesiuni și terminale.

[24] Obligația de punere la dispoziție prevăzută la art. 12^1 alin. (1) din Legea nr. 506/2004 a fost extinsă, prin art. 59 cap. VI din Legea nr. 198/2022, și asupra furnizorilor de servicii de găzduire electronică cu resurse IP, precum și a furnizorilor de servicii de comunicații interpersonale care nu se bazează pe numere, astfel cum sunt definiți de O.U.G. nr. 111/2011 [art. 12^1 alin. (1^1)]. Extinderea privește însă tot datele de trafic, datele de identificare a echipamentului și datele de localizare, nu și datele referitoare la conținut, în timp ce art. 152 C.pr.pen., temeiul procesual al autorizării, se referă în continuare numai la furnizorii de rețele publice de comunicații electronice și la furnizorii de servicii de comunicații electronice destinate publicului.

privind traficul, aceasta acoperind, potrivit art. 3 pct. 11, datele „legate de furnizarea unui serviciu oferit de un furnizor de servicii, care servesc la a oferi informații contextuale sau suplimentare cu privire la un astfel de serviciu", metadatele comunicațiilor electronice, precum și datele legate de începerea și terminarea unei sesiuni de acces. Or, valoarea hash a parolei nu oferă asemenea informații despre serviciu și nu descrie nicio sesiune, ea servind furnizorului exclusiv pentru a verifica, la fiecare autentificare, dacă parola introdusă de utilizator o reproduce. Prin eliminare, ea devine dată referitoare la conținut[25].

Totuși, Regulamentul stabilește normele în temeiul cărora unui furnizor de servicii i se poate cere divulgarea de probe electronice [art. 1 alin. (1)], însă o parolă stocată sub formă de valoare hash nu constituie, prin ea însăși, o probă a faptei ce face obiectul acuzației în materie penală[26], fiindcă nu arată ce s-a spus, ce s-a transmis sau ce s-a făcut. Trebuie precizat, sub acest aspect, că valoarea hash stocată nu reprezintă *per se* un mijloc de autentificare. La fiecare autentificare, furnizorul generează valoare hash după parola introdusă de utilizator și compară rezultatul cu valoarea pe care o stochează în baza de date.

Astfel, nici valoarea hash, nici parola eventual reconstituită nu dovedesc fapta, însă parola în *plaintext* poate servi la atribuire, fiindcă reutilizarea aceleiași parole pe mai multe conturi permite asocierea acestora. De asemenea, ordinul de divulgare având ca obiect valoarea hash poate înlesni o măsură de supraveghere tehnică, respectiv accesul la un sistem informatic [art. 138 alin. (1) lit. b) și alin. (3) C.pr.pen.]. Prin recunoașterea unei asemenea obligații pozitive în sarcina furnizorului, Regulamentul ajunge, așadar, să înlesnească o măsură căreia dreptul intern îi rezervă un regim propriu, cu autorizarea prealabilă a judecătorului de drepturi și libertăți. Deși s-ar putea argumenta că textul Regulamentului permite o asemenea interpretare, rezultatul ei ne apare contrar scopului acestui instrument.

II.6. Criptarea și cheia criptografică aflată în sfera de control a furnizorului

Regulamentul se prezintă ca fiind neutru în raport de problematica criptării datelor informatice. Potrivit considerentului (20), datele se furnizează sau se păstrează indiferent dacă sunt criptate sau nu, fără ca Regulamentul să instituie vreo obligație de decriptare în sarcina furnizorului. De aici rezultă fără echivoc că instituirea unei obligații pozitive privind decriptarea datelor informatice nu este compatibilă cu Regulamentul.

---

[25] Această posibilă controversă a fost deja semnalată în doctrină – a se vedea *V. Franssen*, Cross-border gathering of electronic evidence in the EU: toward more direct cooperation under the e-Evidence Regulation, cap. 9 în *V. Mitsilegas*, *M. Bergström, T. Quintel* (eds.), Research Handbook on EU Criminal Law, ed. a 2-a, Edward Elgar Publishing, 2024, citat aici după versiunea preprint disponibilă la https://ssrn.com/abstract=4789055, p. 12. Autoarea arată că Regulamentul exclude expres parolele din sfera datelor privind abonații, fără a preciza căreia dintre celelalte două categorii de date le aparțin. Aceeași autoare arată totodată că obligația de a permite accesul la un sistem informatic, de pildă prin punerea la dispoziție a parolei, nu se numără printre obligațiile instituite prin Regulament (Ibidem, p. 22). Deducția potrivit căreia parola stocată sub formă de valoare hash devine, prin eliminare, dată referitoare la conținut ne aparține. Prin modificarea adusă art. 132 alin. 3.bis.2 lit. b) din Decretul legislativ italian nr. 196/2003, sunt excluse din datele privind abonații „password o altri mezzi di autenticazione usati al posto di una password, forniti dall'utente o creati a sua richiesta", formulare care preia întocmai excluderea din art. 3 pct. 9 lit. b) din Regulament, fără a preciza însă nici ea căreia dintre celelalte categorii îi aparțin.

[26] Exceptând ipoteza în care parola poate conduce la identificarea titularului de cont (e.g. aceasta este formată din numele acestuia, data nașterii etc.).

Trebuie avute totuși în vedere două aspecte. În cazul criptării de la un capăt la altul (e2e), furnizorul nu deține cheia criptografică și nu poate decripta, iar ordinul are ca obiect conținutul criptat aflat sub controlul său, predat în forma în care este stocat, alături de eventualele date referitoare la conținut pe care furnizorul le deține în clar. Regulamentul nu îi impune însă obligația de a decripta datele [considerentul (20)][27].

În schimb, în cazul criptării server-side[28], furnizorul deține atât conținutul criptat, cât și cheia de decriptare. Întrebarea, în această a doua ipoteză, este ce anume poate face obiectul ordinului emis în temeiul Regulamentului: conținutul criptat, conținutul criptat împreună cu cheia de decriptare sau conținutul decriptat. Cum cheia este ea însăși o dată stocată de furnizor, care nu se încadrează nici la datele privind abonații, nici la cele privind traficul, argumentul că ea poate forma obiectul unui ordin de divulgare este greu de combătut pe textul Regulamentului, deși rezultatul, adică absența unei obligații de decriptare dublată de obligația de a divulga cheia, golește de conținut tocmai neutralitatea pe care considerentul (20) o promovează[29].

II.7. Furnizorul de drept privat ca garant al drepturilor fundamentale

Regulamentul plasează în sarcina furnizorului privat verificări care, în mod tradițional, aparțin unei autorități judiciare. Destinatarul ordinului este chemat să aprecieze, exclusiv pe baza informațiilor cuprinse în certificat, dacă executarea ar putea intra în conflict cu imunități sau privilegii ori cu norme privind stabilirea sau limitarea răspunderii penale referitoare la libertatea presei și la libertatea de exprimare în alte mijloace de informare în masă, în temeiul dreptului statului de executare [art. 10 alin. (5) și art. 11 alin. (4)].

Strict din punct de vedere formal, destinatarul nu decide, ci doar semnalează o posibilă neconformitate. Constatând un asemenea conflict, el informează autoritatea emitentă și autoritatea de executare, utilizând formularul prevăzut în anexa III, iar hotărârea de a retrage, de a adapta ori de a menține ordinul rămâne autorității emitente. Cu toate acestea, prezintă relevanță entitatea care efectuează filtrul inițial[30].

---

[27] Criptarea de la un capăt la altul (end-to-end) presupune că datele sunt criptate pe terminalul expeditorului și decriptate pe terminalul destinatarului, cheile private rămânând pe dispozitivele utilizatorilor. Furnizorul transportă și, eventual, stochează exclusiv conținutul criptat, fără a deține mijloacele tehnice de a-l reconstitui.

[28] Criptarea server-side presupune că furnizorul este cel care criptează datele pe propriile echipamente și administrează cheile criptografice, păstrând astfel posibilitatea tehnică de a le decripta oricând, de exemplu pentru a le afișa utilizatorului la autentificare. Din perspectiva ordinului de divulgare, diferența este deosebit de relevantă: conținutul criptat de la un capăt la altul nu poate fi predat decât în formă criptată, în timp ce în ipoteza criptării server-side furnizorul deține atât conținutul criptat, cât și cheia criptografică necesară pentru decriptare.

[29] Distincția tehnică are consecințe inclusiv din perspectiva Convenției europene a drepturilor omului. În cauza Podchasov c. Rusiei, hotărârea din 13 februarie 2024 (cererea nr. 33696/19), par. 79, Curtea a reținut că obligația legală de a decripta comunicațiile criptate de la un capăt la altul riscă să echivaleze cu o cerință ca furnizorii unor asemenea servicii să slăbească mecanismul de criptare pentru toți utilizatorii, ceea ce nu este proporțional cu scopurile legitime urmărite. Curtea a precizat însă expres, la par. 56, că nu examinează schema de criptare folosită în conversațiile de tip cloud, adică, potrivit par. 5 al aceleiași hotărâri, tocmai ipoteza criptării server-client, în care furnizorul deține cheia. Chestiunea nu a fost, așadar, tranșată, iar situația discutată aici rămâne deschisă.

[30] Sub acest aspect, critica este prezentă în literatura de specialitate, fără a fi însă unanimă. *M. Rojszczak*, e-Evidence Cooperation in Criminal Matters from an EU Perspective, în The Modern Law Review, vol. 85, nr. 4/2022, p. 1010, pornind de la propunerea Comisiei din 2018, apreciază că de la un furnizor de servicii nu se

Dificultatea nu ține doar de natura verificării, ci inclusiv de materialul pe baza căruia ea se efectuează. Astfel, certificatul transmis destinatarului preia din ordin doar informațiile enumerate la art. 5 alin. (5) lit. a)-h), respectiv la art. 6 alin. (4) lit. a)-f) [art. 9 alin. (2) și (3)], încât rămân în afara conținutului acestuia tocmai motivele pentru care s-a stabilit că măsura este necesară și proporțională [art. 5 alin. (5) lit. i) și art. 6 alin. (4) lit. g)], precum și descrierea succintă a cauzei [art. 5 alin. (5) lit. j)]. Aceste informații ajung la autoritatea de executare, însă doar atunci când notificarea este obligatorie [art. 9 alin. (2) al doilea paragraf]. Furnizorul este chemat, prin urmare, să aprecieze asupra imunităților, a privilegiilor și a libertății presei pe baza unui extras din care lipsesc deopotrivă motivarea proporționalității și descrierea faptei.

II.8. Procurorul ca autoritate emitentă

Regulamentul permite ca ordinul de păstrare, pentru orice categorie de date, și ordinul de divulgare a datelor privind abonații ori a datelor solicitate exclusiv în scopul identificării utilizatorului să fie emise de un procuror [art. 4 alin. (1) și (3)], iar ordinul de păstrare poate fi emis pentru orice infracțiune [art. 6 alin. (3)].

Or, în măsura în care aceste date sunt, în dreptul intern, date de trafic, astfel cum am arătat mai sus, Curtea de Justiție a statuat că accesul la datele de trafic și de localizare presupune controlul prealabil al unei autorități independente, calitate pe care procurorul, în procesul penal, nu o are[31], și că un asemenea acces trebuie rezervat combaterii infracțiunilor grave[32].

Concluzia nu poate fi însă generalizată la toate categoriile pe care Regulamentul le încredințează procurorului. Prin hotărârea din 30 aprilie 2024, La Quadrature du Net și alții,

---

poate aștepta în mod realist efectuarea unor asemenea verificări, nu din cauza termenului scurt, ci pentru simplul motiv că îi lipsesc informațiile necesare, autorul având în vedere verificarea unei încălcări vădite a Cartei [art. 9 alin. (5) din propunere] și conformitatea cu dreptul național. Pe forma adoptată, aceeași critică este formulată de *A. Sachoulidou*, Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of „judicial" cooperation, în New Journal of European Criminal Law, vol. 15, nr. 3/2024, p. 268, și, preluând-o, de *V. Polyzoidou*, e-Evidence Regulation: A Contemporary Trojan Horse in Criminal Proceedings?, în *T.-E. Synodinou* ș.a. (eds.), EU Digital Law in the AI Era, Springer, 2025, p. 249, care arată că furnizorilor li se cere acum să funcționeze ca un „prim filtru" în identificarea încălcărilor drepturilor fundamentale, deși le poate lipsi expertiza necesară și deși sunt puși în situația de a alege între conformare și sancțiune, cu riscul ca interesul comercial să prevaleze asupra protecției drepturilor fundamentale. Sintagma „prim filtru" a fost promovată în *S. Tosza*, Mutual Recognition by Private Actors in Criminal Justice? E-Evidence Regulation and Service Providers as the New Guardians of Fundamental Rights, în Common Market Law Review, vol. 61, nr. 1/2024, p. 162, fiind contrazisă în parte în *J. Shurson*, The balance of efficiency and fundamental rights in the EU e-Evidence Regulation, în New Journal of European Criminal Law, vol. 16, nr. 3/2025, p. 289-291, care arată că furnizorul nu se substituie autorităților naționale în aprecierea ordinelor (*J. Shurson,* op. cit., p. 289), dar admite deopotrivă că Regulamentul nu ar trebui să îi impună evaluarea conformității cu drepturile fundamentale (*J. Shurson,* op. cit., p. 289) și că este întemeiată observația potrivit căreia furnizorii privați vor fi motivați de propriile interese comerciale, nu de binele comun (*J. Shurson,* op. cit., p. 291). Autoarea susține totuși că Regulamentul ar trebui să permită furnizorului să conteste ordinele care, din chiar cuprinsul lor, apar ca fiind contrare drepturilor fundamentale (*J. Shurson,* op. cit., p. 289 și 291), și că, în lipsa acestui temei de contestare, Regulamentul lasă drepturile mai slab protejate (*J. Shurson,* op. cit., p. 289).

[31] CJUE, hotărârea din 2 martie 2021, Prokuratuur (Condițiile de acces la datele privind comunicațiile electronice), C-746/18, pct. 51, 54 și 57.

[32] CJUE, hotărârea din 6 octombrie 2020, La Quadrature du Net și alții, C-511/18, C-512/18 și C-520/18, pct. 140.

C-470/21[33], Curtea a reținut că, atunci când o adresă IP este utilizată doar în scopul identificării titularului său în cadrul unei proceduri administrative specifice care ar putea conduce la urmărirea penală a acestuia, nu în scopuri precum dezvăluirea contactelor sau a localizării lui, accesul la acea adresă privește data respectivă mai degrabă ca dată referitoare la identitatea civilă decât ca dată de transfer, în terminologia Directivei 2002/58 (pct. 101), iar, ingerința nefiind gravă, el poate fi justificat prin obiectivul prevenirii, investigării, detectării și urmăririi penale a infracțiunilor în general (pct. 96). Această linie jurisprudențială acoperă tocmai ipoteza datelor solicitate exclusiv în scopul identificării utilizatorului, categorie pe care Regulamentul o reglementează distinct și căreia îi aplică deliberat, prin considerentele (32) și (34), regimul datelor privind abonații.

Critica își păstrează totuși relevanța, cel puțin din două considerente. În primul rând, Curtea a condiționat această soluție de garanții pe care dreptul român nu le prevede, între care păstrarea categoriilor de date astfel încât între ele să fie asigurată, în termenii Curții, „o separare efectiv etanșă" (pct. 84), precum și folosirea adresei IP exclusiv pentru identificarea persoanei suspectate de săvârșirea unei infracțiuni, cu interdicția expresă de a se „reconstitui parcursul de navigare al acestor titulari" (pct. 164). În al doilea rând, art. 152 alin. (1) C.pr.pen. nu operează distincția pe care Curtea o face după capacitatea inferențială a datelor, ci supune întregul set de date de trafic și de localizare autorizării prealabile a judecătorului de drepturi și libertăți, astfel încât, pe terenul condiției cauzei interne similare, problema competenței procurorului rămâne una reală.

II.9. Căile de atac și vidul legislativ cu privire la admisibilitatea mijloacelor de probă

Calea de atac a persoanei ale cărei date sunt solicitate poate fi exercitată doar în statul emitent și numai împotriva ordinului de divulgare, nu și împotriva ordinului de păstrare [art. 18 alin. (1) și (2)][34]. Regulamentul impune totodată, la art. 18 alin. (4), ca termenele și celelalte condiții de exercitare să fie aceleași ca în cazul căilor de atac din cauze interne similare, într-un mod care să garanteze exercitarea efectivă a dreptului. Pentru o persoană care nu are reședința în statul emitent, remediul presupune un forum străin, într-o limbă străină, iar dreptul la informare de care depinde exercitarea lui poate fi amânat, restrâns sau înlăturat în condițiile art. 13 alin. (2), prin trimitere la derogările din materia protecției datelor în domeniul penal[35].

În fine, Regulamentul nu conține nicio normă privind admisibilitatea mijloacelor de probă astfel obținute[36]. Art. 20 privește doar efectele juridice ale documentelor transmise pe

[33] CJUE, hotărârea din 30 aprilie 2024, La Quadrature du Net și alții, C-470/21.

[34] Soluția limitării remediului în statul emitent este criticată în doctrină – a se vedea în acest sens *A. Sachoulidou*, op. cit., p. 272. Autoarea arată că propunerile Comisiei LIBE, adoptate de Parlamentul European, prevedeau posibilitatea de a contesta legalitatea ordinului și în fața instanțelor statului de executare, tocmai în considerarea persoanelor care nu au reședința în statul emitent, nu îi cunosc ordinea juridică și nu îi vorbesc limba.

[35] *S. Tosza*, The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?, în European Data Protection Law Review, vol. 9, nr. 2/2023, p. 171, arată că autoritatea emitentă poate amâna, restrânge sau chiar omite informarea persoanei vizate, pentru motive ținând de interesul anchetei, de combaterea criminalității în general ori de interese naționale, criteriile fiind împrumutate din art. 13 alin. (3) din Directiva (UE) 2016/680 și fiind îndeajuns de largi încât să deschidă posibilități extinse de neinformare a persoanei vizate, limitându-i astfel capacitatea de a contesta ordinul.

[36] În doctrină s-a arătat că propunerea Comisiei LIBE cuprindea dispoziții exprese în sensul inadmisibilității, în fața instanțelor naționale, a informațiilor obținute cu încălcarea Regulamentului, aceeași sancțiune fiind

cale electronică, iar art. 18 alin. (5) se limitează la a impune respectarea dreptului la apărare și a caracterului echitabil al procedurii la evaluarea probelor. Consecința este că legalitatea mijloacelor de probă administrate în jurisdicții diferite urmează să fie reconstituită ex post de instanța de judecată, exact dinamica pe care Curtea de Justiție a lăsat-o dreptului național în hotărârea M.N. (EncroChat), C-670/22, cit. supra[37].

III. ANALIZA PROIECTULUI DE LEGE

III.1. Asimilarea cu procedeele probatorii din dreptul național

Proiectul de Lege își propune asimilarea ordinelor europene cu anumite procedee probatorii reglementate de Codul de procedură penală, indicând și organele judiciare în competența cărora intră emiterea ordinelor prevăzute în Regulament.

Astfel:

a) Ordinele de păstrare sunt asimilate conservării datelor informatice [art. 154 C.pr.pen.]. Emitenții sunt, corespunzător fazelor procesuale, procurorul, judecătorul de cameră preliminară, instanța de judecată și judecătorul delegat cu executarea;

b) Ordinele de divulgare care privesc date privind abonații și date solicitate exclusiv în scopul identificării utilizatorului sunt asimilate predării obiectelor, înscrisurilor sau a datelor informatice [art. 170 C.pr.pen.]. Emitenții sunt procurorul, judecătorul de cameră preliminară, instanța de judecată și judecătorul delegat cu executarea;

c) Ordinele de divulgare care privesc date privind traficul și date referitoare la conținut sunt asimilate obținerii datelor de trafic și de localizare [art. 152 C.pr.pen.]. Emitenții sunt judecătorul de drepturi și libertăți, judecătorul de cameră preliminară, instanța de judecată și judecătorul delegat cu executarea.

Ab initio, trebuie observat că această abordare a legiuitorului român se distanțează semnificativ de abordarea legiuitorului german. Astfel, în timp ce proiectul de Lege L272/2026 procedează la asimilarea ordinelor europene cu procedee probatorii din dreptul intern, prin Elektronische-Beweismittel-Umsetzungs-und-Durchführungsgesetz (EBewMG) se stabilesc

---

prevăzută și pentru informațiile obținute anterior invocării unui motiv de refuz, niciuna dintre aceste dispoziții nefiind însă preluată de redactorii Regulamentului (*A. Sachoulidou*, op. cit., p. 273). Modelul unei asemenea reglementări există, de altfel, sub forma propunerii *European Law Institute*, ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, Viena, 2023, care prevede cauze de inadmisibilitate la art. 5 și art. 6 (p. 31-32), precum și la art. 9 alin. (2) (p. 33), dar care exclude ea însăși din obiectul său accesul direct, extrateritorial, la date, lăsând admisibilitatea probei astfel obținute pe seama normelor statului forului (a se vedea p. 9).

[37] Curtea a reținut, la pct. 128, că „în stadiul actual al dreptului Uniunii, revine, în principiu, numai dreptului național sarcina de a stabili normele referitoare la admisibilitatea și la aprecierea, în cadrul unei proceduri penale, a informațiilor și a elementelor de probă care au fost obținute într-un mod contrar dreptului Uniunii". La pct. 131 a statuat însă că art. 14 alin. (7) din Directiva 2014/41/UE impune judecătorului național să înlăture informațiile și probele dacă persoana vizată „nu este în măsură să pună în discuție în mod eficient aceste informații și aceste probe" și dacă „ele pot influența în mod preponderent aprecierea faptelor". În doctrină, *S. Tosza*, Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems, în Studia Iuridica Lublinensia, vol. 33, nr. 5/2024, p. 251-252, arată că singura dispoziție cu o eventuală incidență asupra admisibilității este art. 20, care nu reprezintă însă decât un fel de clauză de nediscriminare privitoare la forma electronică a probei, și adaugă că din art. 18 alin. (5) rezultă că rămâne la latitudinea statelor membre să stabilească ce consecințe atrage încălcarea regulilor procedurale privitoare la ordinul european de divulgare.

procedurile de autorizare și executare (organul judiciar care emite și validează) a ordinelor europene în funcție de caracterul intruziv al datelor – procurorul ori instanța pentru datele de abonat sau de identificare și exclusiv instanța de judecată pentru datele de trafic și cele de conținut[38].

În context, ne putem pune problema dacă abordarea legiuitorului român este una corespunzătoare. Astfel, din modul în care citim proiectul de Lege, rezultă că organele judiciare nu vor emite propriu-zis ordine europene, ci ordonanțe sau încheieri, în temeiul dispozițiilor legale aferente unor procedee probatorii reglementate în Codul de procedură penală.

Trimiterea explicită la procedeele probatorii din Codul de procedură penală apare exclusiv pentru faza de urmărire penală, respectiv la art. 2 alin. (1) din proiectul de Lege (art. 154 C.pr.pen.), la art. 3 alin. (1) lit. a) din proiectul de Lege (art. 170 alin. (2) lit. b) C.pr.pen.) și la art. 4 alin. (1) lit. a) din proiectul de Lege (art. 152 C.pr.pen.).

Pentru camera preliminară, pentru judecată și pentru punerea în executare, proiectul se limitează să indice actul procesual prin care se emite ordinul, adică încheierea pronunțată de judecătorul de cameră preliminară, de instanța de judecată sau de judecătorul delegat cu executarea, fără a preciza în temeiul cărui procedeu probatoriu și în ce condiții poate fi ea pronunțată [art. 2 alin. (2), art. 3 alin. (1) lit. b) și c), art. 4 alin. (1) lit. b) și c)]. Pentru aceste faze procesuale, proiectul de Lege pare că dorește să inducă o interpretare prin analogie cu procedeele probatorii identificate explicit pentru urmărirea penală.

Apreciem că prin aceste asimilări s-a scăpat din vedere una dintre cerințele esențiale ale Regulamentului.

Astfel, printre alte condiții, Regulamentul prevede pentru emiterea ordinelor (atât de păstrare, cât și de divulgare) o cerință imperativă: ordinul de divulgare poate fi emis „doar dacă un ordin similar ar fi putut fi emis în aceleași condiții într-o cauză internă similară” [art. 5 alin. (2)], iar art. 6 alin. (3) prevede, pentru ordinul de păstrare, că acesta poate fi emis pentru toate infracțiunile „dacă ar fi putut fi emis în aceleași condiții într-o cauză internă similară”.

Practic, din coroborarea acestor prevederi din Regulament rezultă că un ordin de păstrare sau de divulgare poate fi emis pentru furnizorii din celelalte state ale Uniunii doar dacă, într-o cauză internă de același fel, același procedeu probatoriu – sau unul echivalent – poate fi autorizat și aplicat în raport cu furnizorii din România.

De aici apar cel puțin trei posibile incongruențe.

a) În primul rând, în dreptul intern, conservarea datelor informatice *este permisă doar în faza de urmărire penală*. Dispozițiile art. 154 C.pr.pen. nu menționează nimic despre autorizarea acestui procedeu probatoriu în faza de cameră preliminară sau în cea de judecată. Devine deci foarte discutabil dacă ar fi conformă Regulamentului posibilitatea acordată

[38] Elektronische-Beweismittel-Umsetzungs- und -Durchführungsgesetz (EBewMG), art. 1 din Legea din 10 martie 2026 de transpunere a Directivei (UE) 2023/1544 și de punere în aplicare a Regulamentului (UE) 2023/1543, publicată în Bundesgesetzblatt, Partea I, 2026, nr. 64. Potrivit § 9 alin. (1), competența instanțelor și a parchetelor de a emite ordine europene de divulgare privind datele privind abonații și datele solicitate exclusiv în scopul identificării utilizatorului se determină potrivit Codului de procedură penală german, iar potrivit § 10 alin. (1) competența pentru datele privind traficul și cele referitoare la conținut aparține instanțelor. Legiuitorul german nu definește, așadar, ordinul european prin actul procesual intern, ci se limitează să desemneze organul competent prin trimitere la regulile interne de competență, soluție confirmată de § 7, care declară aplicabile celelalte norme de procedură și de competență în măsura în care legea nu dispune altfel.

judecătorului de cameră preliminară sau instanței de a emite ordine de păstrare a probelor electronice.

b) În al doilea rând, în materia ordinelor de divulgare care privesc date privind abonații și date solicitate exclusiv în scopul identificării utilizatorului, trimiterea pe care proiectul de Lege o realizează la procedeul predării obiectelor, înscrisurilor sau a datelor informatice, mai precis la dispozițiile art. 170 alin. (2) lit. b) C.pr.pen., este foarte problematică.

Această corelare stă la baza dispoziției naționale care ar permite și procurorului să emită un asemenea ordin. O atare dispoziție ar fi conformă cu art. 4 alin. (1) lit. a) din Regulament.

Însă predarea acestor date „în aceleași condiții într-o cauză internă similară", în temeiul art. 170 alin. (2) lit. b) C.pr.pen., rămâne, la fel ca mai sus, foarte discutabilă. Și aceasta întrucât dispozițiile art. 154 alin. (6)-(7^1) C.pr.pen. stabilesc că transmiterea datelor conservate se face *cu autorizarea prealabilă a judecătorului de drepturi și libertăți*.

Art. 170 alin. (2) lit. b) C.pr.pen. exclude expres datele prevăzute la art. 138 alin. (1) lit. j) C.pr.pen., adică datele de trafic și de localizare prelucrate de furnizorii de rețele publice de comunicații electronice ori de servicii de comunicații electronice destinate publicului. Or, astfel cum am arătat supra, adresa IP, portul sursă și marca temporală, care alcătuiesc, potrivit art. 3 pct. 10 din Regulament, datele solicitate exclusiv în scopul identificării utilizatorului, sunt în dreptul intern date de trafic. Rezultă că ordonanța emisă în temeiul art. 170 alin. (2) lit. b) C.pr.pen. nu ar putea avea ca obiect, într-o cauză pur internă, asemenea date, singura posibilitate rămânând autorizarea prealabilă a judecătorului de drepturi și libertăți, în condițiile restrictive ale art. 152 C.pr.pen.

Apreciem că, prin trimiterea explicită la art. 170 alin. (2) lit. b) C.pr.pen., legiuitorul român alege să ignore o necorelare care rezultă din simpla comparare a textelor invocate[39]. În opinia noastră, problema ar trebui soluționată în sensul aplicării dispozițiilor art. 154 alin. (6)-(7^1) C.pr.pen., adică pentru divulgarea datelor ar fi necesară autorizarea prealabilă a judecătorului. Argumentul nostru ține de faptul că procedeul probatoriu afectează drepturi fundamentale, deci standardul ar trebui să fie cel în favoarea persoanei afectate de emiterea ordinului european.

În mod cert însă, nu este nici pe departe atât de clar pe cât își dorește proiectul de Lege că un ordin de divulgare care privește date privind abonații și date solicitate exclusiv în scopul identificării utilizatorului ar putea fi emis, într-o cauză similară din România, de către un procuror. Deci, nici că ar putea fi emis pentru furnizorii de servicii din UE.

c) În al treilea rând, nici pentru ordinele de divulgare care privesc date privind traficul și date referitoare la conținut nu este cert că ar putea fi emise de judecătorii de cameră preliminară și de instanțele de judecată.

Proiectul de Lege asimilează aceste ordine cu procedeul obținerii datelor de trafic și de localizare [art. 152 C.pr.pen.].

[39] Legiuitorul italian a ales soluția opusă, intervenind asupra dreptului intern chiar prin actul de punere în aplicare a Regulamentului. Prin Decretul legislativ nr. 215 din 30 decembrie 2025, publicat în Gazzetta Ufficiale, Serie generale, nr. 11 din 15 ianuarie 2026, art. 132 din Decretul legislativ nr. 196/2003 a fost modificat prin introducerea alin. 3.bis.2 și 3.bis.3. Primul exclude datele privind abonații din regimul autorizării prealabile a judecătorului, prevăzut la alin. 3 și 3-bis, și le definește preluând definiția din Regulament, inclusiv excluderea parolelor și a altor mijloace de autentificare. Al doilea atribuie obținerea acestor date procurorului ori poliției judiciare, în temeiul art. 348 din Codul de procedură penală italian. Necorelarea pe care proiectul de Lege o lasă deschisă a fost, așadar, rezolvată legislativ.

Dispozițiile art. 152 C.pr.pen. limitează destul de evident acest procedeu la faza urmăririi penale. În schimb, dispozițiile art. 12^1 din Legea nr. 506/2004 permit obținerea acestor date și de către instanțele de judecată.

Din nou, o necorelare legislativă. Asupra ei s-a pronunțat indirect Înalta Curte de Casație și Justiție, în considerentele Deciziei nr. 15/2016, pronunțată în recurs în interesul legii la 26 septembrie 2016 și publicată în M. Of., Partea I, nr. 892 din 8 noiembrie 2016, prin care sesizarea a fost respinsă ca inadmisibilă, unde se arată că, odată cu intrarea în vigoare a Legii nr. 75/2016 (publicată în M. Of., Partea I, nr. 334 din 29 aprilie 2016), „art. 152 din Codul de procedură penală a devenit temei legal unic (s.n.) și direct pentru autorizarea solicitării datelor de trafic și localizare prelucrate de către furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului [...]".

Față de aceste texte, o eventuală emitere de către judecătorul de cameră preliminară sau de instanța de judecată a unui ordin european de păstrare a probelor electronice sau a unui ordin european de divulgare a datelor privind traficul pare că este *ab initio* nelegală. Regulamentul ar fi încălcat, din moment ce aceleași organe judiciare nu au posibilitatea legală, la nivel intern, de a dispune aceleași procedee probatorii în raport cu furnizorii de servicii cu sediul în România.

III.2. Autorizarea de către procuror

Proiectul de Lege introduce posibilitatea ca, în cazuri urgente, procurorul să autorizeze emiterea ordinelor de păstrare (indiferent de categoria de date) și a celor de divulgare a datelor privind abonații și a datelor solicitate exclusiv în scopul identificării utilizatorului, cu obligația ulterioară de sesizare a judecătorului de drepturi și libertăți.

Precizăm că această posibilitate nu vizează ordinele de divulgare a datelor privind traficul și a datelor referitoare la conținut, pentru care nici Regulamentul și nici proiectul de Lege nu permit autorizarea provizorie.

În opinia noastră, dispoziția din proiectul de Lege este redundantă și riscă, în plus, să inducă confuzie.

Astfel, caracterul *redundant* derivă din împrejurarea că ordinele de păstrare sunt asimilate la nivel intern cu conservarea datelor informatice [art. 154 C.pr.pen.], iar cele de divulgare a datelor privind abonații și a datelor solicitate exclusiv în scopul identificării utilizatorului sunt asimilate cu predarea de obiecte, înscrisuri sau date informatice [art. 170 C.pr.pen.].

Or, în legislația internă, procurorul este cel care dispune, prin ordonanță, conservarea datelor informatice [art. 154 alin. (1) și (2) C.pr.pen.], iar predarea de obiecte, înscrisuri sau date informatice poate fi dispusă de organul de urmărire penală [art. 170 alin. (2) C.pr.pen.], iar Regulamentul îi permite explicit procurorului să emită ordinul de păstrare pentru orice categorie de date și ordinul de divulgare a datelor privind abonații ori a datelor solicitate exclusiv în scopul identificării utilizatorului [art. 4 alin. (1) lit. a) și alin. (3) lit. a) din Regulament].

Precizăm că această competență privește dispunerea procedeelor probatorii ca atare, nu și transmiterea efectivă a datelor conservate, pentru care art. 154 alin. (6) C.pr.pen. cere autorizarea prealabilă a judecătorului de drepturi și libertăți, chestiune asupra căreia ne-am oprit *supra*, la pct. 3.1 lit. b). Sub acest din urmă aspect, s-ar putea aprecia că prevederea legală din proiectul de Lege nu este redundantă. Formula „fără autorizarea judecătorului,

atunci când aceasta este necesară, conform legii" [art. 4 alin. (2) din proiectul de Lege] vizează tocmai ipoteza în care dreptul intern pretinde autorizarea, astfel încât textul nu dublează o competență existentă, ci instituie o derogare de la condiția controlului judiciar, cu atât mai discutabilă cu cât ea nu are corespondent într-o cauză internă similară.

Concluzia se sprijină inclusiv pe temeiul juridic din Proiectul de lege. Astfel, art. 4 alin. (2) din proiectul de Lege face trimitere la art. 4 alin. (5) din Regulament, text care nu reglementează însă autorizarea judecătorească. El permite autorităților competente prevăzute la art. 4 alin. (1) lit. b) și alin. (3) lit. b) să emită în mod excepțional ordinul „fără validarea prealabilă a ordinului în cauză, atunci când validarea nu poate fi obținută la timp", cu obligația de a solicita validarea ex post în cel mult 48 de ore. Or, procurorul este el însuși autoritate emitentă, în temeiul art. 4 alin. (1) lit. a) și alin. (3) lit. a), astfel că ordinele pe care le emite nu sunt supuse validării, iar ipoteza reglementată la alin. (5) nu îl privește. De altfel, din simpla lectură a Regulamentului rezultă că „autoritățile competente menționate la alineatul (1) litera (b) și la alineatul (3) litera (b)" sunt altele decât procurorul. Chiar în ipoteza pe care o are în vedere, alin. (5) condiționează expres derogarea de împrejurarea ca autoritățile respective „ar putea emite un ordin într-o cauză internă similară fără validare prealabilă". Textul european nu creează, prin urmare, o derogare autonomă, ci o preia din dreptul intern, în aceeași logică a cauzei interne similare analizată *supra*.

Dispozițiile din proiectul de Lege privind autorizarea de către procuror pot genera totuși *confuzii*.

Pe de o parte, menținerea lor ar putea genera raționamente care să distingă între situațiile obișnuite și cele urgente (astfel cum o face proiectul de Lege) și, de aici, să susțină că, în cursul urmăririi penale, predarea de obiecte, înscrisuri sau date informatice și conservarea datelor informatice s-ar dispune în condiții diferite, fie de procuror (în situații obișnuite), fie de procuror cu obligația confirmării ulterioare din partea judecătorului de drepturi și libertăți (în cazuri urgente). Aceasta cu atât mai mult cu cât un atare raționament s-ar putea folosi și de argumentul că proiectul de Lege nu impune un standard inferior Regulamentului, ci dimpotrivă unul superior, ceea ce este permis legiuitorului național.

Pe de altă parte, confuzii pot să apară și din cauza plasării inadecvate a dispoziției în proiectul de Lege. Autorizarea provizorie de către procuror, în cazuri urgente, se regăsește în conținutul art. 4 privind ordinele de divulgare a datelor privind traficul și a datelor referitoare la conținut, deși autorizarea provizorie *nu privește aceste ordine*, ci pe cele menționate *la art. 2 și art. 3*, deci ordinele de păstrare (pentru toate categoriile de date) și pe cele de divulgare a datelor privind abonații și a datelor solicitate exclusiv în scopul identificării utilizatorului. Se naște astfel riscul unei interpretări eronate potrivit căreia posibilitatea autorizării provizorii de către procuror vizează divulgarea datelor privind traficul și a datelor referitoare la conținut, deși aceasta nu este permisă de Regulament.

Un ultim aspect potențial problematic ține de asimetria dintre alineatele art. 4 din proiectul de Lege. Astfel, alin. (2) permite procurorului să emită în cazuri de urgență atât ordine de păstrare, cât și ordine de divulgare a datelor privind abonații ori a datelor solicitate exclusiv în scopul identificării utilizatorului, iar alin. (3) îl obligă, fără distincție, să sesizeze judecătorul de drepturi și libertăți în termen de 48 de ore. Cu toate acestea, alin. (5) și (6) reglementează soluțiile pe care judecătorul le poate pronunța (confirmarea și infirmarea) exclusiv cu privire la „ordinul european de *divulgare* a probelor electronice", fiind însă omis cel „de *păstrare*".

III.3. Problema procedeului probatoriu intern pentru „datele referitoare la conținut”

După cum am arătat supra, la pct. 3.1 lit. c), proiectul de Lege asimilează ordinul de divulgare a datelor privind traficul și a datelor referitoare la conținut cu procedeul probatoriu al obținerii datelor de trafic și de localizare, reglementat la art. 152 C.pr.pen.

Dacă în privința datelor privind traficul asimilarea ni se pare corectă, în schimb apreciem că în privința datelor referitoare la conținut ea este eronată.

Datele referitoare la conținut sunt, conform art. 3 pct. 12 din Regulament, orice date în format digital, cum ar fi mesajele scrise, mesajele vocale, înregistrările video, imaginile și sunetele, *altele decât datele privind abonații sau datele privind traficul*. Datele de trafic și de localizare, la care se referă art. 152 C.pr.pen., nu sunt definite în chiar cuprinsul acestui articol, care nu mai trimite expres la legea specială după modificarea adusă prin Legea nr. 75/2016. Definițiile de referință rămân totuși cele stabilite la art. 2 alin. (1) lit. b) și c) din Legea nr. 506/2004, iar ele nu acoperă date de tipul celor indicate exemplificativ la art. 3 pct. 12 din Regulament.

Lipsa de corespondență între aceste categorii este evidentă.

Simpla împrejurare că Regulamentul are în vedere, grupat, ordinul de divulgare privind ambele categorii de date, nu poate reprezenta o justificare pentru ca, la nivel intern, asimilarea obținerii acestor date să se realizeze prin intermediul unui singur procedeu probatoriu. Regulamentul le oferă un tratament unitar *nu pentru că datele ar aparține aceleiași categorii*, ci pentru că divulgarea ambelor categorii de date prezintă un nivel mai ridicat de intruziune față de celelalte tipuri de probe electronice (datele privind abonații și datele solicitate exclusiv în scopul identificării utilizatorului), deci trebuie supuse aceluiași set de condiții restrictive [art. 5 alin. (4) din Regulament] și, totodată, notificării către autoritatea de executare [art. 8 din Regulament].

Asimilarea divulgării datelor referitoare la conținut cu procedeele probatorii interne este problematică. Tentația este, pe de o parte, de a realiza o trimitere la metoda de supraveghere a accesului la un sistem informatic [art. 138 alin. (1) lit. b) și alin. (3) C.pr.pen.] sau la procedeul percheziției informatice [art. 168 C.pr.pen.]. Totuși, poate fi remarcată o diferență importantă: prin acces și percheziție organul judiciar cercetează el însuși sistemul informatic, pe când ordinul european de divulgare presupune o obligație de predare pusă în sarcina unui terț, ceea ce îl face un instrument de cooperare, nu unul de investigare nemijlocită.

Pe de altă parte, s-ar putea susține că, în privința datelor referitoare la conținut, procedeul probatoriu corespondent din dreptul intern ar fi comunicarea de date informatice în temeiul art. 170 alin. (2) lit. a) C.pr.pen. Textul obligă orice persoană fizică sau juridică de pe teritoriul României să comunice datele informatice aflate în posesia sau sub controlul său, stocate într-un sistem informatic ori pe un suport de stocare a datelor informatice, fără a exclude din obiectul său conținutul comunicațiilor, spre deosebire de lit. b) a aceluiași alineat. Totuși, în dreptul intern, competența de a dispune acest procedeu probatoriu în faza de urmărire penală aparține organului de urmărire penală. De asemenea, procedeul nu este limitat la anumite categorii de infracțiuni. Or, față de definiția pe care Regulamentul o dă datelor referitoare la conținut și ținând cont de importanța majoră a acestor date pentru viața privată (este vorba inclusiv despre mesaje scrise sau vocale, imagini, sunete generate de o persoană și stocate de furnizor), este inacceptabilă varianta ca procurorul să le poată accesa fără un control judecătoresc prealabil și în orice tip de cauză penală.

În aceste condiții, opinăm că suntem mai degrabă în prezența unui procedeu sui-generis, pentru care nu trebuie căutată neapărat o corespondență exactă la nivel intern. Esențială ni se pare împrejurarea că emiterea ordinelor de divulgare referitoare la datele de conținut nu poate fi atribuită în competența procurorului, ci se circumscrie condițiilor stricte impuse de Regulament, între care emiterea de către un judecător [art. 4 alin. (2)] și limitarea la infracțiunile prevăzute la art. 5 alin. (4).

III.4. Executarea ordinelor în România, căi de atac și sancțiuni

Analiza nu ar fi completă fără câteva observații privind executarea, de către autoritățile române, a ordinelor emise în alte state membre, precum și regimul căilor de atac și pe cel sancționator, chestiuni pe care proiectul de Lege le reglementează la art. 6-9.

Art. 6 alin. (1) din proiectul de Lege desemnează parchetele drept autorități române de executare pentru ordinele emise, în alte state membre, în faza de urmărire penală. Opțiunea legiuitorului pare la prima vedere a fi conformă, întrucât Regulamentul lasă desemnarea autorității de executare în competența statelor membre, raportat la prevederile legale din dreptul național. Consecința ei este însă aceea că verificările prevăzute la art. 12 alin. (1) din Regulament, între care cea privitoare la imunități și privilegii, la normele referitoare la libertatea presei și, mai ales, aprecierea, potrivit lit. b), dacă executarea ordinului ar implica o încălcare vădită a unui drept fundamental garantat de art. 6 TUE și de Cartă, revin procurorului, care se pronunță prin ordonanță [art. 6 alin. (4)].

Art. 8 alin. (2) din proiectul de Lege condiționează recunoașterea ordinului de inexistența unuia dintre motivele de refuz prevăzute la art. 12 alin. (1) din Regulament, deși norma europeană corespondentă ipotezei pe care o reglementează, aceea a executării la cererea autorității emitente, este art. 16 alin. (2), care trimite la motivele de la art. 16 alin. (4), pentru ordinul de divulgare, și la cele de la art. 16 alin. (5), pentru ordinul de păstrare.

Or, lista de la art. 16 alin. (4) cuprinde motive care lipsesc din art. 12 alin. (1), între care acela că ordinul „nu a fost emis sau validat de o autoritate emitentă astfel cum se prevede la articolul 4”, acela că nu a fost emis pentru o infracțiune dintre cele prevăzute la art. 5 alin. (4) ori acela că serviciul nu intră sub incidența Regulamentului. Rezultă așadar că autoritatea română de executare nu ar putea refuza din oficiu recunoașterea nici măcar a unui ordin emis de o autoritate necompetentă potrivit Regulamentului, acest motiv rămânându-i accesibil doar pe calea obiecțiilor destinatarului, în condițiile art. 8 alin. (5) din proiectul de Lege, care trimite tocmai la art. 16 alin. (4) și (5) din Regulament.

La aceasta se adaugă împrejurarea că art. 12 din Regulament are în vedere doar ordinul de divulgare și se aplică exclusiv atunci când a existat o notificare în temeiul art. 8, iar extinderea lui la ordinul de păstrare este lipsită de temei.

Pe de altă parte, art. 8 alin. (6) și (7) din proiectul de Lege obligă autoritatea română de executare să soluționeze obiecțiile destinatarului în termen de 48 de ore. Termenul apare însă ca fiind imposibil de respectat ori de câte ori autoritatea are în vedere o soluție de nerecunoaștere sau de neexecutare, întrucât art. 16 alin. (7) din Regulament impune, înainte de o asemenea decizie, consultarea autorității emitente, iar aceasta din urmă dispune de cinci zile lucrătoare pentru a răspunde solicitării de informații suplimentare. Termenul intern este cu atât mai greu de explicat cu cât Regulamentul însuși acordă autorității de executare cinci zile lucrătoare pentru a decide asupra recunoașterii [art. 16 alin. (2) al doilea paragraf].

O altă necorelare privește emiterea certificatului. Astfel, potrivit art. 5 alin. (2) din proiectul de Lege, în cazurile prevăzute la art. 4 alin. (1) lit. a) certificatul este emis de procurorul care efectuează sau supraveghează urmărirea penală. Or, ipoteza vizată este tocmai aceea în care ordinul îl constituie, potrivit aceluiași proiect, încheierea judecătorului de drepturi și libertăți dată în condițiile art. 152 C.pr.pen., adică aceea în care autoritatea emitentă este judecătorul.

În privința căilor de atac, art. 7 din proiectul de Lege ridică, în raport cu art. 18 alin. (4) din Regulament, o altă problemă de corelare. Termenul de trei zile prevăzut la alin. (2) și (5) corespunde, într-adevăr, termenului general al contestației, prevăzut de art. 425^1 alin. (2) C.pr.pen.

Însă, potrivit art. 7 alin. (3) din proiectul de Lege, în cursul urmăririi penale contestația se soluționează de un judecător de drepturi și libertăți de la instanța căreia i-ar reveni competența să judece cauza în fond. Calea de atac este reglementată în cazul ordinelor europene de divulgare a probelor electronice, fără însă ca proiectul să distingă după cum acestea au ca obiect date privind abonații sau datele solicitate exclusiv în scopul identificării utilizatorului sau au ca obiect date de trafic și date referitoare la conținut. Or, cel puțin în cazul celei de-a doua categorii (date de trafic și date referitoare la conținut), chiar proiectul de Lege arată că ordinul de divulgare se emite de judecătorul de drepturi și libertăți. Prin urmare, rezultă că, în cazul acestor ordine, atât emiterea, cât și contestația sunt de competența aceleiași instanțe. Regula internă din cauzele similare este, dimpotrivă, aceea de la art. 425^1 alin. (5) C.pr.pen., potrivit căreia contestația se soluționează de judecătorul de drepturi și libertăți de la instanța *superioară* celei sesizate, în ședință publică. Proiectul de Lege o și aplică, de altfel, pentru celelalte faze, alin. (4) făcând trimitere la instanța ierarhic superioară.

Rezultă așadar o asimetrie greu de justificat, care lasă tocmai faza cea mai intruzivă fără control ierarhic.

Regimul sancționator ridică, la rândul său, o problemă la nivel de aplicabilitate. Art. 8 alin. (8) din proiectul de Lege stabilește o amendă judiciară „în cuantum minim de 100.000 lei, până la 2% din cifra de afaceri anuală înregistrată de furnizorul de servicii la nivel mondial în exercițiul financiar precedent".

Or, pentru orice furnizor a cărui cifră de afaceri anuală este mai mică de 5 milioane de lei, plafonul de 2% coboară sub pragul minim de 100.000 lei, încât minimul legal depășește maximul legal, iar textul devine fie inaplicabil, fie sursa unei sancțiuni vădit disproporționate.

IV. CONCLUZII

Scopul Regulamentului (UE) 2023/1543 nu este acela de a extinde transfrontalier procedeele probatorii reglementate de Codul de procedură penală, ci instituie un regim autonom de drept al Uniunii, cu propriile categorii de date, cu propriile autorități emitente și cu propriile condiții de emitere. Atât timp cât ordinul european este privit ca act al dreptului Uniunii, legiuitorul național are doar obligația de a desemna autoritățile competente pentru fiecare fază procesuală și să arate, prin condiția „cauzei interne similare", ce garanții ar fi trebuit respectate dacă aceleași date ar fi fost cerute de la un furnizor din România.

Din momentul în care ordinul european este definit prin actul procesual intern, adică prin ordonanța emisă potrivit art. 154 sau art. 170 alin. (2) lit. b) C.pr.pen. ori prin încheierea

pronunțată în temeiul art. 152 C.pr.pen., este posibil să se creeze o tensiune între dreptul intern și prevederile Regulamentului.

Analiza Regulamentului lasă deschise mai multe chestiuni pe care practica va trebui să le tranșeze. Domeniul de aplicare presupune un sediu desemnat ori un reprezentant legal aflat în alt stat membru, astfel încât ordinele europene nu pot fi folosite în situații pur interne. Sfera furnizorilor de servicii rămâne, la rândul ei, potențial incertă, criteriul numărului semnificativ de utilizatori fiind lipsit deopotrivă de prag și de mecanism de verificare.

În cazul serviciilor bazate pe inteligență artificială, condiția ca stocarea să fie o componentă definitorie a serviciului evidențiază problema stocării temporare a datelor referitoare la conținut. Cea mai mare relevanță practică o are însă necorespondența dintre clasificarea datelor din Regulament și cea cu care operează dreptul intern, în special tratarea datelor solicitate exclusiv în scopul identificării utilizatorului ca fiind puțin intruzive, deși în dreptul român ele sunt date de trafic, supuse regimului prevăzut de art. 152 C.pr.pen. și excluse expres din sfera de aplicabilitate a art. 170 alin. (2) lit. b) C.pr.pen.

La acestea se adaugă calificarea parolei stocate sub formă de valoare hash și regimul cheii criptografice aflate în sfera de control a furnizorului, precum și rolul atribuit furnizorului privat în verificarea imunităților, a privilegiilor și a libertății presei, pe baza unui certificat din care lipsesc tocmai motivarea proporționalității și descrierea faptei. Regulamentul nu conține, în fine, nicio normă privind admisibilitatea mijloacelor de probă astfel obținute.

Din perspectiva proiectului de Lege, necorelările identificate au de asemenea consecințe practice deosebite. Ele expun actele de urmărire penală unui risc de nelegalitate care nu se manifestă la momentul emiterii ordinului, ci abia ex post, în camera preliminară sau în fața instanței de judecată. Un ordin de păstrare emis de judecătorul de cameră preliminară ori de instanța de judecată, un ordin de divulgare a datelor privind abonații și a datelor solicitate exclusiv în scopul identificării utilizatorului emis de procuror fără autorizarea prealabilă a judecătorului de drepturi și libertăți, precum și un ordin de divulgare a datelor referitoare la conținut emis în condițiile art. 152 C.pr.pen. sunt, fiecare în parte, susceptibile de a fi contestate, primele două pe temeiul condiției cauzei interne similare, iar cel din urmă pentru că a fost dispus pe temeiul unui procedeu probatoriu care nu acoperă categoria de date vizată.

Camera Deputaților ar trebui, în opinia noastră, să intervină în raport cu următoarele aspecte:

i. Să renunțe la definirea ordinului european prin actul procesual intern și să se limiteze la desemnarea autorităților emitente și de executare pentru fiecare fază procesuală, lăsând condițiile de emitere să rezulte din Regulament, coroborat cu verificarea concretă, de la caz la caz, a condiției cauzei interne similare.

ii. Să corecteze asimilarea datelor referitoare la conținut cu procedeul obținerii datelor de trafic și de localizare, care nu le acoperă.

iii. Să reexamineze dispoziția privind autorizarea provizorie de către procuror, care fie dublează competența de drept comun a procurorului, fie instituie o derogare de la condiția autorizării judiciare fără corespondent într-o cauză internă similară, și este plasată într-un articol ce privește tocmai ordinele pentru care ea nu operează.

iv. Să reevalueze regimul procedural al căilor de atac și regimul sancționator al neîndeplinirii obligațiilor de către furnizorii de servicii.