

editorial

Dubla semnificație a zilei de 25 mai pentru protecția datelor care au caracter personal

The dual significance of May 25 for the protection of personal data

Prof. univ. dr. Augustin FUEREA*

„Trecutul unui individ se înregistrează în tot organismul său, găsindu-și expresia, mai ales, în trăsăturile feței, ochi și mâini”¹

Ziua de 25 mai va rămâne multă vreme, spre știința și în conștiința tuturor europenilor (din statele membre ale Uniunii Europene, dar nu numai), ca fiind ziua cu dublă semnificație: pe de o parte, este ziua care marchează intrarea în vigoare a Regulamentului (UE) 2016/679 privind protecția datelor², și, pe de altă parte, simbolizează data de la care acest regulament se aplică. Ce diferențiază cele două date? Din punct de vedere formal, nu le diferențiază decât anii în care se petrec cele două evenimente, și anume: 25 mai 2016 – data la care regulamentul a intrat în vigoare³, și 25 mai 2018 – data de la care se aplică⁴. Din punct de vedere juridic, diferența este, însă, una considerabilă. Intrarea în vigoare a regulamentului, la 25 mai 2016, echivalează cu instituirea în sarcina statelor membre ale UE a obligației de a realiza, la nivel național, adaptările legislative necesare pentru aplicarea acestuia, de la 25 mai 2018, de către toți destinatarii săi. Acesta este motivul pentru care, nu de puține ori, apar unele confuzii între data intrării în vigoare și data de la care se aplică

* Facultatea de drept, Universitatea „Nicolae Titulescu” din București, e-mail: augustin.fuerea@univnt.ro. ORCID ID: 0009-0005-9769-9720.

¹ Prof. dr. G. Marinescu despre Nicolae Popoviciu, în *Omule cunoaște-te. Studiu practic complet de caracterologie*, Ed. Sophia, București, 2002.

² Denumirea corectă și completă este următoarea: Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în JO L 119, 4 mai 2016.

³ Art. 99 alin. (1): „Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene” (data publicării a fost 4 mai 2016).

⁴ Art. 99 alin. (2): „Prezentul regulament se aplică de la 25 mai 2018”.

cea mai importantă reglementare în materie, de până acum, cu privire la protecția datelor cu caracter personal, și anume Regulamentul (UE) 2016/679, regulament al cărui obiect de reglementare reprezintă o componentă esențială a drepturilor fundamentale ale omului – „dreptul la viața privată și de familie”.

Adoptarea regulamentului și abrogarea directivei în materie de protecție a datelor persoanelor fizice, ambele fiind acte juridice ale UE de drept derivat, pot fi coroborate cu dobândirea personalității juridice de către Uniunea Europeană, potrivit art. 47 din Tratatul privind Uniunea Europeană⁵.

Oricum ar sta lucrurile, și în acest an, la data de 25 mai, avem motive întemeiate de dublă aniversare, și anume: 8 ani de la intrarea în vigoare a regulamentului și 6 ani de la aplicarea acestuia. Numărul anilor care au trecut de la cele două evenimente importante este, însă, nesemnificativ dacă îl raportăm la alte instrumente juridice de drept internațional și european. Este relevant să evidențiem acest aspect, deoarece, nu de puține ori, în cadrul deselor controverse care apar în această materie extrem de vie și prezentă în viața noastră a tuturor persoanelor vizate⁶ apar opinii potrivit cărora astfel de preocupări de reglementare la cele două niveluri (internațional și european) ar fi lipsit din atenția decidenților.

Faptul că lucrurile nu au stat deloc așa este pus în valoare chiar prin Declarația Universală a Drepturilor Omului, adoptată la 10 decembrie 1948 de Adunarea Generală a ONU, declarație care, prin uz și practică, a dobândit forță juridică obligatorie, ca instrument juridic internațional universal, la care, inclusiv Constituția României, republicată, face referire, la art. 20 alin. (1)⁷. Edificator, potrivit precizării de mai sus, este conținutul art. 12 din Declarație, conform căruia „Nimeni nu va fi supus la imixtiuni arbitrare în viața sa personală, în familia sa, în domiciliul lui sau în corespondența sa, nici la atingeri aduse onoarei și reputației sale. Orice persoană are dreptul la protecția legii împotriva unor asemenea imixtiuni sau atingeri”.

Fără a recurge la o prezentare exhaustivă a reperelor istorice relevante pentru protecția datelor care au caracter personal, activitate extrem de complexă și generoasă din perspectiva diversității abordărilor pe care le presupune, dar și a necesității specializării persoanelor implicate într-un astfel de demers, aducem în discuție, de data aceasta, unele instrumente juridice europene, ca reflectare a Declarației Universale a Drepturilor Omului, și anume: Convenția pentru apărarea Drepturilor Omului și a Libertăților fundamentale din 1950⁸, care, la art. 8, face vorbire despre dreptul la respectarea vieții private și de familie. Astfel, potrivit Convenției, „1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale. 2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea

⁵ După Tratatul de la Lisabona (2007/2009), a fost acordată o mai mare atenție acestui domeniu al reglementării, prin înlocuirea/abrogarea actelor juridice mai flexibile, cum este cazul directivei, în favoarea celor de mai mare rigoare care conțin drepturi și obligații directe pentru destinatari.

⁶ Prin „persoană vizată”, se înțelege „o persoană fizică identificată sau identificabilă” – potrivit art. 4 pct. 1 din Regulamentul (UE) 2016/679.

⁷ Art. 20 alin. (1): „Dispozițiile constituționale privind drepturile și libertățile cetățenilor vor fi interpretate și aplicate în concordanță cu Declarația Universală a Drepturilor Omului, cu pactele și cu celelalte tratate la care România este parte”.

⁸ Cunoscută sub denumirea de Convenția Europeană a Drepturilor Omului. Aceasta a intrat în vigoare în anul 1953.

națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora”.

La același nivel al importanței reglementărilor, se adaugă Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, care, la art. 1, precizează următoarele: „Scopul prezentei convenții este de a garanta pe teritoriul fiecărui stat parte, fiecărei persoane fizice, oricare ar fi cetățenia sa sau reședința sa, respectarea drepturilor și libertăților sale fundamentale și, în special, dreptul la viața privată, față de prelucrarea automatizată a datelor cu caracter personal care o privesc” (protecția datelor). Este motivul pentru care, la data de 28 ianuarie, în toate statele părți la convenție, se sărbătorește „Ziua europeană a protecției datelor cu caracter personal”.

În plan unional, rețin atenția, în primul rând, normele fundamentale, cum ar fi Tratatul privind Uniunea Europeană (TUE), Tratatul privind Funcționarea Uniunii Europene (TFUE) și Carta Drepturilor Fundamentale a UE. Astfel, în temeiul art. 16 alin. (1) TFUE, „orice persoană are dreptul la protecția datelor cu caracter personal care o privesc”. În acest sens, în temeiul art. 39 TUE, Consiliul Uniunii „adoptă o decizie de stabilire a normelor privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către statele membre, în exercitarea activităților care fac parte din domeniul de aplicare (...), precum și a normelor privind libera circulație a acestor date. Respectarea acestor norme face obiectul controlului unor autorități independente”. Acestor prevederi li se adaugă cele cuprinse în art. 8 din Carta Drepturilor Fundamentale a UE, potrivit căroră „(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora. (3) Respectarea acestor norme se supune controlului unei autorități independente”.

Toate acestea reprezintă voința tuturor statelor membre ale Uniunii Europene, fiind semnate și ratificate, în totalitate. Dar, poate cele mai importante, sunt numeroasele reglementări de drept derivat ale UE, între care Regulamentul privind protecția datelor cu caracter personal ocupă un loc de prim rang.

Semnificativă cu privire la importanța domeniului reglementat este chiar atenționarea Comisiei Europene, care, anterior aplicării Regulamentului (UE) 2016/679, în cuprinsul unei Comunicări intitulată *Protecție sporită, noi oportunități – Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecția datelor de la 25 mai 2018*⁹, preciza faptul că „După 25 mai 2018, Comisia va monitoriza îndeaproape aplicarea noilor norme și va fi pregătită să ia măsuri în cazul în care vor apărea probleme semnificative”¹⁰, „inclusiv recurgerea la procedura de constatare a neîndeplinirii obligațiilor”¹¹ de către statele membre (prin declanșarea procedurii de *infringement*), așa cum se precizează în conținutul aceleiași comunicări, alături de multe alte măsuri.

⁹ Comunicare a Comisiei către Parlamentul European și Consiliu, COM(2018) 43 final, Bruxelles, 24 ianuarie 2018, disponibilă la <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=COM:2018:43:FIN>, accesat la 23 aprilie 2024.

¹⁰ *Ibidem*, p. 17.

¹¹ *Ibidem*, p. 18.

Aceeași importanță a protecției datelor care au caracter personal rezidă și din propunerile Comisiei, în calitatea acesteia de executiv al UE, formulate cu prilejul bilanțului prezentat la împlinirea a 2 ani de la aplicarea Regulamentului privind protecția datelor care au caracter personal, între care, în sensul caracterului preventiv, nu doar sancționator, s-a lansat ideea înființării „Academiei de protecție a datelor”, în scopul de a „facilita și a sprijini schimburile dintre autoritățile de reglementare europene și internaționale”¹².

Contextul multiplu oferit de perioada pandemică/post pandemică, la care se adaugă digitalizarea fără precedent, cu toate consecințele din domeniul inteligenței artificiale și, fără îndoială, războaiele hibride, dar și cele clasice duse în proximitatea frontierelor țării noastre, și nu numai, reprezintă tot atâtea temeuri ale consolidării preocupărilor, inclusiv în domeniul protecției datelor care au caracter personal. Consecințele, îndeosebi negative, generate de acest context multiplu sunt de natură să determine o conduită din ce în ce mai conștientă și responsabilă în materie, pregătirea în sensul aplicării legislației interne, europene și internaționale fiind singura de natură să contribuie la prevenirea săvârșirii unor fapte contrare exigențelor care țin de normalitatea și firescul vieții. Echilibrul între drepturi și obligații, între reguli și excepții, între conduita angajaților și cea a angajatorilor este singurul care contribuie la prevenirea exagerărilor și chiar a abuzurilor pe care, în mod inevitabil, le întâlnim transpuse în sesizările și reclamațiile formulate, atât în mediul public, cât și în cel privat. Riscurile, vulnerabilitățile și amenințările, din perspectivă tehnică, naturală ori umană, se pot estompa sau, dimpotrivă, se pot multiplica în funcție de atenția, respectiv preocuparea pentru cunoașterea, înțelegerea și aplicarea legislației domeniului, de la nivel național, european și internațional. Un rol important revine, deopotrivă, jurisprudenței și doctrinei, ambele fiind din ce în ce mai consistente și generatoare de optimism, atât de necesar în această etapă a evoluției societății omenești (interne, europene și internaționale), când asistăm la apariția unor metode mult prea intruzive în viața privată, inclusiv de familie, a persoanei fizice, dobândind forme, uneori și dimensiuni, greu de imaginat.

¹² Comunicarea Comisiei către Parlamentul European și Consiliu, „Protecția datelor ca pilon al capacității cetățenilor și al abordării UE privind tranziția digitală – doi ani de aplicare a Regulamentului general privind protecția datelor”, COM(2020) 264 final, Bruxelles, 24 iunie 2020, disponibilă la <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0264>, accesată la 23 aprilie 2024.

Câteva clarificări jurisprudențiale privind răspunderea operatorului în cazul nerespectării obligației de a asigura securitatea prelucrărilor

Some Judicial Clarifications on Operator Liability for Failing to Ensure Processing Security

Lect. univ. dr. Dana VOLOSEVICI*

▣ Rezumat

Problematika legată de măsurile tehnice și organizatorice în contextul RGPD reprezintă o provocare complexă, deoarece necesită o analiză transdisciplinară care să integreze aspecte tehnice, juridice și organizaționale. În acest context, clarificările jurisprudențiale oferite de Curtea de Justiție a Uniunii Europene joacă un rol crucial pentru o interpretare unitară și corectă a prevederilor RGPD, oferind ghidajul necesar atât operatorilor de date, cât și autorităților de supraveghere. Articolul își propune să analizeze problematica întinderii obligației operatorului pentru asigurarea securității prelucrării datelor cu caracter personal și a răspunderii acestuia în cazul încălcării articolelor 24 și 32 din RGPD, prin raportare în principal la cauza VB c. Natsionalna agentsia za prihodite (C-340/21).

Cuvinte-cheie: RGPD, măsuri tehnice și organizatorice, date personale, securitatea prelucrării, sarcina probei, răspundere

▣ Abstract

The challenge of implementing technical and organizational measures under the GDPR is multifaceted, requiring a transdisciplinary analysis that encompasses technical, legal, and organizational dimensions. Judicial clarifications from the Court of Justice of the European Union are pivotal in providing a unified and accurate interpretation of GDPR provisions, thereby offering essential guidance to both data controllers and supervisory authorities. This paper examines the scope of the controller's obligation to ensure the security of personal data processing and its liability in the event of breaches of Articles 24 and 32 of the GDPR, with a particular focus on the VB v. Natsionalna agentsia za prihodite case (C-340/21).

Keywords: GDPR, technical and organizational measures, data, security of processing, burden of proof, liability

* Universitatea Petrol și Gaze din Ploiești.

Prelucrarea datelor cu caracter personal se realizează în limitele generate de necesitatea asigurării protecției dreptului fundamental al persoanei la protecția datelor cu caracter personal care o privesc, drept statuat de art. 8 alin. (1) din Carta drepturilor fundamentale a Uniunii Europene și de art. 16 alin. (1) din Tratatul privind funcționarea Uniunii Europene (TFUE). În acest cadru, Regulamentul General privind Protecția Datelor impune operatorilor să adopte măsuri tehnice și organizatorice pentru a proteja datele personale, pentru a asigura conformitatea cu cerințele legale, pentru a proteja intimitatea individuală și pentru a permite prelucrarea și utilizarea securizată a acestor date. Conținutul concret al obligației de a implementa măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului nu este în afara dezbaterilor doctrinare și judiciare, cu atât mai mult cu cât art. 32 constituie una dintre cele mai încălcate dispoziții ale Regulamentului¹. O parte a doctrinei a analizat din punct de vedere cantitativ² sancțiunile aplicate pentru nerespectarea obligației de a asigura securitatea prelucrărilor, alte studii au o abordare calitativă³ bazată pe o serie de interviuri legate de provocările implementării măsurilor de securitate, în timp ce alte articole analizează prevederile legale cu instrumentele interpretării juridice⁴. O serie de hotărâri ale Curții de Justiție a Uniunii Europene au clarificat modalitatea de interpretare a prevederilor articolelor 24 și 32 din RGPD, ceea ce permite o nuanțare a analizelor anterioare, în lumina noii jurisprudențe în materie. Articolul își propune să analizeze problematica întinderii obligației operatorului pentru asigurarea securității prelucrării datelor cu caracter personal și a răspunderii acestuia în cazul încălcării articolelor 24 și 32 din RGPD, prin raportare în principal la cauza *Natsionalna agentsia za prihodite* (C-340/21)⁵.

Obligația operatorului de a implementa măsuri tehnice și organizatorice adecvate derivă din „principiul responsabilității”, prevăzut de art. 5 alin. (2), și trebuie interpretată în lumina abordării bazate pe riscuri pe care este fondat Regulamentul⁶. În temeiul acestui principiu, operatorul are responsabilitatea de a lua măsuri corespunzătoare, eficiente, adaptate și proactive pentru a asigura respectarea

¹ C. Barrett, *Emerging Trends from the First Year of EU GDPR Enforcement*, Scitech Lawyer 16, 3 (2020), pp. 22-35; J. Ruohonen, K. Hjerpe, *The GDPR enforcement fines at glance*, Information Systems 106 (2022), 101876; T. Marjanov, M. Konstantinou, M. Jozwiak, D. Spagnuolo, *Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR*, Proceedings on Privacy Enhancing Technologies 2023(3), pp. 405-417.

² J. Wolff, N. Atallah, *Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020*, Journal of Information Policy 11 (2021), pp. 63-103.

³ K. Hjerpe, J. Ruohonen, V. Leppänen, *The general data protection regulation: requirements, architectures, and constraints*, The 27th International Requirements Engineering Conference. IEEE, Jeju Island, South Korea, 2019, pp. 265-275.

⁴ S.-D. Șchiopu, *Privire generală asupra măsurilor tehnice și organizatorice necesare pentru implementarea efectivă a Regulamentului general privind protecția datelor*, Revista Română de Drept al Afacerilor nr. 2/2019, pp. 51-58; C. Lambrinou, *The general data protection regulation (GDPR) era: ten steps for compliance of data processors and data controllers*, International Conference on Trust and Privacy in Digital Business, Springer, Regensburg, Germany, 2018, pp. 3-8.

⁵ CJUE, Hotărârea din 14 decembrie 2023, C-340/2021, *VB c. Natsionalna agentsia za prihodite*.

⁶ C. Docksey, *Article 24. „Responsibility of the controller”*, în C. Kuner, L.A. Bygrave, C. Docksey, L. Drechsler, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 561.

principiilor reglementate în art. 5 alin. (1) și a Regulamentului în ansamblul său și de a dovedi această respectare.

În art. 24 alin. (1), GDPR stabilește o obligație generală pentru operator de a pune în aplicare măsuri tehnice și organizatorice adecvate, pentru a garanta că prelucrarea se efectuează în conformitate cu prevederile regulamentului. Măsurile trebuie instituite numai după efectuarea unei analize asupra naturii, domeniului de aplicare, contextului și scopurilor prelucrării, precum și după determinarea riscurilor și a gradelor de probabilitate și gravitate ale acestora pentru drepturile și libertățile persoanelor fizice. În raportul de analiză trebuie stabilite și termenele și/sau cauzele de revizuire și de actualizare a măsurilor. Obligația privind punerea în aplicare a măsurilor tehnice și organizatorice adecvate este dublată de aceea de a putea demonstra că prelucrarea se realizează în conformitate cu prevederile regulamentului. Art. 24 alin. (3) statuează că un element prin care poate fi demonstrată respectarea obligațiilor de către operator ar putea fi aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat.

Codurile de conduită RGPD sunt instrumente voluntare de responsabilizare, care stabilesc norme specifice de protecție a datelor pentru categoriile de operatori și persoane împuternicite de operatori⁷. Codurile sunt întocmite de asociații sau de alte organisme care reprezintă categorii de operatori sau de către persoane împuternicite de operatori, în scopul de a specifica modul de aplicare a regulamentului. Aceste coduri au un conținut variat, astfel cum prevede lista neexhaustivă cuprinsă în art. 40 alin. (2) din RGPD, și pot include măsurile și procedurile menționate la art. 24 și 25, precum și măsurile de asigurare a securității prelucrării, menționate la art. 32. Proiectul de cod, sau, după caz, de modificare sau de extindere a unui cod existent cu aplicabilitate la nivel național este supus cenzurii autorității de supraveghere, care emite un aviz de conformitate și care aprobă proiectul în cazul în care se constată că acesta oferă garanții adecvate suficiente. În cazul în care proiectul de cod de conduită, sau, după caz, de modificare sau de extindere vizează activități de prelucrare din mai multe state membre, înainte de aprobare, autoritatea de supraveghere competentă este obligată să îl transmită Comitetului, care reprezintă autoritatea competentă pentru emiterea avizului de conformitate. Avizul emis de Comitet trebuie transmis Comisiei, care poate adopta acte de punere în aplicare pentru a decide că respectivul cod de conduită are valabilitate generală în Uniune.

În ceea ce privește certificarea, în contextul articolelor 42 și 43 din RGPD, noțiunea face trimitere la atestarea efectuată de o terță parte în legătură cu operațiunile de prelucrare realizate de operatori și de persoanele împuternicite de către operatori⁸. Art. 42 alin. (5) prevede că certificarea se emite de către un organism de certificare acreditat sau de către o autoritate de supraveghere competentă. Autoritatea de supraveghere poate decide, în mod liber, să aleagă una sau mai multe dintre următoarele opțiuni:

- să emită ea însăși certificarea, cu respectarea propriului său sistem de certificare;

⁷ European Data Protection Board, *Orientările nr. 1/2019 privind codurile de conduită și organismele de monitorizare prevăzute în Regulamentul (UE) 2016/679, Versiunea 2.0*, 4 iunie 2019, p. 7.

⁸ European Data Protection Board, *Orientările nr. 1/2018 privind certificarea și identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulament*, Versiunea 3.0, 4 iunie 2019, p. 9.

- să emită ea însăși certificarea, cu respectarea propriului său sistem de certificare, dar să delege total sau parțial procesul de evaluare către terțe părți;
- să își creeze propriul sistem de certificare și să încredințeze procedura de certificare organismelor de certificare, care emit certificarea; și
- să încurajeze piața să elaboreze mecanisme de certificare⁹.

În ceea ce privește organismele de certificare, în conformitate cu prevederile art. 43 din RGPD, statele membre se asigură că acestea pot fi acreditate de organismul național de acreditare desemnat în temeiul Regulamentului (CE) nr. 765/2008¹⁰, în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea națională de supraveghere. În acest sens, prin Decizia nr. 20/2021¹¹, Autoritatea Națională din România a aprobat cerințele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679.

În domeniul strict al asigurării securității prelucrărilor, art. 32 (1) din GDPR stabilește, cu titlu exemplificativ, o serie de măsuri tehnice și organizatorice, despre care precizează că trebuie cenzurate în funcție de o serie de criterii, prevăzute, de asemenea, de Regulament, respectiv stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice. Alineatul (2) prevede că evaluarea nivelului adecvat de securitate trebuie efectuată în funcție de criterii precum riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Și în materia asigurării securității prelucrărilor, aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor legale.

Instituirea măsurilor tehnice și organizatorice constituie o problemă de apreciere și analiză de riscurilor, ceea ce, din punct de vedere juridic, naște problema stabilirii întinderii obligației de asigurare a securității prelucrării. O primă observație care se impune a fi făcută privește sursa normativă, națională sau europeană, care trebuie analizată pentru determinarea întinderii acestei obligații. Astfel, conform jurisprudenței europene, termenii unei dispoziții a dreptului Uniunii care nu conține nicio trimitere expresă la dreptul statelor membre pentru a stabili sensul și domeniul său de aplicare trebuie, în mod normal, să primească în întreaga Uniune o interpretare autonomă și uniformă¹². Rezultă așadar că pentru stabilirea întinderii obligației de asigurare a securității trebuie făcută raportare la înțelegerea termenilor conform interpretării dreptului Uniunii.

⁹ *Ibidem*.

¹⁰ *Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93*, publicat în JOUE L 218, 13 august 2008.

¹¹ *Decizie nr. 20 din 24 iunie 2021 privind aprobarea Cerințelor suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679 emisă de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*, publicată în M. Of. nr. 689 din 12 iulie 2021.

¹² CJUE, Hotărârea din 22 iunie 2021, *Latvijas Republikas Saeima (Puncte de penalizare)* C-439/19, EU:C:2021:504, pct. 81, și Hotărârea din 10 februarie 2022, *ShareWood Switzerland*, C-595/20, EU:C:2022:86, pct. 21.

Pe fond, trebuie observat că, atât în art. 24, cât și în art. 32, legiuitorul european se raportează la conceptul de adecvare („operatorul pune în aplicare măsuri tehnice și organizatorice *adecvate* (s.n.) pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament” [art. 24 (1)]; „operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice *adecvate* (s.n.) în vederea asigurării unui nivel de securitate corespunzător acestui risc” [art. 32 (1)]; „la evaluarea nivelului adecvat (s.n.) de securitate” [art. 32 (1)]. Utilizarea acestui concept demonstrează că regulamentul nu stabilește o obligație de *eliminare* (s.n.) a riscurilor de încălcare a securității datelor cu caracter personal¹³, ci „institue un regim de gestionare a riscurilor”¹⁴, care presupune că măsurile adoptate pentru protejarea sistemelor informatice trebuie să atingă „un nivel de acceptabilitate”¹⁵, atât din punct de vedere tehnic (relevanța măsurilor), cât și calitativ (eficacitatea protecției). Jurisdicția europeană învederează chiar că evaluarea caracterului adecvat trebuie făcută „în mod concret”, examinând dacă măsurile adoptate au fost implementate „ținând seama de diferitele criterii prevăzute la articolele menționate și de nevoile de protecție a datelor inerente în mod specific prelucrării în cauză, precum și riscurilor pe care le presupune aceasta din urmă”¹⁶. În același sens, considerentul 83 al RGPD statuează că „în vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru *atenuarea* (s.n.) acestor riscuri”, stabilind astfel că limitele obligației sunt conferite de conceptul de *atenuare*, iar nu de *eliminare*.

În acest cadru legal, măsurile luate pot fi dintre cele mai diverse¹⁷, regulamentul însuși enumerând în art. 32 alin. (1) o serie de măsuri: pseudonimizarea¹⁸ și criptarea datelor cu caracter personal; capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare; capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică; un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Ceea ce este important a fi punctat, întrucât este relevant pentru stabilirea răspunderii operatorului, este aceea că Regulamentul nu impune un model inflexibil de securitate a prelucrării, care să fie transpus prin stabilirea unui set de măsuri de securitate prestabilite. Din contră, este adoptată metodologia specifică standardelor internaționale privind gestionarea riscurilor aferente sistemelor de informații. O

¹³ M. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, în V. Cuffaro, R. D’Orazio, V. Ricciuto, *I dati personali nel diritto europeo*, Giappichelli, 2019, p. 1059.

¹⁴ CJUE, Hotărârea din 4 mai 2023, *UI c. Österreichische Post AG*, C-340/21, ECLI:EU:C:2023:986, pct. 29.

¹⁵ CJUE, Concluziile Avocatului General Domnul Giovanni Pitruzzella prezentate la 27 aprilie 2023, Cauza C-340/21, *VB c. Natsionalna agentsia za prihodite*.

¹⁶ CJUE, Hotărârea din 4 mai 2023, *UI c. Österreichische Post AG*, C-340/21, ECLI:EU:C:2023:986, pct. 30.

¹⁷ J. Hagen, E. Albrechtsen, J. Hovden, *Implementation and effectiveness of organizational information security measures*, *Information Management & Computer Security*, 16 (2008), pp. 377-397.

¹⁸ A se vedea și M. Hintze, G. LaFever, *Meeting Upcoming GDPR Requirements While Maximizing the Full Value of Data Analytics*, *Cybersecurity*, 2017, <https://doi.org/10.2139/SSRN.2927540>.

analiză¹⁹ a standardelor²⁰ în materie a relevat că poate fi identificată următoarea metodă sistematică:

- Pasul 1: Identificarea activităților bazate pe riscuri în toate standardele comparate (căutare pe cuvântul cheie „Risk”);
- Pasul 2: Maparea secțiunilor/cerințelor;
- Pasul 3: Descrierea relațiilor sau a punctelor de conexiune între activitățile bazate pe riscuri și cerințele aferente.

Mai mult decât atât, conceptul de „atenuare a riscurilor”, menționat expres de considerentul 83 din RGPD, este parte integrală a cadrului de gestionare a riscurilor, precum ISO 31000, care oferă linii directoare și bune practici în materie. Astfel, scopul atenuării riscurilor este de a reduce probabilitatea și consecințele evenimentelor adverse, iar principalele strategii utilizate pot fi, în funcție de situația concretă, evitarea riscului, reducerea riscului, fie că este vorba despre probabilitatea sau de impactul acestuia, partajarea riscului sau, în unele situații, acceptarea riscului²¹.

Rezultă așadar că întinderea obligației operatorului de a asigura securitatea prelucrării trebuie analizată prin raportare la conceptul de *atenuare a riscurilor*, iar nu de *eliminare* a acestora. În acest sens, Curtea de Justiție a UE a stabilit în Cauza 340/2021 că o divulgare neautorizată de date cu caracter personal sau un acces neautorizat la asemenea date de către „părți terțe” în sensul art. 4 pct. 10 din RGPD nu sunt în sine suficiente pentru a considera că măsurile tehnice și organizatorice implementate de operatorul în cauză nu erau „adecvate”, în sensul articolelor 24 și 32, și că operatorului trebuie să îi fie permis să facă proba contrară.

Pentru a face proba contrară, trebuie stabilit caracterul adecvat al măsurilor luate. Or, așa cum am arătat, în conformitate cu regulile aplicabile în materia standardelor de gestionare a riscurilor, ulterior analizei de risc efectuate, operatorul „dispune de o anumită marjă de apreciere”²² pentru a stabili măsurile ce urmează a fi implementate, cu condiția ca acestea să fie eficiente pentru gestionarea riscurilor identificate.

Într-un prim rând, măsurile luate trebuie să țină cont de „stadiul actual al dezvoltării”, sintagmă care stabilește cele două limite ale obligației operatorului. Pe de o parte, la limita superioară a obligației, operatorul trebuie să identifice toate măsurile care sunt disponibile în momentul realizării analizei, orice triere ulterioară trebuind să fie făcută plecând de la această mulțime. Dintre aceste măsuri, o parte vor fi înlăturate ca urmare a aplicării altor criterii, menționate, de asemenea, de art. 32 (1), inclusiv cele vizând costurile implementării. Abordând problematica legată de costuri, avocatul general G. Pitruzzella învederează că aprecierea caracterului adecvat al

¹⁹ B. Barafort, A. Mesquida, A. Picahaco, *Integrating risk management in IT settings from ISO standards and management systems perspectives*, Computer Standards & Interfaces, 54, 2017, pp. 176-185, <https://doi.org/10.1016/j.csi.2016.11.010>.

²⁰ Standardele care au stat la baza analizei sunt: *ISO 31000:2009 Risk management – principles and guidelines*, *ISO Annex SL: high-level structure for management system standards*, *ISO 9001:2015 Quality management systems – requirements*, *ISO 21500:2012 Guidance on project management*, *ISO 20000-1:2011 IT service management – service management system requirements*, *ISO 27001:2013 Information security management*.

²¹ P. Hopkin, *Fundamentals of Risk Management*, Kogan Page Ltd, 2021; D. Hillson (eds), *The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk*, Kogan Page Ltd, 2023.

²² CJUE, Hotărârea din 14 decembrie 2023, C-340/2021, *VB c. Natsionalna agentsia za prihodite*, pct. 43.

măsurilor implementate trebuie să se bazeze pe o evaluare comparativă, care să respecte cerințele principiului proporționalității, între interesele persoanei vizate, care tind, în general, să se situeze la un nivel mai ridicat de protecție, și interesele economice și capacitatea tehnologică a operatorului, care uneori tind să se situeze la un nivel de protecție mai scăzut²³.

Pe de altă parte, obligația operatorului de a implementa măsuri de securitate nu poate fi stabilită prin raportare la mai mult decât soluțiile pe care le oferă stadiul actual al științei, tehnicii, tehnologiei și cercetării, soluții care trebuie să fie validate ca atare de comunitatea științifică și care să fie disponibile publicului. Trebuie punctat totuși că noțiunea de „actual” evoluează rapid în materia tehnologiei informației și că operatorul are obligația de a revizui și actualiza măsurile tehnice și organizatorice puse în aplicare [art. 24 (1) teza finală]. Rezultă așadar că operatorul, pe lângă faptul că trebuie să identifice măsurile adecvate, este obligat să stabilească, prin raportare la analiza de risc efectuată, și intervalele de timp la care acestea trebuie revizuite și actualizate.

Din analiza cazurilor sancționate de autoritățile de supraveghere a prelucrărilor de date cu caracter personal, au fost considerate ca măsuri neadecvate, spre exemplu, cele în care cerințele de parolă pentru conturile utilizatorilor au fost insuficiente²⁴; mecanismul de criptare a datelor bancare prezenta vulnerabilități²⁵; s-a utilizat protocolul http, care este vulnerabil la atacurile informatice²⁶.

În ceea ce privește riscurile care trebuie acoperite de măsurile implementate, la evaluarea nivelului adecvat de securitate trebuie să se identifice cu precădere riscurile pe care le prezintă prelucrarea datelor, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod [considerent 83 și art. 32 alin. (2)]. În situația în care din analiza efectuată ar rezulta că unul sau mai multe tipuri de prelucrare, în special dintre cele bazate pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul va trebui să efectueze, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal [art. 35 alin. (1)] din RGPD. În acest caz, conținutul minimal al raportului de evaluare este prevăzut expres de alin. (7) al art. 35 din RGPD. Astfel, evaluarea va conține descrierea sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării; evaluarea necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri; evaluarea riscurilor pentru drepturile și libertățile persoanelor vizate; măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele stabilite. Măsurile preconizate trebuie să asigure protecția datelor cu caracter personal, iar operatorul trebuie să demonstreze conformitatea cu dispozițiile RGPD, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor

²³ CJUE, Concluziile Avocatului General Domnul Giovanni Pitruzzella prezentate la 27 aprilie 2023, *Cauza C-340/21, VB c. Natsionalna agentsia za prihodite*, pct. 36.

²⁴ CNIL, *Deliberarea formației restrânse nr. SAN-2023-008 din 8 iunie 2023 privind societatea KG COM*, CNIL, *Deliberarea formației restrânse nr. SAN-2022-021 din 24 noiembrie 2022 privind societatea Électricité de France*.

²⁵ CNIL, *Deliberarea formației restrânse nr. SAN-2023-008 din 8 iunie 2023 privind societatea KG COM*.

²⁶ CNIL, *Deliberarea formației restrânse nr. SAN-2023-006 din 11 mai 2023 privind societatea Doctissimo*.