CUPRINS

editorial

Dubla semnificaţie a zilei de 25 mai pentru protecţia 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-şi expresia, mai ales, în trăsăturile feţei, ochi şi mâini"[1]

Ziua de 25 mai va rămâne multă vreme, spre ştiinţa şi în conştiinţa tuturor europenilor (din statele membre ale Uniunii Europene, dar nu numai), ca fiind ziua cu dublă semnificaţie: pe de o parte, este ziua care marchează intrarea în vigoare a Regulamentului (UE) 2016/679 privind protecţia datelor[2], şi, pe de altă parte, simbolizează data de la care acest regulament se aplică. Ce diferenţiază cele două date? Din punct de vedere formal, nu le diferenţiază decât anii în care se petrec cele două evenimente, şi anume: 25 mai 2016 – data la care regulamentul a intrat în vigoare[3],, şi 25 mai 2018 – data de la care se aplică[4]. Din punct de vedere juridic, diferenţa este, însă, una considerabilă. Intrarea în vigoare a regulamentului, la 25 mai 2016, echivalează cu instituirea în sarcina statelor membre ale UE a obligaţiei de a realiza, la nivel naţional, adaptările legislative necesare pentru aplicarea acestuia, de la 25 mai 2018, de către toţi destinatarii săi. Acesta este motivul pentru care, nu de puţine ori, apar unele confuzii între data intrării în vigoare şi 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 protecţia datelor cu caracter personal, şi anume Regulamentul (UE) 2016/679, regulament al cărui obiect de reglementare reprezintă o componentă esenţială a drepturilor fundamentale ale omului – „dreptul la viaţa privată şi 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 personalităţii juridice de către Uniunea Europeană, potrivit art. 47 din Tratatul privind Uniunea Europeană[5].

Oricum ar sta lucrurile, şi 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 internaţional şi european. Este relevant să evidenţiem acest aspect, deoarece, nu de puţine ori, în cadrul deselor controverse care apar în această materie extrem de vie și prezentă în viaţa noastră a tuturor persoanelor vizate[6] apar opinii potrivit cărora astfel de preocupări de reglementare la cele două niveluri (internaţional şi european) ar fi lipsit din atenţia decidenţilor.

Faptul că lucrurile nu au stat deloc aşa este pus în valoare chiar prin Declaraţia Universală a Drepturilor Omului, adoptată la 10 decembrie 1948 de Adunarea Generală a ONU, declaraţie care, prin uz şi practică, a dobândit forţă juridică obligatorie, ca instrument juridic internaţional universal, la care, inclusiv Constituţia României, republicată, face referire, la art. 20 alin. (1)[7]. Edificator, potrivit precizării de mai sus, este conţinutul art. 12 din Declaraţie, conform căruia „Nimeni nu va fi supus la imixtiuni arbitrare în viaţa sa personală, în familia sa, în domiciliul lui sau în corespondenţa sa, nici la atingeri aduse onoarei şi reputaţiei sale. Orice persoană are dreptul la protecţia legii împotriva unor asemenea imixtiuni sau atingeri".

Fără a recurge la o prezentare exhaustivă a reperelor istorice relevante pentru protecţia datelor care au caracter personal, activitate extrem de complexă şi generoasă din perspectiva diversităţii abordărilor pe care le presupune, dar şi a necesităţii specializării persoanelor implicate într-un astfel de demers, aducem în discuţie, de data aceasta, unele instrumente juridice europene, ca reflectare a Declaraţiei Universale a Drepturilor Omului, şi anume: Convenţia pentru apărarea Drepturilor Omului şi a Libertăţilor fundamentale din 1950[8], care, la art. 8, face vorbire despre dreptul la respectarea vieţii private şi de familie. Astfel, potrivit Convenţiei, „1. Orice persoană are dreptul la respectarea vieţii sale private și de familie, a domiciliului său și a corespondenţei sale. 2. Nu este admis amestecul unei autorităţi publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege şi 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.

naţională, siguranţa publică, bunăstarea economică a ţării, apărarea ordinii şi prevenirea faptelor penale, protecţia sănătăţii, a moralei, a drepturilor şi a libertăţilor altora".

La acelaşi nivel al importanţei reglementărilor, se adaugă Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, care, la art. 1, precizează următoarele: „Scopul prezentei convenţii este de a garanta pe teritoriul fiecărui stat parte, fiecărei persoane fizice, oricare ar fi cetăţenia sa sau reşedinţa sa, respectarea drepturilor şi libertăţilor sale fundamentale şi, în special, dreptul la viaţa privată, faţă de prelucrarea automatizată a datelor cu caracter personal care o privesc" (protecţia datelor). Este motivul pentru care, la data de 28 ianuarie, în toate statele părţi la convenţie, se sărbătoreşte „Ziua europeană a protecţiei datelor cu caracter personal".

În plan unional, reţin atenţia, în primul rând, normele fundamentale, cum ar fi Tratatul privind Uniunea Europeană (TUE), Tratatul privind Funcţionarea Uniunii Europene (TFUE) şi Carta Drepturilor Fundamentale a UE. Astfel, în temeiul art. 16 alin. (1) TFUE, „orice persoană are dreptul la protecţia 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 protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către statele membre, în exercitarea activităţilor care fac parte din domeniul de aplicare (...), precum şi a normelor privind libera circulaţie a acestor date. Respectarea acestor norme face obiectul controlului unor autorităţi independente". Acestor prevederi li se adaugă cele cuprinse în art. 8 din Carta Drepturilor Fundamentale a UE, potrivit cărora „(1) Orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc. (2) Asemenea date trebuie tratate în mod corect, în scopurile precizate şi pe baza consimţământului 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 şi dreptul de a obţine rectificarea acestora. (3) Respectarea acestor norme se supune controlului unei autorităţi independente".

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

Semnificativă cu privire la importanţa domeniului reglementat este chiar atenţionarea Comisiei Europene, care, anterior aplicării Regulamentului (UE) 2016/679, în cuprinsul unei Comunicări intitulată *Protecţie sporită, noi oportunităţi – Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecţia datelor de la 25 mai 2018*[9], preciza faptul că „După 25 mai 2018, Comisia va monitoriza îndeaproape aplicarea noilor norme şi va fi pregătită să ia măsuri în cazul în care vor apărea probleme semnificative"[10], „inclusiv recurgerea la procedura de constatare a neîndeplinirii obligaţiilor"[11] de către statele membre (prin declanşarea procedurii de *infringement*), aşa cum se precizează în conţinutul aceleiaşi comunicări, alături de multe alte măsuri.

[9] Comunicare a Comisiei către Parlamentul European şi 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.

Aceeaşi importanţă a protecţiei datelor care au caracter personal rezidă şi din propunerile Comisiei, în calitatea acesteia de executiv al UE, formulate cu prilejul bilanţului prezentat la împlinirea a 2 ani de la aplicarea Regulamentului privind protecţia datelor care au caracter personal, între care, în sensul caracterului preventiv, nu doar sancţionator, s-a lansat ideea înfiinţării „Academiei de protecţie a datelor", în scopul de a „facilita şi a sprijini schimburile dintre autorităţile de reglementare europene şi internaţionale"[12].

Contextul multiplu oferit de perioada pandemică/post pandemică, la care se adaugă digitalizarea fără precedent, cu toate consecinţele din domeniul inteligenţei artificiale şi, fără îndoială, războaiele hibride, dar şi cele clasice duse în proximitatea frontierelor ţării noastre, şi nu numai, reprezintă tot atâtea temeiuri ale consolidării preocupărilor, inclusiv în domeniul protecţiei datelor care au caracter personal. Consecinţele, îndeosebi negative, generate de acest context multiplu sunt de natură să determine o conduită din ce în ce mai conştientă şi responsabilă în materie, pregătirea în sensul aplicării legislaţiei interne, europene şi internaţionale fiind singura de natură să contribuie la prevenirea săvârşirii unor fapte contrare exigenţelor care ţin de normalitatea şi firescul vieţii. Echilibrul între drepturi şi obligaţii, între reguli şi excepţii, între conduita angajaţilor şi cea a angajatorilor este singurul care contribuie la prevenirea exagerărilor şi chiar a abuzurilor pe care, în mod inevitabil, le întâlnim transpuse în sesizările şi reclamaţiile formulate, atât în mediul public, cât şi în cel privat. Riscurile, vulnerabilităţile şi ameninţările, din perspectivă tehnică, naturală ori umană, se pot estompa sau, dimpotrivă, se pot multiplica în funcţie de atenţia, respectiv preocuparea pentru cunoaşterea, înţelegerea şi aplicarea legislaţiei domeniului, de la nivel naţional, european şi internaţional. Un rol important revine, deopotrivă, jurisprudenţei şi doctrinei, ambele fiind din ce în ce mai consistente şi generatoare de optimism, atât de necesar în această etapă a evoluţiei societăţii omeneşti (interne, europene şi internaţionale), când asistăm la apariţia unor metode mult prea intruzive în viaţa privată, inclusiv de familie, a persoanei fizice, dobândind forme, uneori şi dimensiuni, greu de imaginat.

[12] Comunicarea Comisiei către Parlamentul European și Consiliu, „Protecția datelor ca pilon al capacitării 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 jurisprudenţiale privind răspunderea operatorului în cazul nerespectării obligaţiei de a asigura securitatea prelucrărilor

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

Lect. univ. dr. Dana VOLOSEVICI*

❑ Rezumat

Problematica 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 protecţiei dreptului fundamental al persoanei la protecţia datelor cu caracter personal care o privesc, drept statuat de art. 8 alin. (1) din Carta drepturilor fundamentale a Uniunii Europene şi de art. 16 alin. (1) din Tratatul privind funcţionarea Uniunii Europene (TFUE). În acest cadru, Regulamentul General privind Protecţia Datelor impune operatorilor să adopte măsuri tehnice şi organizatorice pentru a proteja datele personale, pentru a asigura conformitatea cu cerinţele legale, pentru a proteja intimitatea individuală şi pentru a permite prelucrarea şi utilizarea securizată a acestor date. Conţinutul concret al obligaţiei de a implementa măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului nu este în afara dezbaterilor doctrinare şi judiciare, cu atât mai mult cu cât art. 32 constituie una dintre cele mai încălcate dispoziţii ale Regulamentului[1]. O parte a doctrinei a analizat din punct de vedere cantitativ[2] sancţiunile aplicate pentru nerespectarea obligaţiei de a asigura securitatea prelucrărilor, alte studii au o abordare calitativă[3] bazată pe o serie de interviuri legate de provocările implementării măsurilor de securitate, în timp ce alte articole analizează prevederile legale cu instrumentele interpretării juridice[4]. O serie de hotărâri ale Curţii de Justiţie a Uniunii Europene au clarificat modalitatea de interpretare a prevederilor articolelor 24 şi 32 din RGPD, ceea ce permite o nuanţare a analizelor anterioare, în lumina noii jurisprudenţe în materie. Articolul îşi propune să analizeze problematica întinderii obligaţiei operatorului pentru asigurarea securităţii prelucrării datelor cu caracter personal şi a răspunderii acestuia în cazul încălcării articolelor 24 şi 32 din RGPD, prin raportare în principal la cauza *Natsionalna agentsia za prihodite* (C-340/21)[5].

Obligaţia operatorului de a implementa măsuri tehnice şi organizatorice adecvate derivă din „principiul responsabilităţii", prevăzut de art. 5 alin. (2), şi trebuie interpretată în lumina abordării bazate pe riscuri pe care este fondat Regulamentul[6]. În temeiul acestui principiu, operatorul are responsabilitatea de a lua măsuri corespunzătoare, eficiente, adaptate şi 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. Hjerppe, *The GDPR enforcement fines at glance*, Information Systems 106 (2022), 101876; T. Marjanov, M. Konstantinou, M. Jozwiak, D. Spagnuelo, *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. Hjerppe, 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. Lambrinoudakis, *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) şi a Regulamentului în ansamblul său şi de a dovedi această respectare.

În art. 24 alin. (1), GDPR stabileşte o obligaţie generală pentru operator de a pune în aplicare măsuri tehnice şi 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 şi scopurilor prelucrării, precum şi după determinarea riscurilor şi a gradelor de probabilitate şi gravitate ale acestora pentru drepturile şi libertăţile persoanelor fizice. În raportul de analiză trebuie stabilite şi termenele şi/sau cauzele de revizuire şi de actualizare a măsurilor. Obligaţia privind punerea în aplicare a măsurilor tehnice şi 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 obligaţiilor 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 protecţie a datelor pentru categoriile de operatori şi persoane împuternicite de operatori[7]. Codurile sunt întocmite de asociaţii 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 conţinut variat, astfel cum prevede lista neexhaustivă cuprinsă în art. 40 alin. (2) din RGPD, şi pot include măsurile şi procedurile menţionate la art. 24 şi 25, precum şi măsurile de asigurare a securităţii prelucrării, menţionate la art. 32. Proiectul de cod, sau, după caz, de modificare sau de extindere a unui cod existent cu aplicabilitate la nivel naţional este supus cenzurii autorităţii de supraveghere, care emite un aviz de conformitate şi care aprobă proiectul în cazul în care se constată că acesta oferă garanţii adecvate suficiente. În cazul în care proiectul de cod de conduită, sau, după caz, de modificare sau de extindere vizează activităţi 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 priveşte certificarea, în contextul articolelor 42 şi 43 din RGPD, noţiunea face trimitere la atestarea efectuată de o terţă parte în legătură cu operaţiunile de prelucrare realizate de operatori şi de persoanele împuternicite de către operatori[8]. 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 opţiuni:

- să emită ea însăşi 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 însăşi certificarea, cu respectarea propriului său sistem de certificare, dar să delege total sau parţial procesul de evaluare către terţe părţi;

• să îşi creeze propriul sistem de certificare şi să încredinţeze procedura de certificare organismelor de certificare, care emit certificarea; şi

• să încurajeze piaţa să elaboreze mecanisme de certificare[9].

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. 765/2008[10], 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. 20/2021[11], 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 securităţii prelucrărilor, art. 32 (1) din GDPR stabilește, cu titlu exemplificativ, o serie de măsuri tehnice și organizatorice, despre care precizează că trebuie cenzurate în funcţie 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 libertăţile persoanelor fizice. Alineatul (2) prevede că evaluarea nivelului adecvat de securitate trebuie efectuată în funcţie 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 securităţii 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 cerinţelor 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 obligaţiei de asigurare a securităţii prelucrării. O primă observaţie care se impune a fi făcută privește sursa normativă, națională sau europeană, care trebuie analizată pentru determinarea întinderii acestei obligaţii. Astfel, conform jurisprudenţei europene, termenii unei dispoziţii a dreptului Uniunii care nu conţine 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 uniformă[12]. Rezultă aşadar că pentru stabilirea întinderii obligaţiei de asigurare a securităţii trebuie făcută raportare la înţelegerea 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 şi în art. 32, legiuitorul european se raportează la conceptul de adecvare („operatorul pune în aplicare măsuri tehnice şi organizatorice *adecvate* (s.n.) pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament" [art. 24 (1)]; „operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi 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 stabileşte o obligaţie de *eliminare* (s.n.) a riscurilor de încălcare a securităţii datelor cu caracter personal[13], ci „instituie 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 (relevanţa măsurilor), cât şi calitativ (eficacitatea protecţiei). Jurisdicţia europeană învederează chiar că evaluarea caracterului adecvat trebuie făcută „în mod concret", examinând dacă măsurile adoptate au fost implementate „ţinând seama de diferitele criterii prevăzute la articolele menţionate şi de nevoile de protecţie a datelor inerente în mod specific prelucrării în cauză, precum şi riscurilor pe care le presupune aceasta din urmă"[16]. În acelaşi sens, considerentul 83 al RGPD statuează că „în vederea menţinerii securităţii şi a prevenirii prelucrărilor care încalcă prezentul regulament, operatorul sau persoana împuternicită de operator ar trebui să evalueze riscurile inerente prelucrării şi să implementeze măsuri pentru *atenuarea* (s.n.) acestor riscuri", stabilind astfel că limitele obligaţiei sunt conferite de conceptul de *atenuare*, iar nu de *eliminare*.

În acest cadru legal, măsurile luate pot fi dintre cele mai diverse[17], regulamentul însuşi enumerând în art. 32 alin. (1) o serie de măsuri: pseudonimizarea[18] şi criptarea datelor cu caracter personal; capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare; capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică; un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi 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 internaţionale privind gestionarea riscurilor aferente sistemelor de informaţii. 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.

analiză[19] a standardelor[20] în materie a relevat că poate fi identificată următoarea metodă sistematică:

• Pasul 1: Identificarea activităţilor bazate pe riscuri în toate standardele comparate (căutare pe cuvântul cheie „Risk”);

• Pasul 2: Maparea secţiunilor/cerinţelor;

• Pasul 3: Descrierea relaţiilor sau a punctelor de conexiune între activităţile bazate pe riscuri şi cerinţele aferente.

Mai mult decât atât, conceptul de „atenuare a riscurilor”, menţionat expres de considerentul 83 din RGPD, este parte integrală a cadrului de gestionare a riscurilor, precum ISO 31000, care oferă linii directoare şi bune practici în materie. Astfel, scopul atenuării riscurilor este de a reduce probabilitatea şi consecinţele evenimentelor adverse, iar principalele strategii utilizate pot fi, în funcţie de situaţia concretă, evitarea riscului, reducerea riscului, fie că este vorba despre probabilitatea sau de impactul acestuia, partajarea riscului sau, în unele situaţii, acceptarea riscului[21].

Rezultă aşadar că întinderea obligaţiei 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 Justiţie 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 „părţi terţe” în sensul art. 4 pct. 10 din RGPD nu sunt în sine suficiente pentru a considera că măsurile tehnice şi organizatorice implementate de operatorul în cauză nu erau „adecvate”, în sensul articolelor 24 şi 32, şi că operatorului trebuie să îi fie permis să facă proba contrară.

Pentru a face proba contrară, trebuie stabilit caracterul adecvat al măsurilor luate. Or, aşa 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 condiţia ca acestea să fie eficiente pentru gestionarea riscurilor identificate.

Într-un prim rând, măsurile luate trebuie să ţină cont de „stadiul actual al dezvoltării”, sintagmă care stabileşte cele două limite ale obligaţiei operatorului. Pe de o parte, la limita superioară a obligaţiei, operatorul trebuie să identifice toate măsurile care sunt disponibile în momentul realizării analizei, orice triere ulterioară trebuind să fie făcută plecând de la această mulţime. Dintre aceste măsuri, o parte vor fi înlăturate ca urmare a aplicării altor criterii, menţionate, 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 cerinţele principiului proporţionalităţii, între interesele persoanei vizate, care tind, în general, să se situeze la un nivel mai ridicat de protecţie, şi interesele economice şi capacitatea tehnologică a operatorului, care uneori tind să se situeze la un nivel de protecţie mai scăzut[23].

Pe de altă parte, obligaţia operatorului de a implementa măsuri de securitate nu poate fi stabilită prin raportare la mai mult decât soluţiile pe care le oferă stadiul actual al ştiinţei, tehnicii, tehnologiei şi cercetării, soluţii care trebuie să fie validate ca atare de comunitatea ştiinţifică şi care să fie disponibile publicului. Trebuie punctat totuşi că noţiunea de „actual" evoluează rapid în materia tehnologiei informaţiei şi că operatorul are obligaţia de a revizui şi actualiza măsurile tehnice şi organizatorice puse în aplicare [art. 24 (1) teza finală]. Rezultă aşadar că operatorul, pe lângă faptul că trebuie să identifice măsurile adecvate, este obligat să stabilească, prin raportare la analiza de risc efectuată, şi intervalele de timp la care acestea trebuie revizuite şi actualizate.

Din analiza cazurilor sancţionate de autorităţile de supraveghere a prelucrărilor de date cu caracter personal, au fost considerate ca măsuri neadecvate, spre exemplu, cele în care cerinţele de parolă pentru conturile utilizatorilor au fost insuficiente[24]; mecanismul de criptare a datelor bancare prezenta vulnerabilităţi[25]; s-a utilizat protocolul http, care este vulnerabil la atacurile informatice[26].

În ceea ce priveşte 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 şi art. 32 alin. (2)]. În situaţia 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 şi libertăţile persoanelor fizice, operatorul va trebui să efectueze, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal [art. 35 alin. (1)] din RGPD. În acest caz, conţinutul minimal al raportului de evaluare este prevăzut expres de alin. (7) al art. 35 din RGPD. Astfel, evaluarea va conţine descrierea sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării; evaluarea necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri; evaluarea riscurilor pentru drepturile şi libertăţile persoanelor vizate; măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele stabilite. Măsurile preconizate trebuie să asigure protecţia datelor cu caracter personal, iar operatorul trebuie să demonstreze conformitatea cu dispoziţiile RGPD, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi 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*.