

**DANIEL-MIHAIL ȘANDRU
IRINA ALEXE
(Editori)**

**LEGISLAȚIA UNIUNII EUROPENE
PRIVIND
PROTECȚIA DATELOR PERSONALE**



**EDITURA UNIVERSITARĂ
București, 2018**

SUMAR

Punerea în aplicare a Regulamentului General privind Protecția Datelor 2016/679. Experițe din România	7
LEGISLAȚIE:	
Tratatul privind Funcționarea Uniunii Europene – extras	25
Carta Drepturilor Fundamentale a Uniunii Europene – extras	26
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)...	28
Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului	156
Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave	221
Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală	245
Regulamentul (CE) 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date	266
Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice)	296
Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune	315

Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și al normelor privind serviciile societății informaționale...	355
Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic)...	373
Comunicare a Comisiei către Parlamentul European și Consiliu. Protecție sporită, noi oportunități - Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecția datelor de la 25 mai 2018 [Bruxelles, 24.1.2018 COM(2018) 43 final]	399
DOCUMENTE ALE GRUPULUI DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR:	
Ghid privind Responsabilul cu protecția datelor (‘DPOs’) [16/RO; WP 243 rev.01], revizuit și adoptat în data de 5 aprilie 2017.....	420
Orientări privind aplicarea și stabilirea unor amenzi administrative în sensul Regulamentului nr. 2016/679 [17/RO; GL 253], adoptate la 3 octombrie 2017.....	446
Orientări privind dreptul la portabilitatea datelor [16/RO GL 242 rev. 01], adoptate la 13 decembrie 2016; revizuite și adoptate ultima dată la 5 aprilie 2017..	462
Orientări privind dreptul la portabilitatea datelor. GL242 ANEXĂ – Întrebări frecvente	483
Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă [17/RO GL 249], adoptat la 8 iunie 2017	487
Orientări privind evaluarea impactului asupra protecției datelor (DPIA) și modul în care se determină dacă prelucrarea este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului 2016/679 [17/RO; WP 248 rev. 01], adoptate la 4 aprilie 2017; revizuite și adoptate la 4 octombrie 2017.....	514
Orientări pentru identificarea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de către operator [16/RO; GL 244 rev. 01], adoptate la 13 decembrie 2016, astfel cum au fost revizuite și adoptate ultima dată la 5 aprilie 2017.....	538
Avizul nr. 3/2017 privind prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative (STI cooperative) [17/RO; WP 252]; adoptat la 4 octombrie 2017	553
Orientări asupra consimțământului în temeiul Regulamentului 2016/679 [PROIECT] [17/RO; WP259], adoptate la 28 noiembrie 2017.	567

Punerea în aplicare a Regulamentului General privind Protecția Datelor 2016/679. Experiențe din România

The implementation of the General Data Protection Regulation 2016/679. Experience from Romania

Daniel-Mihail Șandru¹
Irina Alexe²

Rezumat:

În continuarea activităților de cercetare din domeniul dreptului la o viață privată, respectiv al dreptului privind protecția datelor cu caracter personal, prezentul material reprezintă metodologic o cercetare privind consecințele intrării în vigoare a Regulamentului General privind Protecția Datelor (GDPR, acronimul englezesc) în România. Acest articol urmărește să pună în evidență efectele practice ale intrării în vigoare, cadrul normativ european, mult mai dezvoltat decât pare la prima vedere, precum și eventualele implicații ale regulamentului, pentru judecătorul român.

Cuvinte cheie:

GDPR, judecător, protecția datelor, efecte practice, conformare; responsabil cu protecția datelor; sancțiuni.

Abstract:

In continuation of the research activities in the right to privacy field, namely the right to protect one's personal data, the present material is methodologically a research on the consequences of the General Data Protection Regulation's entry into force (also known as GDPR) in Romania. This article seeks to highlight the practical effects of the entry into force, the European normative framework, which is much more developed than it

¹ Prof. univ. dr. Universitatea Creștină „Dimitrie Cantemir”, Universitatea din București și Universitatea Petru Maior, Tîrgu-Mureș; fondator și coordonator al Centrului de Studii de Drept European (CSDE) din cadrul Institutului de Cercetări Juridice „Acad. Andrei Rădulescu” al Academiei Române; judecător ad-hoc la Curtea Europeană a Drepturilor Omului; adresa: Calea Victoriei, nr. 125, Sector 1, București; e-mail: mihai.sandru@csde.ro mihaisandru.ro.

² Cercetător științific asociat la Institutul de Cercetări Juridice „Acad. Andrei Rădulescu” al Academiei Române. Autor al unor volume și articole în domeniu, ariile sale de interes vizează dreptul administrativ, dreptul constituțional și dreptul european. Poate fi contactată la adresa irina_alex@yahoo.com.

might seem at a first glance, as well as the possible implications of the regulation for the Romanian judge.

Keywords:

GDPR, judge, data protection, practical effects, compliance; data protection officer; sanctions.

I. Intrarea în vigoare a Regulamentului General privind Protecția Datelor

În continuarea activităților de cercetare din domeniul dreptului la o viață privată, respectiv al dreptului privind protecția datelor cu caracter personal, prezentul material reprezintă metodologic o cercetare privind consecințele intrării în vigoare a Regulamentului General privind Protecția Datelor (GDPR, acronimul englezesc). În precedentele două conferințe organizate în cadrul mureșean³ am evidențiat teme centrale ale noului regulament, teme legate de fondul reglementării. Acest articol urmărește să pună în evidență efectele practice ale intrării în vigoare, cadrul normativ european, mult mai dezvoltat decât pare la prima vedere, precum și eventualele implicații ale regulamentului, pentru judecătorul român.

Internetul și noile tehnologii se găsesc într-un moment dual: pe de o parte dezvoltarea noilor tehnologii, pe de altă parte necesitatea reglementării. Reglementările se află și ele (oarecum) la început, dar și într-o stare de schimbare esențială, în mai multe domenii: neutralitatea internetului, protecția datelor, internetul lucrurilor (IoT). Protecția datelor este un subiect care a răsărit pe un teren neinclus în dezbaterile mari de până acum. Regulamentul privind protecția datelor reprezintă o declarație a drepturilor, chiar dacă teritorial ar părea cu efecte limitate. Cu toate acestea, datorită faptului că Regulamentul General privind Protecția Datelor se aplică tuturor cetățenilor europeni indiferent de sediul operatorilor, aplicarea teritorială devine în fapt globală. Protecția datelor pune în centru persoana

³ Acest material a fost pregătit pentru Conferința Națională ”Impactul Regulamentului General privind Protecția Datelor (GDPR) în domeniul sănătății (ed. a III-a)”, organizată la data de 22 martie 2018, de Universitatea de Medicină și Farmacie și Universitatea Petru Maior, ambele din Tîrgu-Mureș. Ca urmare, majoritatea exemplurilor din material sunt din domeniul medical, fără însă a le afecta aplicabilitatea în orice alt domeniu. Conferințele anterioare: *Conferința națională Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, 17 martie 2017 și Conferința internațională *Repere naționale și internaționale în domeniul GDPR (Regulamentul General privind Protecția Datelor)*, 14 decembrie 2017, ambele organizate de Universitatea Petru Maior, Tîrgu-Mureș.

vizată, reglementările având rolul nu doar de a o proteja în fața valului de descoperiri tehnico-științifice, dar și pentru a reglementa activitatea marilor organizații care prelucrează date cu caracter personal (magazine on-line, rețele sociale sau motoare de căutare).⁴ În domeniul medical, regulamentul a explicitat pe larg, chiar în preambul, semnificația datelor cu caracter medical, printr-o listă exhaustivă de date: „Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European și a Consiliului⁵; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.”

În România, directiva și legea referitoare la protecția datelor s-au aplicat și se interpretează de instanțele române, aspect dovedit de numărul mare de cauze soluționate.⁶

Nu toate problemele referitoare la informații, comunicare de informații publice sau confidențialitate sunt probleme de protecția datelor.

⁴ Cei mai importanți jucători din mediul on-line FAMGA (Facebook, Apple, Microsoft, Google and Amazon) consideră că sunt dezavantajați de GDPR, însă sunt în căutarea soluțiilor tehnice și a schimbării termenilor și condițiilor pentru a se conforma regulamentului.

⁵ Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45). Pe larg: **Gabriella Berki**, *Free Movement of Patients in the EU. A Patient's Perspective*, Intersentia, 2017.

⁶ Peste 200 au fost analizate în: **Daniel-Mihail Șandru, Dragoș-Alin Călin, Constantin-Mihai Banu**, *Aplicarea și interpretarea Directivei 95/46 de către instanțe române. Tipologii și consecințe juridice*, în vol. **Irina Alexe, Nicolae-Dragoș Ploșteanu, Daniel-Mihail Șandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 41.

Toate acestea însă au implicații și referitoare la protecția datelor. În special trebuie observate situațiile în care legi din domenii diferite (pază⁷) solicită informații care din punctul de vedere al regulamentul încalcă principiile referitoare la reducerea la minimum a datelor (art. 5 alin. 1 lit. c).

Potrivit art. 99 din regulament, intrarea în vigoare s-a făcut la 20 de zile de la publicarea în Jurnalul Oficial, urmând ca din 25 mai 2018 regulamentul să fie pus în aplicare.

II. Relația cu alte reglementări relevante

Regulamentul general privind protecția datelor face parte dintr-un sistem general de reglementare a informațiilor care se referă atât la domenii speciale de prelucrare a datelor cu caracter personal (datele în materie polițienească sau datele privind pasagerii) dar și comerțul electronic. Relațiile dintre aceste acte normative, precum și între acestea și documentele soft law vor face obiectul aplicării și interpretării de către instanțe (naționale sau europene) și de autorități publice.

*Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului*⁸.

Directiva are termen de transpunere 6 mai 2018, dar în România nu a fost discutată până în prezent. Potrivit GDPR, „protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și libera circulație a acestor date, face obiectul unui act juridic specific al Uniunii.” (considerentul (19)) Regulamentul nu se aplică activităților de prelucrare în aceste scopuri, prelucrarea fiind reglementată printr-un „act juridic mai specific al Uniunii”, și anume Directiva (UE) 2016/680. Statele membre au rol important în delimitarea competențelor precum și a definirii anumitor direcții de aplicare între Regulamentul 679 și Directiva 680.

Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele

⁷ Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată.

⁸ JO L 119, 4.5.2016, p. 89–131.

*pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave*⁹.

Potrivit art. 13 din Directivă, aceasta nu aduce atingere aplicabilității Regulamentului „în ceea ce privește prelucrarea datelor cu caracter personal de către transportatorii aerieni, în special obligația acestora de a lua măsuri tehnice și organizatorice adecvate pentru a proteja securitatea și confidențialitatea datelor cu caracter personal”.

*Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice)*¹⁰.

Raportul acestei directive cu Regulamentul este subliniat în considerentul (173) în care se reamintește că este necesar ca aceste acte normative să fie puse în concordanță. Se pare că este o întârziere în adoptarea Regulamentului care să înlocuiască Directiva 2002/58.

Directiva 2000/31/CE privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic).

Regulamentul „nu aduce atingere aplicării Directivei 2000/31/CE, în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15”. De altfel, Directiva 2000/31 stipula că nu se aplică în „chestiunile referitoare la serviciile societății informaționale reglementate de Directivele 95/46/CE și 97/66/CE”.

*Regulamentul nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date.*¹¹

Potrivit art. 1 alin. 3 „pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, se aplică Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 și alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile și normele din prezentul regulament în conformitate cu articolul 98.”¹²

⁹ JO L 119, 4.5.2016, p. 132–149.

¹⁰ Ediție specială în limba română, cap. 13, vol. 036, p. 63-73. Este în procedură de abrogare și înlocuire cu un regulament. Detalii: http://eur-lex.europa.eu/procedure/EN/2017_3

¹¹ Ediție specială în limba română: Capitolul 13 Vol. 030, p. 142 – 164.

¹² Art. 98 are ca denumire marginală ” *Revizuirea altor acte juridice ale Uniunii în materie de protecție a datelor*”. Potrivit acestui articol, ”dacă este cazul, Comisia prezintă propuneri legislative în vederea modificării altor acte juridice ale Uniunii privind protecția datelor cu caracter personal, în vederea asigurării unei protecții uniforme și consecvente a persoanelor fizice în ceea ce privește prelucrarea. Acest lucru privește în special normele referitoare la

III. Forța juridică a actelor și documentelor aplicabile în materia protecției datelor personale

Este semnificativ să discutăm forța juridică a diferitelor instrumente aplicabile în materia protecției datelor. Dacă despre regulamentul și directivă¹³ lucrurile sunt (relativ) clare, avizele și documentele de lucru ale Grupului de Lucru art. 29¹⁴ vor ocupa un loc central în analiză.

Temeiul esențial este art. 16 TFUE, urmat de art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene (CDFUE).¹⁵

Forța juridică a opiniilor/ ghidurilor adoptate de Grupul de lucru art. 29 este aceea de recomandare. Însă, dacă observăm cauza *Grimaldi*,¹⁶ documentele cu caracter de recomandare se impun instanțelor naționale. Recent a fost observat faptul că, deși nu a fost citat, unul din documentele Grupului de lucru „Art. 29” a fost utilizat în cauza *Nowak*¹⁷.

Preambulul Regulamentului este esențial pentru interpretarea și aplicarea acestuia. Preambulul aduce, în unele situații, importante precizări, pe care Curtea de Justiție, le va utiliza la momentul potrivit.

Va fi foarte important de stabilit raportul dintre regulamentul și legislația specială, atunci când există un conflict normativ privind protecția datelor.¹⁸

protecția persoanelor fizice în ceea ce privește prelucrarea de către instituțiile, organismele, oficiile și agențiile Uniunii, precum și normele referitoare la libera circulație a acestor date.”

¹³ **Irina Alexe, Constantin Mihai Banu**, *De la directivă la regulament în reglementarea, la nivelul Uniunii Europene, a protecției datelor cu caracter personal*, în vol. **Irina Alexe, Nicolae-Dragoș Ploșteanu, Daniel-Mihail Șandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 14 și urm.

¹⁴ Pentru o analiză a atribuțiilor Grupului de lucru „Art.29” dar și a Comitetului European pentru Protecția Datelor, care îl va înlocui, a se vedea **Irina Alexe**, *Reforma instituțională, în materia protecției datelor, la nivel european*, în vol. **Andrei Săvescu**, *Regulamentul general privind protecția datelor. Comentarii și explicații*, Editura Hamangiu, 2018 (în curs de publicare).

¹⁵ Pentru o evidențiere a rolului Curții de Justiție în interpretarea articolelor din tratat și CDFUE, a se vedea, **Adriana Maria Șandru**, *Privire critică asupra jurisprudenței Curții de Justiție a UE referitor la interpretarea art. 8 privind protecția datelor cu caracter personal din Carta drepturilor fundamentale a Uniunii Europene (CDFUE)*, *Pandectele române*, nr. 1/2018 (în curs de publicare).

¹⁶ Cauza 322/88, *Grimaldi / Fonds des maladies professionnelles*, hotărârea din 13 decembrie 1989, ECR 1989 p. 4407, ECLI:EU:C:1989:646.

¹⁷ C-434/16, *Nowak*, hotărârea din 20 decembrie 2017, ECLI:EU:C:2017:994.

¹⁸ Alte obligații, care au natură juridică diferită de GDPR pot fi analizate separat, sau în contextul afectării datelor personale, dacă prin comportamentul reglementat se ajunge la încălcarea protecției datelor. De ex. obligația de confidențialitate este reglementată de art. 653 din Legea nr. 95/2006, potrivit căruia personalul medical răspunde civil și pentru toate prejudiciile ce decurg din nesocotirea obligației de confidențialitate. A se vedea și **Bianca Luntraru**, *Protecția datelor pacienților în sistemul medical*, în vol. **Irina Alexe, Nicolae-**

IV. Starea de fapt în privința protecției datelor cu caracter personal.

Starea de fapt, reflectată în multe articole științifice, dar și în practica din România și alte state, este incertitudinea. Sunt prea multe dispoziții vechi care, coroborate cu puținele noutăți, dau o astfel de rezultantă. Este subliniată în primul rând necesitatea pregătirii, nu doar a operatorului și a desemnării unui responsabil pentru protecția datelor dar și a salariaților care operează în mod direct cu datele personale, iar în domeniul medical aproape a tuturor salariaților.¹⁹

Sunt multe cercetări sociologice din care rezultă că organizațiile nu sunt pregătite. Oricare ar fi sursa cercetării, de mai mică sau de mai mare amploare, concluziile sunt aceleași: gradul de pregătire a angajaților este scăzut, pregătirea organizațiilor pentru desemnarea unui responsabil cu protecția datelor este abia la început și nu se cunosc dispozițiile esențiale ale Regulamentului 679/2016.

Astfel, într-o cercetare la nivel mondial,²⁰ care a avut în vedere răspunsurile a 745 de respondenți, reies câteva cifre:

- 78% consideră conformarea la normele de protecție și de confidențialitate a datelor personale un motiv tot mai puternic de îngrijorare;
- 60 % dintre respondenții cu societăți în Uniunea Europeană au un plan de respectare a normelor GDPR;
- la nivel mondial, 33% dintre respondenți au în derulare un plan de aliniere la GDPR.

Un sondaj²¹ arată că 78% din angajații din domeniul medical nu au cunoștințe despre securitate cibernetică sau protecția datelor.

În Irlanda mai puțin de 2 din 5 participanți la un sondaj sunt siguri că sunt pregătiți pentru GDPR. În timp ce majoritatea participanților consideră că principala problemă în aplicarea Regulamentului sunt proprii salariați, doar 18% au urmat programe de pregătire.²²

Dragoș Ploșteanu, Daniel-Mihail Șandru (coordonatori), *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 247.

¹⁹ A se vedea: **Bernadette John**, *Are you ready for General Data Protection Regulation?*, BMJ, 2018, p. 360; Articolul evidențiază rolul GDPR în domeniul medical.

²⁰ *EY - Global Forensic Data Analytics Survey 2018*, disponibil la adresa <http://www.ey.com/gl/en/services/assurance/ey-global-forensic-data-analytics-survey-2018>, p. 25-27. Sondajul s-a desfășurat în perioada octombrie-noiembrie 2017.

²¹ MediaPro a realizat sondajul "2017 State of Privacy and Security Awareness Report" <https://healthitsecurity.com/news/78-of-healthcare-workers-lack-data-privacy-security-preparedness>. Interviu a fost realizat în SUA cu peste 1000 de respondenți.

²² Sondajul a fost realizat de Irish Computer Society și National Data Protection și este disponibil la adresa <http://www.techcentral.ie/less-2-5-sure-prepared-gdpr/>

Potrivit unui alt studiu, care indică într-o oarecare măsură și direcțiile de dezvoltare a domeniului protecției datelor, se arată că 79% dintre cetățenii europeni nu sunt la curent cu intrarea în vigoare a GDPR. Cu toate acestea, 82% dintre aceștia spun că vor încerca să-și protejeze drepturile, să aplice GDPR, ori să solicite ștergerea datelor.²³

V. Drepturile și obligațiile operatorilor

Etapele pentru conformarea la cerințele GDPR.

Dacă modificările GDPR nu sunt multe față de dispozițiile directivei, totuși acestea sunt foarte importate. De la amenzi, la probarea îndeplinirii principiilor, trecând prin numirea unui responsabil cu protecția datelor și resurse pentru satisfacerea drepturilor persoanelor vizate (portabilitate, ștergerea datelor, dreptul la acces). În consecință conformarea cu noile reguli de protecția datelor este esențială atât pentru evitarea unor sancțiuni, dar, în unele situații, și pentru mai buna funcționare a organizației.

Prima etapă este a stabilirii dacă organizația prelucrează **date cu caracter personal**²⁴ la un nivel la care să atragă obligativitatea desemnării unui responsabil cu protecția datelor. Dacă desemnarea DPO este obligatorie, următoarele etape ar trebui parcurse împreună cu acesta. Dacă desemnarea DPO nu este obligatorie potrivit reglementărilor, însă organizația are dubii cu privire la desemnarea acestuia, este mai bine să fie desemnat unul.²⁵

Stabilirea tipurilor de conținut de date cu caracter personal. Nu trebuie evitată nicio sursă de date dintre cele pe care organizația le deține. Trebuie stabilite locurile fizice în care sunt depozitate datele cu caracter personal sau sursele electronice. În acest din urmă caz trebuie stabilite atât sursele cu date personale cât și persoanele care au acces la aceste date. Va fi realizată o listă, pe departamente, cu persoanele care vor avea acces la anumite fluxuri de informații. Angajații care operează cu datele cu caracter personal trebuie instruiți în mod special, atât în privința operațiunilor curente cât și în privința limitelor competențelor acestora. Trebuie observat

²³ EU Consumers Poised to Take Back Control of Personal Data from Businesses, According to Pega Survey on GDPR, <https://www.pega.com/about/news/press-releases/eu-consumers-poised-to-take-back-control-of-personal-data-from-businesses-according>

²⁴ ”Date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale (art. 1 lit. a).

²⁵ **Irina Alexe**, *Principalele noutăți privind responsabilul cu protecția datelor, incluse în GDPR*, Pandectele române, nr. 1/2018 (în curs de publicare).

unde sunt ținute atât datele fizice (pe hârtie) cât și datele informatice, atât în cloud (dacă accesul este gratuit riscurile sunt aproape toate în sarcina operatorului) sau pe servere, cât și stocate în calculatoarele organizației. În cazul în care există un contract pentru cloud/ servere, acesta trebuie să se refere expres la securitate și riscuri legate de protecția datelor. Operatorul ar trebui să cunoască datele fizice cu privire la servere pentru a nu avea probleme referitoare la prelucrarea datelor sau transferul datelor în afara UE.

Verificarea surselor datelor cu caracter personal deținute/obținute de organizație înainte de intrarea în vigoare a Regulamentului. Dacă până la intrarea în vigoare a regulamentului nu există posibilitatea stabilirii surselor deținerii datelor cu caracter personal, se va verifica dacă aceste date sunt prelucrate în condiții de legalitate (art. 6) precum și dacă sunt respectate celelalte principii GDPR (art. 5).

Sunt cel puțin două categorii de date: ale propriilor angajați și ale terților (clienți). În privința salariaților, regulamentul are reglementări proprii mergând până la declararea ca dată sensibilă apartenența la un sindicat, problemă pe care angajatorul va trebui să o rezolve, conform art. 9. În cadrul relației angajator angajat trebuie observate și alte date sensibile, cum ar fi cele medicale, de orice natură; de exemplu, cele care privesc motivele absențelor pentru recuperarea medicală. Transmiterea diagnosticului către angajator este în afara protecției datelor personale,²⁶ cu excepțiile rezultate din interpretarea art. 9 alin. 2 lit. h. Datele cu caracter personal ale clienților sunt foarte importante mai ales dacă acestea sunt utilizate în vederea obținerii de beneficii de către organizația care le deține. Toate modalitățile de prelucrare a datelor cu caracter personal trebuie să fie atent realizate. În toate situațiile, înainte de utilizarea unui soft, aceste modalități trebuie evaluate printr-o procedură care să evalueze riscurile,²⁷ precum și fluxul de date.

Desemnarea DPO se realizează conform prevederilor legale pentru personalul angajat, în cadrul raporturilor de muncă, sau în afara raporturilor de muncă, prin încheierea unui contract de servicii prevăzut de art. 37 alin. 6.²⁸ De asemenea, este necesar ca, indiferent de modalitatea de desemnare a

²⁶ A se vedea: HM Revenue & Customs, *Guidance Statutory Sick Pay: employee fitness to work*, disponibil la adresa <https://www.gov.uk/guidance/statutory-sick-pay-employee-fitness-to-work>. Bolile și GDPR sunt elemente surpriză pentru economiștii care calculează „Full-time equivalent (FTE)” sau „whole time equivalent (WTE)”.

²⁷ De exemplu, cunoscutul snapchat a fost identificat ca nefiind sigur pentru pacienți. **Sohini Patel, Susan Bewley, Nathan Hodson**, *Snapchat is not for sharing*, *BMJ* 2016; 352.

²⁸ **Irina Alexe**, *Responsabilul cu protecția datelor (DPO) - funcționar public sau personal contractual?*, *RRDM*, nr. 2/2018 (în curs de publicare).

unui responsabil cu protecția datelor (în cadrul sau în afara raporturilor de muncă – funcționar public, personal contractual sau parte a unui contract de servicii, cu normă întreagă sau *part-time*, prevăzându-i un post distinct în cadrul organizației, sau prin cumul de funcții, ori desemnându-l ca șef al unei structuri specializate, sau ca reprezentant unic al unui grup de societăți, ori ca reprezentant unic al mai multor autorități sau organisme publice), acestuia să îi fie asigurate toate resursele, precum și garanțiile necesare, prevăzute de Regulament, pentru a-și îndeplini sarcinile.

Certificarea DPO. Certificarea cea mai sigură provine din încredere și cunoștințele DPO dar deocamdată, în România, certificarea DPO este la început. Primul pas a fost făcut în luna noiembrie 2017 când ocupația de responsabil pentru protecția datelor a fost inclusă în Clasificarea Ocupațiilor din România (COR) însă până la certificare calea este lungă și se așteaptă cu nerăbdare parcurgerea acesteia.

Raporturile cu **împuternicitul** sunt raporturi contractuale, care nu-l exonerează total de răspundere pe operator. Împuternicitul trebuie să ofere garanții suficiente, în sensul regulamentului, iar contractul dintre operator și persoana împuternicită trebuie să conțină cel puțin cerințele prevăzute de regulament, ce vizează elementele esențiale ale contractului, drepturile și obligațiile părților, confidențialitatea sau interzicerea delegării activității delegate, fără acordul prealabil al operatorului.

Modificarea structurii organizaționale. Ulterior desemnării unui DPO, organizația trebuie să-și modifice actele interne: regulament de organizare și funcționare, regulament de organizare internă, organigramă, contract colectiv de muncă. DPO trebuie „amplasat” în relație apropiată cu conducerea organizației, într-o organizare autonomă.²⁹ În unele situații trebuie concepută și relația cu alte entități de profil, cum este situația în domeniul medical.³⁰

Relația cu autoritatea de protecția datelor, mai precis, în România relația cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal este foarte importantă și trebuie să aibă în vedere:

- comunicarea datelor de contact ale responsabilului cu protecția datelor;

²⁹ Cu privire la raportul dintre responsabilul cu protecția datelor (DPO) și personalul tehnic (așa numitul departament IT): **Laurence Eastham**, *Data Protection: ICO Charges under the GDPR*, 30.10.2017, <https://www.scl.org/blog/10043-data-protection-ico-charges-under-the-gdpr>

³⁰ **Louise H. K. Blume, Nico J. H. W. van Weert, Jamiu O. Busari, Annemiek M. V. Stoopendaal, Diana M. J. Delnoij**, *What hospitals need to know about guidelines—A mixed-method analysis of guideline implementation in Dutch hospitals*, *Journal of Evaluation in Clinical Practice*, vol. 23, 6/2017, p. 1266–1273.

- notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal.

În raport cu autoritatea, operatorul are dreptul a de fi consiliat. Deși considerentul (129) din Preambul se referă la persoane vizate, acesta nu exclude și o relație coerentă cu operatorii și împuterniciții ("competențe de autorizare și de consiliere, în special în cazul plângerilor depuse de persoane fizice"). În cadrul art. 36 „autoritatea de supraveghere oferă consiliere în scris operatorului”, în anumite condiții și în anumite termene. În special alin. 3 din art. 58 enumeră tipurile de competențe în materia consilierii.

Fără a intra în detalii privind sancțiunile, trebuie remarcat faptul că, pe de o parte, Regulamentul³¹ stabilește condiții generale pentru impunerea amenzilor administrative, iar pe de altă parte, realizează o tipologie a sancțiunilor. Rolul autorităților naționale va fi foarte important în aplicarea Regulamentului. Și, desigur, al Curții de Justiție, în eventuale cereri privind pronunțarea unor decizii preliminare.³²

Verificarea conformării cu GDPR din punctul de vedere al prelucrării datelor. Acest lucru privește îndeosebi consimțământul în situațiile art. 6 lit. a dar și în celelalte situații în care prelucrarea s-a realizat fără acordul persoanei vizate. Conformarea se referă la numirea DPO, realizarea procedurilor și a fluxurilor de date; fiecare element al regulamentului trebuie respectat.

Programele informatice de conformare. Dincolo de toate aceste reglementări, mai mult sau mai puțin detaliate, trebuie să avem în vedere că nu există rețete de verificare și aplicare universale. Bineînțeles, indicatori și chestionare privind gradul de conformare, disponibile în număr foarte mare pe internet, ar putea fi utile. Însă toate acestea au o limitare serioasă care provine din specificul fiecărei organizații. Niciun produs software nu este pe deplin util dacă nu a fost pregătit pentru o anumită entitate, după ce au fost stabilite fluxurile de informații și procedurile proprii. Și, în toată ecuația, cu toate softurile achiziționate, cea mai importată resursă sunt oamenii pregătiți pentru prelucrarea legală a datelor cu caracter personal.

³¹ **Irina Alexe**, *Regimul sancționator prevăzut de Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal*, Curierul Judiciar, nr. 1/2018, p. 36.

³² Pentru trimiterile preliminare din România, a se vedea: **Daniel-Mihail Șandru**, *Importanța trimiterilor preliminare în materia protecției datelor cu caracter personal. Cauze semnificative și experiențe românești*, Revista Română de Drept al Afacerilor, nr. 4/2017, p. 157-167.

VI. Drepturile și obligațiile persoanelor vizate

Drepturile persoanelor vizate nu sunt absolute.³³ Acest drept la protecția datelor intră în conflict cu alte drepturi, uneori dreptul la protecția datelor fiind mai puțin preferat între valorile sociale protejate în legislație. Explicațiile derivă din faptul că, mai ales în actuala stare a tehnicii și mai ales a dezvoltării internetului, o insularizare a ființei umane este (aproape) imposibilă, sau cu efecte foarte complicate. Internetul a introdus celeritate și comoditate dar a adus și riscurile care sunt presupuse de accesul la această rețea informațională. Cu atât mai mult în constituirea comunităților virtuale, unde persoanele vizate renunță de bunăvoie la propria protecție a vieții private.³⁴

Începând cu 25 mai persoanele vizate vor solicita aplicarea GDPR. Poate nu va fi o presiune din partea autorităților publice, a Comisiei Europene sau a autorităților naționale, cât fi din partea persoanelor vizate.

Regulamentul prevede în considerentul 59 exercitarea de către persona vizată a dreptului la acces, a dreptului la rectificarea și ștergerea datelor precum și exercitarea dreptului la opoziție.³⁵

O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia (considerentul (63)). Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale (considerentul (64)).

³³ Considerentul (4) din Regulament. A se vedea și analiza recentă din articolul **Lothar Determann**, *No One Owns Data*, UC Hastings Research Paper No. 265 (February 14, 2018), disponibil la <https://ssrn.com/abstract=3123957>

³⁴ Pe larg, **Daniel Mihail Șandru**, *Imposibila coexistență între protecția datelor și comunitățile virtuale? Ce urmează?*, Pandectele române, nr.1/2018 (în curs de publicare). Referindu-se la controlul asupra informației, Pedro Cruz Villalón, afirmă că acesta este uneori irealizabil: "din momentul în care un conținut informațional este postat pe internet, particularii se transformă imediat, voluntar sau involuntar, în distribuitori de informații prin rețele de socializare, prin comunicare electronică, prin linkuri, prin bloguri sau prin orice alte mijloace oferite de internet." (par. 47 din Concluziile Avocatului General Pedro Cruz Villalón prezentate la 29 martie 2011 în cauzele conexe C-509/09 și C-161/10).

³⁵ "Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivelor cereri, să motiveze acest refuz." (consid. 59)

Dreptul de a fi informat cu privire la încălcarea securității datelor (art. 34) este oarecum limitat pentru că regulamentul consideră că se poate face și o informare publică atunci când costurile nu ar fi rezonabile.

Dreptul la ștergere trebuie realizat în limitele regulamentului și trebuie verificată distincția dintre consimțământul acordat pentru încheierea contractului și consimțământul privind prelucrarea datelor personale. Dreptul la ștergere nu ar trebui să fie exercitat abuziv; ștergerea (distrugerea) datelor se face cu responsabilitatea operatorului.³⁶

”**Dreptul la portabilitatea datelor** are două componente: dreptul persoanei vizate de a primi ea însăși datele (art. 20 alineatul 1 RGPD) și dreptul de a solicita ca datele să fie transferate direct unui alt operator (art. 20 alineatul 2 RGPD).”³⁷

VII. Interpretarea și aplicarea Regulamentului 2016/697 de către instanțele române

Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Într-o cauză soluționată definitiv,³⁸ instanța face referire la art. 8 alin. 1 și 2 CDFUE, art. 17 alin. 1 din Regulament³⁹, după care se subliniază că „dispozițiile art. 17 din regulamentul reglementează „*dreptul de a fi uitat*”, drept ce constă în dreptul persoanelor de a cere eliminarea completă a datelor lor atunci când acestea nu mai sunt folositoare pentru scopurile în care au fost colectate ori chiar postate de bunăvoie, precum și atunci când utilizatorul retrage consimțământul publicării lor.” În continuare se face referire la reglementarea națională (“Totodată, conform art. 14 alin. 1 lit. a) din Legea 677/2001”). Urmează și motivarea instanței:

„Punând în balanță dreptul la viața privată și la protecția datelor reclamantului și dreptul la libertatea de exprimare, în speță, libertatea presei,

³⁶ Google, probabil cea mai mare organizație care prelucrează date cu caracter personal a raportat că a de-listat aproape două milioane și jumătate de link-uri: **Nicolas Vega**, *Google gets 2.4M requests from Europeans to be ‘forgotten’*, New York Post, 28.02.2018, By <https://nypost.com/2018/02/27/google-gets-2-4m-requests-from-europeans-to-be-forgotten/>. Desigur este o problemă de balanță a valorilor: libertatea de exprimare vs. dreptul la viața privată, problemă greu de rezolvat.

³⁷ **Andreea Lisievici**, Dreptul la portabilitatea datelor potrivit Regulamentului General privind Protecția Datelor, în vol. **Irina Alexe, Nicolae-Dragoș Ploșteanu, Daniel-Mihail Șandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 146.

³⁸ Judecătoria Sectorului 3 București, Sentința civilă nr. 3731/27.03.2017, nepublicată, disponibilă la adresa <http://rolii.ro/hotarari/590b19dde490098c890000ec>

³⁹ Forma în care instanța (nota citată supra) face referire este foarte importantă întrucât aplică regulamentul: ” De asemenea, art. 17 alin. 1 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016, prevede că (...)”.

instanța consideră că primează primul drept la care s-a făcut referire. Astfel, având în vedere că articolul publicat la data de 27.09.2006, în care se face referire la numele reclamantului, nu mai este de actualitate și nici nu prezintă informații care să fi fost de interes național și care să fi prezentat o problemă îndelung mediatizată la acea dată, instanța consideră că nu se mai impune menținerea acestuia pe pagina de internet a publicației „România Liberă”. Menținerea în continuare a articolului în spațiul on-line ar reprezenta o ingerință în dreptul reclamantului la protecția datelor ce nu mai este proporțională cu scopul urmărit.

Mai mult, instanța va avea în vedere și faptul că pârâta a achiesat pretențiilor reclamantului, recunoscând că respectivul articol prezintă informații care, cu trecerea timpului (peste 10 ani) au dobândit caracter nesemnificativ.”

Hotărârea aceasta, pronunțată după intrarea în vigoare a Regulamentului, dar înainte de punerea în aplicare, soluționează mai degrabă echitabil cererea decât să aibă în vedere aplicarea dispozițiilor legale.

Exceptarea persoanelor juridice de la aplicarea Regulamentului.

O altă cauză, care a opus Registrul Comerțului și Autoritatea de protecție a datelor, a avut ca obiect anularea unui act administrativ (contestarea unei sancțiuni). Registrul Comerțului s-a apărat invocând că a aplicat reglementari europene,⁴⁰ și în plus

„Consimțământul persoanei vizate nu era necesar conform art. 5 alin. 2 lit. c și f din Legea nr. 677/2001. Judecătorul delegat este cel care stabilește documentele care trebuie depuse pentru înregistrarea unei societăți, astfel încât susținerea intimatei cum că ar fi fost eliberate copii după înregistrări care nu erau obligatorii a fi depuse în vederea efectuării înregistrărilor referitoare la modificarea sediului societății este neîntemeiată, întrucât ONRC nu are această atribuție. Publicitatea realizată prin registrul comerțului are la bază Directiva 2009/101/CE și trebuie să permită terților să cunoască datele esențiale ale societăților comerciale și alte informații privind societatea. Considerentul 14 din Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal prevede că acest regulament nu se aplică prelucrării datelor cu caracter personal care

⁴⁰ Tribunalul București, Secția a II a – Contencios Administrativ și Fiscal, Sentința civilă nr. 24 din 08.01.2018, nepublicată, disponibilă la adresa <http://rolii.ro/hotarari/5a7286f6e490095421000b3a>; a se vedea și Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 132/24.10.2017, disponibilă la adresa <http://rolii.ro/hotarari/5a3099f6e49009580b000038>

privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice."⁴¹

Autoritatea a arătat că: „Regulamentul UE 2016/679 al Parlamentului European și al Consiliului privind protecția datelor persoanelor fizice se aplică de la data de 25.05.2018, în prezent fiind aplicabilă Directiva 95/46/CE, transpusă în legislația internă prin Legea nr. 677/2001.” Astfel, Autoritatea a constatat că s-au „dezvăluit în mod excesiv mai multe date cu caracter personal ale [persoanei vizate] cuprinse în înscrisurile depuse la Registrul Comerțului decât cele prevăzute de lege în situația eliberării copiilor, încălcând chiar propria Procedură Operațională privind eliberarea de înscrisuri nr. 1485/14.04.2016. Instanța, după ce a analizat cererea inclusiv din perspectiva Legii nr. 544/2001 privind cererile de liber acces la informații de interes public și a Legii nr. 26/1990, în special a art. 4 și 51¹, a constatat încălcarea legii (respectiv a respins cererea de anulare a actului administrativ).

Într-o altă cauză, una din părți (reclamantul) a solicitat aplicarea directă a directivei privind protecția datelor, formularea unei trimiteri preliminare⁴² și a ridicat o excepție de neconstituționalitate. În privința regulamentului, partea din acțiunea dedusă judecății se referă la acesta ca fiind „incident doar pentru comparație”.⁴³ Astfel, se afirmă că „analizând

⁴¹ Astfel, „au fost invocate dispozițiile Legii nr. 26/1990 privind registrul comerțului republicată, normele metodologice privind registrul comerțului, Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, Directiva 95/46/CE, Avizul nr. 4/2007 privind conceptul de date personale, Directiva 2009/101/CE, Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, H.G. nr. 902/2012.”

⁴² Solicitarea de formulare a unei trimiteri preliminare a fost realizată și în alt dosar instanța consideră că „se reține că reclamantul nu a solicitat adresarea unei anumite întrebări punctuale Curții [de Justiție a Uniunii Europene], ci doar a invitat instanța să formuleze o cerere "dacă consideră că nu are suficiente informații relevante din jurisprudența CJUE", astfel încât nu se poate reține formularea unei cereri asupra căreia instanța ar trebui să se pronunțe în mod expres.” A se vedea: Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 4754/06.13.2017, disponibilă la adresa <http://rolii.ro/hotarari/5a879e99e49009a84d00003e>

⁴³ Curtea de Apel Timișoara, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 47/2 februarie 2017, disponibilă la adresa <http://rolii.ro/hotarari/58b6a431e49009ac0700002a>. De asemenea, Curtea de Apel Timișoara, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 58/14 februarie 2017, disponibilă la adresa <http://rolii.ro/hotarari/58c24effe49009d41e000038>; Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 211/30.01.2017, disponibilă la adresa <http://rolii.ro/hotarari/58c24ef9e49009d8200000c3> (în această cauză, pârâta a indicat lipsa incidenței Regulamentului până în 25 mai 2018).

prin analogie și Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 care înlocuiește Directiva 95/46/CE începând cu data de 25 mai 2018, rezultă cu certitudine faptul că ANSPDCP, nu este investită prin Directiva 95/46/CE și cu aplicarea sancțiunilor contravenționale.” Desigur, o asemenea afirmație nu poate fi primită în totalitate, fără a indica totuși câteva nuanțe, care rezultă chiar din natura juridică a actului legislativ al Uniunii (directivă). Într-adevăr, nu ANSPDCP din România este investită de directivă, și nici nu ar fi putut să fie, întrucât aceasta prevede, în textul art.28, principalele atribuții, minimale, pentru autoritățile de supraveghere din fiecare stat membru, urmând ca fiecare stat membru să aplice prevederile respective. Este cunoscut faptul că directiva lasă la latitudinea statelor membre modalitatea efectivă de transpunere. Faptul că prin legea națională de transpunere a prevederilor directivei ANSPDCP a fost desemnată ca autoritate competentă să aplice și sancțiunile contravenționale este nu numai în spiritul, ci chiar se face aplicarea concretă a dispozițiilor directivei în dreptul intern.

Într-o altă cauză una din părți, invocând regulamentul (incident pentru comparație), ajunge la concluzia că „*incidența Directivei 95/46/CE este statuată și prin considerentele (9), (10) și (20) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 care înlocuiește Directiva 95/46/CE începând cu data de 25 mai 2018*”, pe care desigur, instanța nu a analizat-o.⁴⁴ În alte situații, acțiunea a fost întemeiată atât pe directivă cât și pe regulament (fără să se mai indice faptul că este „incident pentru comparație”).⁴⁵

Majoritatea hotărârilor disponibile pe rolul.ro, analizate în prezentul material, conțin doar invocări, de către părți, a Regulamentului 2016/679. Am analizat 32 de cauze, cu hotărâri pronunțate în perioada anilor 2016-

⁴⁴ Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 1038/23.03.2017, disponibilă la adresa <http://rolul.ro/hotarari/5914c3cee490099093000185>

⁴⁵ Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 2330/14.06.2017, disponibilă la adresa <http://rolul.ro/hotarari/5950debde49009b01100004e>; Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 3896/24.10.2017, disponibilă la adresa <http://rolul.ro/hotarari/5a0d00b7e49009d80e0000a1>; Curtea de Apel București, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 2443/20.06.2017, disponibilă la adresa <http://rolul.ro/hotarari/5a348e94e49009781100002e>. Curtea de Apel Timișoara, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 53/14.02.2017, disponibilă la adresa <http://rolul.ro/hotarari/58b6a432e49009ac0700009a> Curtea de Apel Timișoara, Secția de Contencios Administrativ și Fiscal, Sentința civilă nr. 15/2018, disponibilă la adresa <http://rolul.ro/hotarari/5a6fdb1de49009c41500002e>. În aceste exemple se menționează că regulamentul ”*înlocuiește Directiva 95/46/CE începând cu data de 25 mai 2018*”. Instanța nu a luat în considerare în vreun fel trimiterea la regulament.

2018. Din punctul de vedere al obiectului cauzei, cu două excepții,⁴⁶ în majoritatea cauzelor este implicată Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, fiind considerate cauze de contencios administrativ. Din punctul de vedere al instanțelor, majoritatea sunt din București, în primul rând Curtea de Apel București (24), apoi Judecătoria Sectorului 3, Tribunalul București, iar din țară, Curtea de Apel Timișoara (5 cauze) și Curtea de Apel Ploiești (1). Cu o singură excepție (în care de fapt, nu se poate preciza dacă Regulamentul este parte a motivării în drept a hotărârii, sau dacă mai degrabă este amintit de instanță cu argument de autoritate), instanțele nu au făcut trimitere la regulamentul și nu au „răspuns” părților care și-au întemeiat acțiunile (și) pe dispozițiile Regulamentului 2016/679. În nicio cauză nu este invocat doar Regulamentul ca temei al acțiunii, ci întotdeauna după Directiva 95/46. Se poate afirma că suntem în fața unei analize privind comportamentul justițiabililor din România înainte de intrarea în vigoare a Regulamentului.

Concluzii

Principalul subiect în raport cu intrarea în vigoare a, respectiv cu aplicarea Regulamentului General privind Protecția Datelor, este pregătirea organizațiilor, iar constatările unanime sunt că această importantă modificare legislativă găsește cele mai multe entități nepregătite.

⁴⁶ Cele două excepții sunt: cauza referitoare la dreptul la ștergere (citată supra) și o cauză de dreptul muncii. În această cauză, Regulamentul este amintit din punctul de vedere al importanței pe care o are protecția datelor și sancțiunile la care se poate ajunge, fără să aibă o legătură propriu-zisă cu fondul litigiului: „Protecția datelor cu caracter personal ale angajaților reprezintă unul dintre angajamentele majore ale societății. Or, încălcarea regulilor de prelucrare a datelor prin dezvăluirea nelegală a datelor de care contestatorii s-au făcut responsabili a adus o gravă atingere vieții private a angajaților, drept fundamental stabilit de Constituție. De asemenea, conduita - continuată în timp - a contestatorilor a avut și are în continuare un impact negativ asupra societății, prin tensiunile și climatul de neîncredere față de capacitatea acesteia de a proteja datele cu caracter personal ale angajaților și, în cele din urmă, de a-și proteja angajații care au fost create. Nu în cele din urmă, gravitatea încălcării regulilor privind protecția datelor și implicit a faptelor de care se fac vinovați contestatorii și care a făcut necesară aplicarea sancțiunii concedierii rezultă și prin raportare la noua reglementare privind protecția datelor aplicabilă începând cu anul 2018. Importanța protejării datelor împotriva utilizărilor nelegale (de tipul celor de care contestatorii se fac vinovați) și justețea sancțiunii disciplinare aplicate de societate rezultă și din sancțiunile care au fost considerate necesare în această nouă reglementare pentru a asigura protecția datelor și a preveni încălcările cerințelor legale. Astfel, Regulamentul nr. 679/2016 prevede că prelucrările excesive ale datelor cu caracter personal (exact situația de care se fac vinovați contestatorii) sunt sancționabile cu amenzi de până la 20.000.000 de Euro sau de până la 4% din cifra de afaceri totală la nivel mondial, luându-se în calcul valoarea cea mai mare.” Curtea de Apel Ploiești, Secția I Civilă, Decizia nr. 1842/2016, disponibilă la adresa <http://rolii.ro/hotarari/5899fdb3e490095c2b00090a>

Persoanele vizate devin cu această ocazie mai conștiente de dreptul lor la viață privată și cu privire la datele cu caracter personal. Instanțele judecătorești deja s-au aflat în fața invocării Regulamentului, dar din 25 mai 2018 va începe aplicarea efectivă a acestuia.

Legislația privind protecția datelor este mult mai stufoasă, și nu se reduce doar la un regulament⁴⁷, iar coroborarea normelor europene cu normele naționale va fi un alt aspect important în aplicare.

⁴⁷ Anexăm prezentului studiu cele 21 de acte relevante, incluzând TFUE și CDFUE (în extras), precum și textul complet al GDPR, dar și al directivelor, deciziilor-cadru, orientărilor, ghidurilor sau avizelor emise de instituțiile competente ale Uniunii Europene, respectiv de Grupul de lucru „Articolul 29”, ce alcătuiesc, în opinia noastră, tabloul corect al legislației europene în materia protecției datelor.

Începând cu 25 mai 2018, data punerii sale în aplicare, Regulamentul 2016/679/UE 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 (GDPR), va aduce transformări semnificative în materia protecției datelor cu caracter personal. Regulamentul se aplică tuturor cetățenilor europeni indiferent de sediul operatorilor, iar protecția datelor pune în centru persoana vizată, reglementările având rolul nu doar de a o proteja în fața valului de descoperiri tehnico-științifice, dar și pentru a reglementa activitatea marilor organizații care prelucrează date cu caracter personal.

Regulamentul face parte dintr-un sistem general de reglementare a informațiilor care se referă atât la domenii speciale de prelucrare a datelor cu caracter personal (datele în materie polițienească sau datele privind pasagerii) dar și la comerțul electronic. Relațiile dintre aceste acte normative, precum și între acestea și documentele soft law vor face obiectul aplicării și interpretării de către instanțe (naționale sau europene) și de autorități publice.

Volumul conține un studiu în care sunt analizate experiențele din România, referitoare la punerea în aplicare a Regulamentului General privind Protecția Datelor 2016/679, căruii îi sunt atașate și cele 21 de acte relevante, incluzând TFUE și CDFUE (în extras), precum și textul complet al GDPR, dar și al directivelor, deciziilor-cadru, orientărilor, ghidurilor sau avizelor emise de instituțiile competente ale Uniunii Europene, respectiv de Grupul de lucru „Articolul 29”, ce alcătuiesc, în opinia noastră, tabloul corect al legislației europene în materia protecției datelor.

Daniel-Mihail Șandru
Irina Alexe

