

Învățământul universitar – provocări și perspective în protecția datelor

Higher education – Challenges and perspectives in data protection

Nicolae Ploeșteanu*

Timp de 3 zile, în perioada 8-10 iunie 2023, la Cluj-Napoca s-a desfășurat Conferința Națională cu tematica „*Protecția datelor cu caracter personal în învățământul universitar românesc – provocări și perspective*”, organizată de Universitatea Babeș-Bolyai. Mi-am propus în acest material să expun câteva gânduri despre conferință, precum și câteva idei pe care le-am prezentat într-una dintre zilele de activități.

Am ajuns la Universitatea din Cluj, unde am constatat că sala dedicată prezentării lucrărilor era complet plină de practicieni, dintre care majoritatea erau persoane care îndeplineau funcția de responsabil cu protecția datelor cu caracter personal în cadrul unei universități din România. Cu toate că am participat la peste o sută de conferințe pe subiecte legate de protecția datelor, recunosc că aceasta m-a impresionat datorită seriozității și pregătirii participanților. Intensitatea dezbaterilor se datorează în cea mai mare măsură acestora, dar inițiativa și organizarea extrem de bune se datorează exclusiv organizatorilor, cadre didactice ale Universității Babeș Bolyai din Cluj. Conferinței i s-a alocat și un domeniu web distinct: <https://dataprotection.conference.ubbcluj.ro/>

Există însă și o altă latură care întregește perspectiva asupra importanței subiectului: *intensitatea* prelucrărilor de date cu caracter personal realizate în cadrul unei universități. În acest fel, ne apropiem și de subiectul cu care m-am prezentat la conferință pentru a-l supune atenției și dezbaterii participanților: „*Unele consecințe ale rolului de «arhivar» de date personale al universităților, din perspectiva protecției acestora. Dreptul la viață privată vs. Libertatea de exprimare*”. Tematica fusese stabilită împreună cu unul dintre moderatorii evenimentului, profesorul Raul Felix Hodoș, de la Universitatea din Alba Iulia. Universitățile se află în mod inerent printre cele mai importante depozite de date cu caracter personal, din două motive principale: *depozitează dovezile oficiale* privind deținerea unor calificări în diferitele specialități pe

* Conf. univ. dr. Nicolae Ploeșteanu este directorul Centrului de studii pentru protecția datelor din cadrul UMFST G.E. Palade din Târgu Mureș.

care le organizează și, în plus, intervin într-o perioadă care creează *premisele evoluției profesionale* pentru o mare parte dintre studenți. Prima valență, reflectă dependența studenților față de universitate pe tot parcursul vieții, deoarece acolo este sursa oficială a dovezii nivelului de studii absolvit. Cea de-a doua valență, reflectă ideea că evoluția ulterioară profesională a oricărui dintre absolvenți sau, mai mult, a cadrelor didactice, ar putea să devină de interes public și să se particularizeze relația dintre absolvent, cadrul didactic și universitate, pe de o parte și societatea civilă, pe de altă parte. În prezentarea conferențiată am oferit repere de abordare a interesului public de a cunoaște date personale ale studenților, absolvenților, cadrelor didactice din cadrul universităților, prin raportare la legislația în materie de protecție a datelor și libertatea de exprimare.

În pofida unei semantici extrem de avangardiste pe care o prezintă noțiunea de „universitate” și pe care majoritatea dintre noi o legăm inerent de stâlpul educației acelei părți a populației care își dorește mai mult și care tinde spre o cunoaștere fără limite, aceste instituții (universitățile) concurează pe primele locuri în rândul celor mai mari depozitari de date cu caracter personal. La o „contabilitate” extrem de rece, s-ar putea să observăm că, în prezent, rolul universității de arhivar/depozitar al datelor cu caracter personal prezintă o importanță mai mare în societate decât rolul său elitist. Evident că acest lucru se datorează și unei scăderi generalizate a nivelului și interesului de cunoaștere personală directă, altfel decât prin apelul la soluția clasică: „caută un prieten”, adică AI (artificial intelligence) și laptop-ul/telefonul.

De asemenea, se datorează și faptului că mass-media are un interes mai mare de a promova știri scandaloase decât de a se îngriji cu cumpătare de sprijinul de imagine a unui student promițător, dar care pe moment nu le poate oferi mai nimic pentru a-și vinde știrea exponențial.

În termeni simpli, una dintre consecințele rolului de arhivar de date cu caracter personal al universităților este aceea că orice solicitări de informații, realizate de către terți, se vor îndrepta către aceste universități, unde se realizează prima stocare și constituire de baze de date care reflectă și au scopul de a evidenția studiile efectuate/neefectuate de către persoanele fizice vizate, studenți/foști studenți, respectiv cadre didactice. Din experiența practică proprie, am observat că sunt anumite tipologii de cereri formulate de cetățeni sau mass-media cu privire la studenți sau foști studenți, mai exact la studiile sau statutul acestora.

Temeiul juridic invocat este de regulă Legea nr. 544/2001 privind liberul acces la informații de interes public. *Numeroase cereri* sunt venite din partea mass-media pentru a se confirma unele specializări și perioade de studii efectuate de persoane care ocupă în prezent funcții publice, foști studenți ai universității, astfel că se dorește o anumită „verificare” a realității portofoliului acestor persoane.

Alte cereri sunt formulate pentru a se verifica conținutul unor lucrări de licență, masterat, dar mai ales doctorat, urmărindu-se fie persoane extrem de publice, absolvenți ai unor astfel de licențe, doctorate, fie unii posibili uzurpatori de proprietate intelectuală, fenomen care a prins în ultimul deceniu un avânt deosebit, odată ce printre cei „acuzati” se numără și un fost prim-ministru.

Trebuie să punctez existența și a altor cereri, puțin mai aparte, chiar dacă se încadrează, cel mai adesea, într-una dintre categoriile de mai sus; este vorba de cereri care privesc cadre didactice care ocupă și alte funcții în sistemul de stat, fiind o tradiție socială românească, împănarea diferiților avocați, judecători, procurori, demnitari sau funcționari publici cu o titlatură universitară, numai bună să conducă la o idolatrizare de familie. În spatele imaginii de lemn se găsesc atât interese financiare, cât și consecințe financiare și sociale: dubla recompensare, cu salarii de titulari și cu pensii publice, de

regulă. După anii 1990, vom observa că în sistemul universitar toți foștii miniștri și miniștri, demnitari de stat, parlamentari etc, pe scurt oameni de stat, care aveau și statut de cadru didactic, și-au luat pe perioada mandatului lor mai departe salariu întreg de titular de la universitățile unde erau angajați, deși, dacă ar fi îndeplinit atribuțiile și orarul specific unui asemenea post, nu ar fi avut fizic posibilitatea să își exercite și mandatul lor. De aceea, adesea informațiile solicitate de mass-media, prin întrebări adresate universităților, vizează aceste anomalii și încasări fantastice din slujbe adesea înmulțite doar pe hârtie și plătite extrem de bine, dar *in absentia*.

Dacă aceasta este situația din „teren”, iată și câteva repere juridice pentru a încorpora informațiile solicitate și răspunsurile într-un cadru juridic.

1. Cine poate solicita informații și ce fel de informații, care să se refere la informații de interes public?

Art. 1 al Legii nr. 544/2001 ne oferă răspunsul: „Accesul liber și neîngrădit al persoanei la orice informații de interes public, definite astfel prin prezenta lege, constituie unul dintre principiile fundamentale ale relațiilor dintre persoane și autoritățile publice, în conformitate cu Constituția României și cu documentele internaționale ratificate de Parlamentul României”. Din art. 1 reiese că obiectul unei solicitări în baza Legii nr. 544/2001 îl reprezintă doar informațiile de interes public.

2. Sunt datele personale, informații de interes public? Legea nu le califică, dar în legătură cu ele stabilește o excepție de la *accesul liber* la aceste informații; astfel, art. 12 prevede: „(1) Se exceptează de la accesul liber al cetățenilor, prevăzut la art. 1 și, respectiv, la art. 11¹, următoarele informații: (...) d) informațiile cu privire la datele personale, potrivit legii”;

3. Când informațiile privind date personale devin de interes public? Art. 13 al Legii nr. 544/2001 prevede că „Informațiile care favorizează sau ascund încălcarea legii de către o autoritate sau o instituție publică nu pot fi incluse în categoria informațiilor clasificate și constituie informații de interes public”, iar art. 14 stabilește că „(1) Informațiile cu privire la datele personale ale cetățeanului pot deveni informații de interes public numai în măsura în care afectează capacitatea de exercitare a unei funcții publice. (2) Informațiile publice de interes personal nu pot fi transferate între autoritățile publice decât în temeiul unei obligații legale ori cu acordul prealabil în scris al persoanei care are acces la acele informații potrivit art. 2”. Aceste prevederi, ridică la rândul lor unele problematici și întrebări, precum: alin. (1) va fi o excepție de strictă interpretare, excluzând orice altă posibilitate ca o informație să devină „informație publică de interes personal”? Este corectă această expresie: „informație publică de interes personal”? sau era mai corect să se spună „date personale de interes public”? La ce ipoteze se referă expresia „capacitatea de exercitare a unei funcții publice”?

4. Oare art. 11 nu ascunde o situație faptică care permite încălcarea confidențialității datelor personale, deoarece permite accesul concret la acele informații din partea unor terți: art. 11 – (1) Persoanele care efectuează studii și cercetări *în folos propriu sau în interes de serviciu* au acces la fondul documentaristic al autorității sau al instituției publice pe baza solicitării personale, în condițiile legii.

5. Care este întrepătrunderea dintre Legea nr. 544/2001 și RGPD?

Permite Regulamentul General privind Protecția Datelor o divulgare de date personale, chiar dacă aceasta nu este prevăzută distinct în categoria excepțiilor de la regula interzicerii accesului liber la informații, atunci când acestea privesc date cu caracter personal? Și dacă da, temeiul juridic al unei asemenea divulgări ar putea fi interesul legitim, în pofida faptului că RGPD spune că acest temei nu poate fi invocat de către instituțiile și autoritățile publice? În ceea ce mă privește pe mine, eu consider că răspunsul este afirmativ, iar universitățile nu trebuie puse în aceeași categorie a

instituțiilor publice sau autorităților publice din perspectiva puterii de a prelucra date personale pe diferite temeuri, precum interesul legitim. Într-adevăr, universitățile, dincolo de faptul că au această alocare de bani din bugetul public de stat, se comportă asemănător entităților private, iar Constituția noastră le conferă autonomie universitară, ceea ce înseamnă un statut extrem de liber în raporturile juridice pe care le întreprinde.

Fără a intra în amănunte, acestea fiind oferite în cadrul prezentării de la Cluj, îi felicit și îi încurajez pe organizatorii conferinței să facă o tradiție anuală din conferința organizată în premieră, în perioada 8-10 iunie 2023.

studii și cercetări

Protecția datelor personale în ecosistemul spațiului european al datelor privind sănătatea

Personal data protection in the European health data space ecosystem

Drd. Alexandru GEORGESCU*

Drd. Roxana GEORGESCU-TOMȘA**

□ Rezumat

Acest articol analizează protecția datelor cu caracter personal în ecosistemul spațiului European al datelor privind sănătatea. Lucrarea explorează cadrul legal de prelucrare a datelor personale în UE, subliniind principiile și reglementările cheie care guvernează prelucrarea datelor.

Lucrarea examinează diferitele preocupări juridice și de etică medicală care apar în prelucrarea datelor de sănătate, inclusiv aspecte legate de consimțământul informat al pacientului, transferul internațional al datelor și incidentele de securitate. Se subliniază importanța protecției datelor personale și necesitatea unui sistem robust și eficient pentru a proteja confidențialitatea și încrederea pacienților și în același timp pentru a îmbunătăți serviciile medicale.

Cuvinte-cheie: *spațiul european al datelor privind sănătatea, date personale, date medicale, securitatea datelor, incidente de securitate a datelor medicale, etică medicală, consimțământ*

□ Abstract

This paper discusses the protection of personal data in the European ecosystem of health data. The article explores the background of EU data protection framework highlighting the key principles and regulations that govern data protection in Europe. The article provides an overview of health data, detailing the different types of data that fall under this category and the potential risks involved in handling such information. The paper goes on to examine the various legal and ethical concerns

* Doctorand, Institutul de Cercetări Juridice „Acad. Andrei Rădulescu” al Academiei Române.

** Doctorand, Școala Doctorală a Universității de Medicină și Farmacie „Carol Davila” București (a contribuit prin prezentarea cu privire la datele folosite în cercetarea științifică a managementului fistulelor în patologia esofagiană).

that arise in the context of health data protection, including issues related to informed consent, international data transfers and data breaches.

The article highlights the importance of protecting personal data in the context of health data and the need for a robust and effective data protection framework to safeguard patient privacy and trust and at the same time improving medical services.

Keywords: *European health data space, personal data, medical data, data security, medical data breach, medical ethics, consent*

I. Crearea unui cadru juridic pentru un ecosistem al datelor personale privind sănătatea. Prevederile proiectului de Regulament pentru spațiul european al datelor privind sănătatea. Oportunități și provocări.

Constituirea unui ecosistem al datelor personale privind sănătatea pare să reprezinte o oportunitate uriașă atât pentru cercetătorii din domeniul sanitar, cât și pentru medicii sau personalul medical implicat direct în desfășurarea actului medical. Nu în ultimul rând beneficiarul direct ar trebui să fie cetățeanul în calitatea sa de pacient. Constituirea unui spațiu european al datelor privind sănătatea presupune utilizarea unei cantități foarte mari de date cu caracter personal astfel că funcționarea unui astfel de „ecosistem” presupune o mare provocare pentru că reprezintă un element de politică transnațională în domeniul sănătății. Cercetând asupra opiniilor conturate în legătură cu prelucrarea datelor cu caracter personal în scopul utilizării acestor date într-un spațiu european al datelor privind sănătatea am constatat că se conturează trei mari linii directoare: în primul rând este vorba despre interesul pentru drepturile pacientului pentru a căror respectare se invocă reguli foarte stricte de prelucrare a datelor pentru a oferi sau pentru a menține controlul asupra datelor cu caracter personal, iar la polul opus se situează opinia potrivit căreia este esențial să se acorde atenție asupra modalității utilizării raționale a datelor astfel încât să se păstreze caracterul lor nealterat (calitatea datelor). Pozițiile intermediare au în vedere chestiuni tehnice de obținere, utilizare și conservare a datelor.

S-a demonstrat că în perioada de manifestare a crizelor sanitare nu pot fi adoptate măsuri ample de reformare a politicilor și protoalelor ci mai degrabă se pune accentul pe adaptabilitate și pe decizii rapide în baza datelor avute la dispoziție. Este esențial așadar ca datele cu care se operează să fie calitative (nealterate) astfel încât scopul să poată fi atins.

Pandemia de coronavirus a pus în practică un astfel de exercițiu atât pentru actorii de pe piața serviciilor medicale, cât și pentru decidenții în domeniul politicilor de sănătate. Pentru aceste considerente, acest articol încearcă să răspundă la întrebarea: Poate reuși Uniunea Europeană (UE) să creeze un sistem funcțional al datelor privind sănătatea?

Opinăm că punctul de pornire trebuie să fie reprezentat de asigurarea cadrului juridic pentru acest sistem, ceea ce presupune să stabilim care sunt competențele Uniunii Europene în promovarea politicilor privind sănătatea. Art. 9 din Tratatul de funcționare a Uniunii Europene (TFUE) statuează că în definirea politicilor și acțiunilor sale UE, printre alte obiective, „ține seama” de cerințele unui nivel ridicat de protecție a sănătății umane¹.

¹ Art. 9 TFUE „În definirea și punerea în aplicare a politicilor și acțiunilor sale, Uniunea ține seama de cerințele privind promovarea unui nivel ridicat al ocupării forței de muncă, garantarea unei protecții sociale corespunzătoare, combaterea excluziunii sociale, precum și de

În acest context, se conturează o problemă care vizează capacitatea UE de a armoniza norme în domeniul ocrotirii sănătății în temeiul repartizării competențelor. Acțiunea UE este stabilită prin art. 168 TFUE, care stabilește prin alin. (3) că atât UE, cât și statele membre susțin cooperarea cu țările terțe și organizațiile internaționale competente în domeniul sănătății publice².

Nu mai puțin important este faptul că astfel cum se statuează în alin. (2) al aceluiași art. 168 TFUE, este încurajată cooperarea statelor membre pentru a se asigura îmbunătățirea complementarității serviciilor lor de sănătate în regiunile transfrontaliere³.

Pentru adoptarea unui Regulament european⁴ care să stabilească un cadru juridic pentru funcționarea unor mecanisme de guvernare a datelor personale cu caracter medical în UE într-un mediu de prelucrare securizat, o analiză minuțioasă cu participarea tuturor operatorilor esențiali (autorități de reglementare UE, cercetători, inovatori, responsabili de elaborare a politicilor de securitate ș.a.) este esențială întrucât efectul produs de actul normativ trebuie să fie prevenirea bolilor și tratamentul adecvat al persoanelor fizice. Chiar dacă elaborată și sub imboldul experienței pandemice, propunerea de Regulament este în concordanță cu prioritățile Comisiei de a pregăti Europa pentru era digitală construind o economie adaptată exigențelor și provocărilor unui viitor digitalizat al sănătății.

În privința temeiului juridic, propunerea de Regulament se fundamentează pe art. 14⁵ și art. 114 TFUE⁶ însă considerăm în aceeași măsură ca importantă temeiul art. 16 TFUE⁷.

cerințele privind un nivel ridicat de educație, de formare profesională și de protecție a sănătății umane”.

² Art. 168 alin. (3) TFUE „Uniunea și statele membre favorizează cooperarea cu țările terțe și cu organizațiile internaționale competente în domeniul sănătății publice”.

³ Pentru un studiu aprofundat asupra chestiunilor privind competențele UE în domeniul sănătății a se vedea: D.M. Șandru, C.-M. Banu, *Competențele Uniunii Europene în soluționarea crizei medicale*, în Revista Română de Drept European nr. 4/2021 p. 19.

⁴ Propunerea de Regulament al Parlamentului European și al Consiliului referitor la spațiul european al datelor privind sănătatea poate fi consultat la: <https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX:52022PC0197>.

⁵ Art. 14 TFUE „Fără a aduce atingere articolului 4 din Tratatul privind Uniunea Europeană și articolelor 93, 106 și 107 din prezentul tratat și având în vedere locul ocupat de serviciile de interes economic general în cadrul valorilor comune ale Uniunii, precum și rolul pe care îl au acestea în promovarea coeziunii sociale și teritoriale a Uniunii, Uniunea și statele membre, fiecare în limita competențelor care le revin și în limita domeniului de aplicare a tratatelor, asigură funcționarea serviciilor respective pe baza principiilor și în condiții, în special economice și financiare, care să le permită îndeplinirea misiunilor lor. Parlamentul European și Consiliul, hotărând prin regulamente, în conformitate cu procedura legislativă ordinară, stabilesc aceste principii și prevăd aceste condiții, fără a aduce atingere competenței statelor membre de a furniza aceste servicii, de a încredința prestarea lor și de a le finanța, cu respectarea tratatelor”.

⁶ Art. 114 alin. (1) „Cu excepția cazului în care tratatele dispun altfel, dispozițiile următoare se aplică în vederea realizării obiectivelor enunțate la articolul 26. Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară și după consultarea Comitetului Economic și Social, adoptă măsurile privind apropierea actelor cu putere de lege și a actelor administrative ale statelor membre care au ca obiect instituirea și funcționarea pieței interne”. (...) alin. (3) „În formularea propunerilor prevăzute la alin. (1) în domeniul sănătății, securității, protecției mediului și protecției consumatorilor, Comisia pornește de la premisa asigurării unui nivel ridicat de protecție ridicat, ținând seama în special de orice evoluție nouă,

Propunerea de Regulament se întemeiază pe acte normative precum Regulamentul general privind protecția datelor (RGPD)⁸, Regulamentul privind dispozitivele medicale (Regulamentul privind dispozitivele medicale)⁹, Regulamentul privind dispozitivele medicale pentru diagnostic in vitro (Regulamentul privind diagnosticarea in vitro)¹⁰, propunerea de regulament privind inteligența artificială¹¹, propunerea de regulament privind guvernarea datelor¹² și propunerea de regulament privind datele¹³, Directiva 2016/1148 privind securitatea rețelelor și a sistemelor informatice (Directiva NIS)¹⁴ și Directiva CBHC.

Perioada pandemiei de coronavirus a reprezentat și un test de aplicabilitatea legislației de protecție a datelor și după cum am constatat nicio măsură nu a limitat aplicabilitatea normelor privind apărarea acestui drept fundamental. Cu toate acestea, RGPD oferă un cadru general privind asigurarea securității datelor cu caracter personal și stabilește un regim strict de prelucrare al datelor medicale (date sensibile). Pentru funcționarea unui ecosistem al datelor privind sănătatea apreciem însă că este necesar să fie stabilite standardele privind:

(i) Datele și categoriile de date considerate relevante pentru spațiul european al datelor¹⁵;

întemeiată pe fapte științifice. În cadrul atribuțiilor ce le revin, Parlamentul European și Consiliul depun eforturi, de asemenea, pentru realizarea acestui obiectiv”.

⁷ Art. 16 TFUE (ex-articolul 286 TCE) „(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară, stabilesc normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii, precum și normele privind libera circulație a acestor date. Respectarea acestor norme face obiectul controlului unor autorități independente. Normele adoptate în temeiul prezentului articol nu aduc atingere normelor specifice prevăzute la articolul 39 din Tratatul privind Uniunea Europeană”.

⁸ 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).

⁹ Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, pp. 1-175).

¹⁰ Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5 mai 2017, pp. 176-332).

¹¹ Propunere de regulament de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) COM/2021/206 final.

¹² Propunere de regulament privind guvernarea datelor la nivel european (Legea privind guvernarea datelor) COM/2020/767 final.

¹³ Propunere de regulament privind norme armonizate pentru un acces echitabil la date și o utilizare corectă a acestora (Legea privind datele) COM/2022/068 final.

¹⁴ 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 (JO L 194, 19 iulie 2016, pp. 1-30).

¹⁵ Art. 5 al Propunerii de Regulament, intitulat „Categorii prioritare de date electronice cu caracter personal privind sănătatea pentru utilizare primară”, stabilește:

- (ii) Mijloacele tehnice permise pentru prelucrare acestor date;
- (iii) Formarea personalului operatorilor de date pentru prelucrarea acestor date ceea ce presupune reguli precise și cunoștințe specifice evaluate periodic.

Aceste măsuri ar trebui monitorizate, după cum prevede Propunerea de Regulament, de o autoritate pentru sănătatea digitală: art. 10 stipulând că: „Fiecărei autorități privind sănătatea digitală i se încredințează următoarele sarcini:

(a) asigură punerea în aplicare a drepturilor și obligațiilor prevăzute în capitolele II și III prin adoptarea soluțiilor tehnice necesare la nivel național, regional sau local și prin stabilirea unor norme și mecanisme relevante;

(b) se asigură că informațiile complete și actualizate cu privire la punerea în aplicare a drepturilor și obligațiilor prevăzute în capitolele II și III sunt puse cu promptitudine la dispoziția persoanelor fizice, a cadrelor medicale și a furnizorilor de servicii medicale;

(c) la punerea în aplicare a soluțiilor tehnice menționate la lit. (a), asigură conformitatea acestora cu capitolele II și III și cu anexa II;

(d) contribuie, la nivelul Uniunii, la dezvoltarea de soluții tehnice care să permită persoanelor fizice și cadrelor medicale să își exercite drepturile și obligațiile prevăzute în prezentul capitol;

(e) facilitează exercitarea de către persoanele cu handicap a drepturilor enumerate la art. 3 din prezentul regulament, în conformitate cu Directiva (UE) 2019/882 a Parlamentului European și a Consiliului;

(f) supraveghează punctele naționale de contact pentru sănătatea digitală și cooperarea cu alte autorități privind sănătatea digitală și cu Comisia în ceea ce privește dezvoltarea în continuare a MyHealth@EU;

„(1) În cazul în care datele sunt prelucrate în format electronic, statele membre pun în aplicare accesul la datele electronice cu caracter personal privind sănătatea care se încadrează, integral sau parțial, în categoriile de mai jos și schimbul acestor date, în vederea utilizării primare:

- (a) dosare de sănătate ale pacienților;
- (b) prescripții electronice;
- (c) eliberări electronice de medicamente;
- (d) imagini medicale și rapoarte de imagistică;
- (e) rezultate de laborator;
- (f) rapoarte de externare din spital.

Principalele caracteristici ale categoriilor de date electronice privind sănătatea menționate la primul paragraf sunt stabilite în anexa I. Accesul la datele electronice privind sănătatea și schimbul acestora pentru utilizarea primară pot fi permise pentru alte categorii de date electronice cu caracter personal privind sănătatea disponibile în DES ale persoanelor fizice.

(2) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 67 pentru a modifica lista categoriilor prioritare de date electronice privind sănătatea menționate la alin. (1). Aceste acte delegate pot modifica, de asemenea, anexa I prin adăugarea, modificarea sau eliminarea principalelor caracteristici ale categoriilor prioritare de date electronice privind sănătatea și prin indicarea, după caz, a unei amânări a datei de aplicare. Categoriile de date electronice privind sănătatea adăugate prin intermediul unor astfel de acte delegate îndeplinesc următoarele criterii:

- (a) categoria este relevantă pentru serviciile de sănătate furnizate persoanelor fizice;
- (b) conform celor mai recente informații, categoria este utilizată într-un număr semnificativ de sisteme DES utilizate în statele membre;
- (c) există standarde internaționale pentru categoria respectivă, care au fost examinate în vederea aplicării lor în Uniune”.

(g) asigură punerea în aplicare, la nivel național, a formatului european pentru schimbul de dosare electronice de sănătate, în cooperare cu autoritățile naționale și cu părțile interesate;

(h) contribuie, la nivelul Uniunii, la dezvoltarea formatului european pentru schimbul de dosare electronice de sănătate și la elaborarea unor specificații comune abordând preocupările legate de interoperabilitate, securitate, siguranță sau drepturi fundamentale, în conformitate cu art. 23, precum și a specificațiilor bazei de date a UE pentru sistemele DES și aplicațiile de wellness menționată la art. 32;

(i) după caz, desfășoară activități de supraveghere a pieței în conformitate cu art. 28, asigurându-se totodată că se evită orice conflict de interese;

(j) consolidează capacitatea națională de implementare a interoperabilității și a securității utilizării primare a datelor electronice privind sănătatea și participă la schimburile de informații și la activitățile de consolidare a capacităților la nivelul Uniunii;

(k) oferă, în conformitate cu legislația națională, servicii de telemedicină și se asigură că aceste servicii sunt ușor de utilizat, accesibile diferitelor grupuri de persoane fizice și de cadre medicale, inclusiv persoanelor fizice cu handicap, nu discriminează și oferă posibilitatea de a alege între serviciile cu prezență fizică și cele digitale;

(l) cooperează cu autoritățile de supraveghere a pieței, participă la activitățile legate de gestionarea riscurilor prezentate de sistemele DES și a incidentelor grave și supraveghează punerea în aplicare a acțiunilor corective în conformitate cu art. 29;

(m) cooperează cu alte entități și organisme relevante la nivel național sau la nivelul Uniunii, pentru a asigura interoperabilitatea, portabilitatea datelor și securitatea datelor electronice privind sănătatea, precum și cu reprezentanți ai părților interesate, inclusiv cu reprezentanți ai pacienților, furnizori de servicii medicale, cadre medicale, asociații industriale;

(n) cooperează cu autoritățile de supraveghere în conformitate cu Regulamentul (UE) nr. 910/2014, cu Regulamentul (UE) 2016/679 și cu Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului, cu alte autorități relevante, inclusiv cu cele competente în materie de securitate cibernetică, identificare electronică, Comitetul european pentru inteligența artificială, Grupul de coordonare privind dispozitivele medicale, Comitetul european pentru inovare în domeniul datelor și cu autoritățile competente în temeiul Regulamentului (...) (Legea privind datele – COM/2022/68 final);

(o) elaborează, după caz în colaborare cu autoritățile de supraveghere a pieței, un raport anual de activitate, care conține o prezentare cuprinzătoare a activităților sale. Raportul este transmis Comisiei. Raportul anual de activitate respectă o structură convenită la nivelul Uniunii în cadrul Comitetului pentru spațiul european al datelor privind sănătatea, pentru a sprijini analiza comparativă în temeiul art. 59. Raportul conține cel puțin informații privind:

(i) măsurile luate pentru punerea în aplicare a prezentului regulament;

(ii) procentul de persoane fizice care au acces la diferite categorii de date din dosarele lor electronice de sănătate;

(iii) informații privind tratarea cererilor din partea persoanelor fizice referitoare la exercitarea drepturilor lor în temeiul prezentului regulament;

(iv) numărul de furnizori de servicii medicale de diferite tipuri, inclusiv farmacii, spitale și alte locuri de acordare a asistenței medicale, conectați la MyHealth@EU, calculat: a) în termeni absoluți, b) ca procent din numărul total de furnizori de servicii medicale de același tip și c) ca procent de persoane fizice care pot utiliza serviciile”;

(v) volumele de date electronice privind sănătatea din diferite categorii partajate la nivel transfrontalier prin intermediul MyHealth@EU;

- (vi) nivelul de satisfacție a persoanelor fizice cu privire la serviciile MyHealth@EU;
- (vii) numărul de sisteme DES certificate și de aplicații de wellness cărora li s-a acordat o etichetă, care au fost înscrise în baza de date a UE;
- (viii) numărul de cazuri de neconformitate cu cerințele obligatorii;
- (ix) o descriere a activităților sale desfășurate în legătură cu implicarea și consultarea părților interesate relevante, inclusiv a reprezentanților persoanelor fizice, organizațiilor pacienților, cadrelor medicale, cercetătorilor și comitetelor de etică;
- (x) informații privind cooperarea cu alte organisme competente, în special în domeniul protecției datelor, al securității cibernetice și al inteligenței artificiale”.

Care sunt oportunitățile unei astfel de inițiative legislative la nivel european?

În primul rând apreciem că stabilirea unui cadru de prelucrare a datelor la nivel sectorial – în domeniul sănătății este o abordare promițătoare chiar dacă este atipică pentru politica de până în prezent a UE. Nu putem să nu observăm astfel că are loc o abordare specială prin separarea serviciilor de asistență medicală de directiva privind serviciile. Nu mai puțin adevărat este și faptul că și celelalte acte normative ca de exemplu, Regulamentul privind dispozitivele medicale sau Regulamentul privind dispozitivele medicale pentru diagnostic in vitro și nu în ultimul rând Regulamentul general privind protecția datelor au avut o abordare generală. Ceea ce remarcăm acum este faptul că această propunere legislativă marchează o schimbare în dezvoltarea legislației UE. Pe de o parte asistăm la îndepărtarea de la modelul unei legislații imperative care s-a dovedit ulterior ca fiind problematică în partea practică de implementare necesitând reformări complexe și perioade extinse de implementare pentru a contracara problemele practice insuficient analizate la momentul adoptării, iar pe de altă parte suntem într-o etapă care ne arată că sistemul medical a evoluat îndeajuns încât poate să intervină decisiv în procesul de legiferare¹⁶. Ne aflăm așadar, prin această Propunere de Regulament, în fața unei mari oportunități pentru sistemul medical în ansamblul său pentru că o utilizare mai eficientă a datelor la nivel sectorial, cu măsuri adecvate de securitate și profitând de beneficiile noilor tehnologii va crește eficacitatea sistemului medical în genere.

II. Cercetarea în domeniul medical și spațiul european al datelor privind sănătatea

Ne-am propus să analizăm în acest context și un caz practic pornind de la o cercetare științifică de ordin medical în managementul fistulelor întâlnite în patologia esofagiană. Pentru a realiza o astfel de cercetare este imperios necesar să se analizeze experiența continuă, prezentându-se evaluarea diagnostică și terapeutică multidisciplinară aplicată pacienților. În acest scop sunt necesare date, precum și acces la aceste date pentru analiză și interpretare. Avându-se în vedere faptul că în prezent, în România, cercetarea se realizează prin consultarea cu precădere a datelor din unitatea în care cercetătorul își desfășoară activitatea, accesul la o bază de date (cu respectarea principiului necesității de a cunoaște, precum și cu o instruire adecvată a utilizatorilor)

¹⁶ A se vedea, în acest sens, Studiul de Impact al Propunerii de Regulament, disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com%3AAres%282020%297907993.