editorial

GDPR – 2 ani de aplicare, prezent şi viitor

GDPR – 2 years of enforcement, presently and in the future

dr. DORU DOROBANŢU[1]

Motto: *„Reflecting on the past and future of the EU, we appreciate enormously the extraordinary value in these extraordinary times of three fundamental notions of the EU:* ***Solidarity, Free Movement and Data Protection****".*

„Reflectând asupra trecutului şi viitorului UE, apreciem enorm valoarea extraordinară, în aceste vremuri extraordinare, a celor trei noţiuni fundamentale ale UE: ***solidaritatea, libera circulaţie şi protecţia datelor****".*

Wojciech Wiewiórowski,
European Data Protection Supervisor

La 25 mai 2018 se punea în aplicare Regulamentul General privind Protecţia Datelor, cunoscut sub acronimul GDPR, legislaţie introdusă la nivelul Uniunii Europene cu scopul principal de uniformizare a normelor de protecţie a datelor din statele membre, precum şi pentru îmbunătăţirea confidenţialităţii şi protecţia drepturilor persoanelor vizate de prelucrarea acestor date. Este pe bună dreptate considerat un moment de referinţă privind protecţia şi confidenţialitatea datelor cu caracter personal.

După doi ani, GDPR şi reglementările sale continuă să fie un subiect destul de „fierbinte" în România, dar şi în alte state membre, atât în mediul privat, cât şi în instituţiile publice.

Trebuie să spunem că deşi intrarea sa în vigoare, în anul 2016, a permis operatorilor şi autorităţilor ca timp de doi ani să se organizeze, GDPR a ajuns să fie pus în aplicare în România într-un moment în care majoritatea companiilor erau foarte puţin sau deloc pregătite. Este de discutat dacă aceasta s-a datorat nepăsării şi lipsei de interes a operatorilor după ani de aplicare a reglementărilor existente, respectiv Legea

[1] Lector asociat/CS III la Universitatea Politehnica din Bucureşti, Secretar general de redacţie Revista Română pentru Protecţia şi Securitatea Datelor cu Caracter Personal.

nr. 677/2001, lipsei de înţelegere a noilor reglementări europene ori deficienţelor de mediatizare a noilor reglementări.

O problemă la fel de gravă a fost, în unele cazuri, calitatea slabă a consilierii pe care a primit-o managementul companiilor de la cei desemnaţi să facă acest lucru, fie că vorbim de persoane fizice, fie de anumite firme de consultanţă. Chiar şi pentru aceia care au avut în atenţie preocuparea de a fi pregătiţi pentru implementarea cerinţelor GDPR înainte de luna mai 2018 şi, într-adevăr, companii importante au angajat persoane sau firme specializate pe acest segment juridic, au existat situaţii în care suportul a fost lipsit de substanţă ori nu s-a înţeles pentru că nu a fost adecvat specificului situaţiei lor.

Dacă ne orientăm analiza către amenzile aplicate de autorităţile se supraveghere din statele membre, inclusiv Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), în primul an vom constata că acestea au fost puţine (9) şi blânde (cuantum total de aproximativ 436.400 euro), abordarea fiind mai degrabă una de a încerca educarea operatorilor atunci când au fost constatate nereguli. Este adevărat că nici nu ne aşteptam la altceva, mai ales că investigarea, de exemplu, a unei încălcări a securităţii datelor necesită timp pentru a putea aprecia şi sancţiona obiectiv acest tip de incident.

În confirmarea celor de mai sus, la marcarea a 2 ani de la data aplicării efective a Regulamentului General pentru Protecţia Datelor, ANSPDCP menţiona pe site: *„Dacă anul 2018 a fost marcat de adoptarea legislaţiei naţionale aplicabile (Legea nr. 129/2018, Legea nr. 190/2018), inclusiv a deciziilor normative ale Autorităţii, putem afirma că, începând cu anul 2019, s-a dat efectivitate deplină monitorizării implementării corecte a noului Regulament şi a reglementărilor naţionale aferente, la nivelul operatorilor din sectorul public şi privat. Afluxul plângerilor şi al solicitărilor de puncte de vedere primite în aceşti doi ani au constituit un important indicator pentru instituţia noastră cu privire la existenţa unei creşteri reale a nivelului de conştientizare a publicului larg referitor la drepturile de care beneficiază, precum şi a interesului semnificativ al operatorilor în respectarea noilor reguli europene".*

O abordare vizibil mai fermă a autorităţilor am constat-o în cel de-al doilea an al GDPR, cu amenzi semnificative aplicate unor actori majori în domeniul prelucrării datelor cu caracter personal, precum furnizorii de servicii de internet şi telecomunicaţii, hoteluri sau operatori aerieni.

Semnalul privind încheierea perioadei de aşteptare pentru îndeplinirea cerinţelor de conformitate cu prevederile Regulamentului a fost dat brusc, în ianuarie 2019, de către autoritatea de supraveghere din Franţa, Commission nationale de l'informatique et des libertés (CNIL), care după 5 luni de investigaţie a aplicat gigantului Google o amendă record de 50 milioane de euro pentru încălcarea regulilor de transparenţă, a informării insuficiente a persoanelor vizate şi, nu în ultimul rând, a lipsei unui consimţământ valabil exprimat de către persoanele vizate pentru personalizarea publicităţii livrate prin intermediul telefoanelor mobile cu sistem de operare Android. Aceasta a fost urmată imediat de autoritatea italiană care a amendat operatorul de telefonie mobilă TIM cu 27.8 milioane de euro pentru prelucrarea ilegală a datelor în scopuri de marketing, iar în luna iulie 2019, de autoritatea britanică, Information Commissioner's Office (ICO), care a sancţionat Marriott International Inc. cu 99 milioane sterline (110.390.200 euro) şi British Airways cu 183 milioane lire sterline (204.600.000 euro), aceasta din urmă fiind până în prezent cea mai mare amendă aplicată în Europa.

Trebuie subliniat faptul că scopul principal al GDPR este acela de îmbunătăţire a securităţii şi confidenţialităţii, de apărare a drepturilor şi libertăţilor persoanelor vizate, prin protecţia prelucrării datelor cu caracter personal care să respecte principiile

necesității, proporționalității, transparenței și responsabilității. Referindu-ne generic la eficacitatea măsurilor de până acum, nu putem să nu observăm o transformare în bine.

Din punct de vedere al creșterii nivelului de conștientizare și înțelegere a persoanelor cu privire la problemele legate de confidențialitate și drepturile la viață privată, în general, și la protecția datelor cu caracter personal, în special, GDPR a avut cu siguranță un impact major.

În același timp, persoane vizate mai conștiente și mai educate au determinat și creșterea neîncrederii atunci când a fost vorba de prelucrarea datelor cu caracter personal de către autorități, ceea ce nu a făcut decât să contribuie la prevenirea utilizării excesive sau neadecvate a acestor date.

Acest lucru a putut fi observat atunci când, în contextul pandemiei COVID-19, au fost impuse sau recomandate, este adevărat că nuanțat la nivelul anumitor state membre (printre care și România), prin acte normative cu putere de lege, măsuri care obligă la prelucrarea unor categorii speciale de date, respectiv cele privind starea de sănătate, sau cu privire la inițiativa de dezvoltare, la nivel european, a unor aplicații de urmărire a contactelor COVID-19.

Foarte atenți la implicațiile prelucrării acestor date, persoane fizice, organizații, practicieni și specialiști în drept s-au exprimat pentru dezbateri deschise privind respectarea principiilor și asigurarea garanțiile adecvate, scopul și perioada de retenție a acestor date. Încă o dovadă că publicul înțelege mult mai bine care îi sunt drepturile și cum poate acționa cu privire la protecția propriilor date cu caracter personal.

Tot în perioada de referință, având în vedere cuantumul deosebit de mare al amenzilor prevăzut de GDPR pentru încălcarea securității datelor cu caracter personal – până la 20 de milioane EUR sau 4% din cifra de afaceri globală anuală – companiile au devenit mult mai atente în ceea ce privește securizarea sistemelor informatice. S-a constatat astfel că GDPR a contribuit la îmbunătățirea practicilor de securitate cibernetică ale companiilor, chiar dacă nu acesta este obiectivul principal al legislației.

Un alt impact semnificativ al GDPR este influența acestuia la nivel internațional, devenind un element de referință pentru legi de protecție a datelor mult mai stricte și mai ample pentru a proteja persoanele fizice la nivel global. Legea privind protecția consumatorilor din California (California Consumer Privacy Act AB-375), care și-a început aplicarea la 1 ianuarie 2020, reprezintă răspunsul transatlantic la Regulamentul General privind Protecția Datelor. De asemenea, New York Shield Act, Privacy Data Protection Act (PDPA) din Singapore sau Principiile privind confidențialitatea (Privacy Principles) adoptate de guvernul australian și Legea generală privind protecția datelor din Brazilia sunt toate exemple de legislație care urmează principiile create de GDPR, de unde putem concluziona că există o influențare a legislației globale.

Cu toate acestea, atât autoritățile de supraveghere cât și organizațiile, fie că vorbim despre entități publice fie despre cele private, mai au multe de făcut, iar ceea ce este foarte important este conștientizarea și formarea celor care prin natura atribuțiilor de serviciu prelucrează diferite categorii de date cu caracter personal, din perspectiva creșterii responsabilității și abordării preventive pentru reducerea incidentelor de securitate. Deși există o tendință clară la nivel european de îmbunătățire a sistemelor care asigură securitatea informatică, de multe ori este ignorat faptul că cea mai mare vulnerabilitate pentru securitate o reprezintă factorul uman. Lipsa unor programe de pregătire și instruire inițială și continuă care să se desfășoare în mod constant, ori minimizarea importanței acestor activități, generează de cele mai multe ori probleme ce afectează organizațiile atât financiar cât și din punct de vedere al credibilității în domeniile în care activează.

Dacă privim din perspectiva autorităţilor de supraveghere, deşi nu pare cea mai mare problemă, totuşi, notificarea excesivă a situaţiilor ipotetic considerate incidente de securitate a condus la supraîncărcarea activităţii acestora şi, prin urmare, la afectarea unor investigaţii importante. Această situaţie a fost generată într-o mare măsură de excesul de a nu greşi al operatorilor, speriaţi de potenţialul unei sancţiuni contravenţionale mari pentru nerespectarea obligaţiei de notificare prevăzută la art. 33 din GDPR. Pe de altă parte, această situaţie ne poate conduce la ideea că poate este necesară o interpretare mai clară, o delimitare într-un ghid sau metodologie, care să asigure pentru operatori limitarea exactă a situaţiilor care obligă la notificarea autorităţilor de supraveghere competente. Potrivit raportului Asociaţiei Internaţionale a Profesioniştilor în Confidenţialitate (IAPP) numai în anul 2018 s-au transmis peste 64.000 de notificări către autorităţile naţionale de supraveghere; cu toate acestea doar în 240 cazuri au fost aplicate amenzi.

Pe de altă parte, din analiza sancţiunilor aplicate în perioada 2018-2020 s-a putut constata o oarecare incoerentă a acţiunilor diferitelor autorităţi din statele membre. Dacă unele autorităţi şi-au concentrat activitatea pe două-trei investigaţii mari, cum este cazul Marii Britanii sau Franţei, altele au abordat cazuri mai numeroase dar mai mici (Spania, România, Ungaria). De asemenea, s-a putut constata o activitate mai intensă în anumite state, marcată de implicare şi transparenţă în activităţile publice ale acestora, de unde se poate deduce că este nevoie de o mai bună armonizare şi o mai strânsă cooperare între aceste autorităţi.

Am lăsat la final un subiect care nu poate fi ignorat. Actuala pandemie COVID-19 are un impact profund asupra afacerilor la nivel mondial. Industria, lanţurile de aprovizionare, organizarea evenimentelor şi călătoriile sunt deja afectate şi există un impact semnificativ asupra cetăţenilor şi funcţionării tuturor organizaţiilor. Situaţia rămâne imprevizibilă, iar organizaţiile sunt în situaţia de a acţiona prompt pentru a schimba rapid abordarea cu privire la toate circumstanţe, inclusiv aspectele referitoare la prelucrarea şi protecţia datelor cu caracter personal.

Pandemia de coronavirus a accelerat digitalizarea în toate domeniile iar infrastructura ori deprinderile digitale ale persoanelor nu au mai reprezentat impedimente pentru a răspunde nevoilor situaţiei actuale. Domenii până mai ieri considerate incompatibile cu accesul de la distanţă, precum învăţământul, serviciile publice sau cele de sănătate au fost forţate la transferul on-line.

Creşterea bruscă, fără precedent, a numărului persoanelor angajate care lucrează de acasă reprezintă pe lângă preocupările legate de securitate cibernetică, provocări suplimentare pentru organizaţii în ceea ce priveşte protecţia datelor. Deoarece o mare parte a organizaţiilor nu obişnuiau să lucreze în regim de telemuncă, neavând organizată infrastructura, proceduri ori mecanisme interne pentru a permite un acces securizat şi facil la sisteme, baze de date şi aplicaţii, acestea au fost nevoite să se adapteze din mers la noua filozofie, asumându-şi de cele mai multe ori riscuri care includ inerent încălcarea confidenţialităţii, integrităţii sau disponibilităţii datelor cu caracter personal prelucrate. Lucrurile au fost accelerate iar instituţii ale statului au fost nevoite să facă eforturi pentru a oferi acces on-line la servicii, altfel amorţite în prea multă birocraţie.

Totodată, necesitatea distanţării sociale a obligat cetăţenii sa devină mai confortabili cu interacţiunea virtuală, mai toleranţi şi deschişi la conceptul de partajare a propriilor date personale.

Ceea ce nu trebuie să uităm însă este că dependenţa de mediul digital şi convieţuirea cu noile tehnologii vine la pachet cu asumarea unor riscuri. Tocmai în acest

context, concepte precum *accountability*, *privacy by design*, *privacy by default* sau *data protection impact assessment* îşi găsesc adevăratul sens şi trebuie să fie obligatoriu parte a noilor strategii dezvoltate de organizaţii pentru abordarea operaţiunilor de prelucrare a datelor personale.

În final, putem aprecia că dată fiind complexitatea şi aria vastă de aplicabilitate a reglementărilor GDPR ar fi fost de neconceput lipsa provocărilor sau a confruntărilor în primii ani de aplicare a sa. Cel puţin aparent, atât operatorii cât şi autorităţile de supraveghere sunt mai degrabă încă în situaţia de a se obişnui cu exigenţele Regulamentului, iar aceasta contribuie la îmbunătăţirea treptată a practicilor în domeniul protecţiei datelor, cu efect direct în reducerea incidentelor care ar putea afecta drepturile şi libertăţile persoanelor ale căror date sunt prelucrate.

Cel mai mare câştig, la finalul celor doi ani de aplicare a GDPR, este acela al creşterii gradului de conştientizare a problemelor de confidenţialitate a publicului larg şi cunoaşterii drepturilor pe care persoanele vizate de prelucrări le au, esenţial pentru o societate din ce în ce mai digitalizată în care ameninţările generate de utilizarea ilegală şi criminalitatea informatică reprezintă o realitate.

Care va fi evoluţia viitoare a reglementărilor?

Schimbările pe care pandemia COVID-19 le-a produs în societate, şi în particular în peisajul prelucrării datelor cu caracter personal, reprezintă o oportunitate pentru ca inovaţia şi tehnologia să stimuleze elaborarea unor mecanisme adecvate de creştere a responsabilităţii şi a gradului de conştientizare astfel încât să permită asigurarea protecţiei drepturilor fundamentale ale cetăţenilor.

Libertatea de exprimare şi protecţia datelor cu caracter medical în timpul stării de urgenţă impuse de pandemia COVID-19 din anul 2020

Freedom of expression and protection of medical data during the state of emergency imposed by the 2020 COVID-19 outbreak

NICOLAE PLOEŞTEANU[1]

❑ Rezumat

În perioada pandemiei, o serie de drepturi şi libertăţi au fost restrânse şi supuse unui test de eficienţă datorită necesităţii de a se combate transmiterea virusului şi de a fi luate măsuri adecvate pentru gestionarea în ansamblu a comunităţilor. Fiecare stat a avut propriul său mod de abordare, care a variat la rândul său în funcţie de perioadă, de circumstanţele naţionale şi regionale şi de modul de reacţie a populaţiei la diferitele măsuri. Printre drepturile cele mai încercate s-au numărat dreptul la liberă circulaţie, dreptul la ocrotirea sănătăţii, dreptul la viaţă privată sau chiar libera exprimare. Studiul îşi propune să ofere perspective juridice asupra situaţiei în care unele liste cu date cu caracter personal ale celor infectaţi sau suspecţi de infectare au fost divulgate în mod nelegal către public, după care au fost retransmise pe reţele de socializare sau chiar în mass media instituţionalizată.

Cuvinte-cheie: *Regulamentul General privind Protecţia Datelor; Covid-19; libertatea de exprimare; date cu caracter medical; divulgare.*

❑ Abstract

During the pandemic crisis a number of rights and liberties have had restrained and in fact passed through an efficiency test because of necessity to prevent or combat the Covid-19, in an attempt to manage the community as a whole. Each state have its own manner in this fight, depending on the national and regional circumstances, the period and evolution of the pandemia or the diverse reactions of the people of a specific community. Among the most tried rights were the right to free

[1] Nicolae Ploeşteanu este doctor conferenţiar în cadrul Universităţii de Medicină, Farmacie, Ştiinţe şi Tehnologie „George Emil Palade" din Târgu Mureş, fiind director Centrului de Studii pentru Protecţia Datelor.

movement, the right to health care, the right to privacy or even free expression. The study aims to provide legal perspectives on the situation in which some lists of personal data of those infected or suspected of being infected were illegally disclosed to the public, after which they were relayed on social networks or even in the institutionalized media.

Keywords: *GDPR; Covid-19; freedom of expression; medical health data; data disclosure.*

1. Ipoteza/ipotezele supuse analizei

În aceste zile[2] de angajare a întregii societăţi şi a întregului aparat de stat în lupta împotriva Covid-19, fiecare corp profesional (inclusiv juriştii, fie ei procurori, judecători, notari, agenţi de aplicare a legii, executori, avocaţi etc.) se confruntă cu numeroase provocări, iar una dintre acestea priveşte cu certitudine ***Libertatea de exprimare***, prin simpla comunicare, prin presa scrisă sau on-line. Adesea au apărut mesaje oficiale adresate de instituţii abilitate[3], mesaje prin care se anunţa că cei care divulgă sau transmit ori prelucrează listele în care erau consemnate date cu caracter personal ale unor persoane infectate cu Covid-19 sau doar suspecţi, pot să fie supuşi unor sancţiuni, cum ar fi închisoarea sau amenda. În general, asemenea mesaje au pornit de la premisa reală că respectivele informaţii ar avea fie caracter de secret de serviciu, fie că nu sunt destinate publicităţii.

Câteva opinii juridice asupra ipotezei aflate în studiu!

2. În această situaţie de excepţie, întrebarea firească este Dacă nu avem dreptul să cunoaştem informaţii de genul celor de mai sus, iar dacă nu, atunci care sunt impedimentele?

Pentru a răspunde la această întrebare, pentru început, trebuie să constatăm că populaţia are un drept fundamental, prevăzut de art. 31 al Constituţiei României, anume ***dreptul la informaţie***. Acest articol[4] garantează oricărei persoane dreptul de a avea

[2] Materialul este elaborat în perioada martie-aprilie 2020.

[3] https://www.mediafax.ro/social/o-lista-cu-15-persoane-infectate-cu-noul-covid-19-a-circulat-in-mures-pe-paginile-de-facebook-si-pe-whatsapp-19047254, site vizitat la data de 8 aprilie 2020; https://www.zi-de-zi.ro/2020/04/03/ultima-ora-lista-cu-zonele-din-targu-mures-infectate-cu-covid-19-reala/, site vizitat la data de 8 aprilie 2020.

[4] Articolul 31 din Constituţia României, dreptul la informaţie:

(1) Dreptul persoanei de a avea acces la orice informaţie de interes public nu poate fi îngrădit.

(2) Autorităţile publice, potrivit competenţelor ce le revin, sunt obligate să asigure informarea corectă a cetăţenilor asupra treburilor publice şi asupra problemelor de interes personal.

(3) Dreptul la informaţie nu trebuie să prejudicieze măsurile de protecţie a tinerilor sau securitatea naţională.

(4) Mijloacele de informare în masă, publice şi private, sunt obligate să asigure informarea corectă a opiniei publice.

(5) Serviciile publice de radio şi de televiziune sunt autonome. Ele trebuie să garanteze grupurilor sociale şi politice importante exercitarea dreptului la antenă. Organizarea acestor servicii şi controlul parlamentar asupra activităţii lor se reglementează prin lege organică.

acces la ***orice informaţie de interes public***, iar autorităţile publice sunt obligate să asigure o informare corectă a cetăţenilor asupra treburilor publice sau asupra problemelor de interes personal.

Ca urmare, din această perspectivă chestiunea de a se cunoaşte listele cu persoanele infectate, izolate sau carantinate s-ar putea rezuma la a se şti în primul rând dacă asemenea informaţii sunt sau nu de interes public iar, în al doilea rând, dacă informarea ar trebui realizată chiar de către autorităţile statului, deoarece reprezintă „treburi publice" sau priveşte „probleme de interes personal" ale altora.

Nu răspunsul la aceste întrebări este dificil, ci identificarea unei soluţii legale asupra situaţiei privită în ansamblul său, deoarece apare cu evidenţă că asemenea date sunt de interes public[5], cel puţin identitatea persoanelor şi localizarea lor, din multe puncte de vedere: unii nu mai ştiu de rudele lor şi doresc să afle pe orice cale dacă se numără printre cei supuşi unei intervenţii de acest tip (internare, izolare, carantină etc.); alţii doresc să cunoască dacă într-o anumită zonă există un risc mai mare sau mai mic, în funcţie de anunţurile făcute. Este foarte adevărat că în anumite situaţii nu este necesară identificarea persoanei în mod direct, dar precizarea domiciliului poate conduce la identificarea sa. În fine, astfel cum opinam soluţia informării este cea delicată şi asupra căreia trebuie să se lucreze.

3. Cât de mult, asemenea informaţii pot fi supuse unui secret profesional sau chiar inserate într-un mecanism de secretizare prin care controlul judiciar la cererea unui posibil justiţiabil devine mult mai anevoios şi mai ales mult mai lent?[6]

Trebuie spus, că în mod obişnuit, datele referitoare la starea medicală a unei persoane intră în categoria datelor sensibile şi, de principiu, nu sunt destinate publicităţii, fiind vorba de protecţia vieţii private a persoanei despre a cărei sănătate este vorba. Din acest motiv, relaţia de confidenţialitate dintre medic şi pacient este supusă unor garanţii, precum secretul profesional. Ca urmare, de principiu, asemenea date, precum cele din ipoteza supusă analizei nu se vor divulga şi vor angaja răspunderea juridică a celor care sunt supuşi obligaţiei de secret profesional.

Cu toate acestea trebuie să observăm că din momentul în care asemenea date sunt făcute publice pe reţele de socializare, re-transmiterea de către persoanele fizice a acestor date nu este supusă obligaţiei de secret profesional, pe de o parte, şi nici nu mai pot fi văzute ca fiind nedestinate publicităţii, din moment ce acestea sunt deja publice într-o reţea de socializare. Ca urmare, pare destul de hazardat să fie anunţată o comunitate de persoane, mai mică sau mai mare, de începerea procedurilor penale pentru săvârşirea infracţiunii prevăzute de art. 304 alin. (2) C. pen.: „Divulgarea, fără drept, a unor informaţii secrete de serviciu sau care nu sunt destinate publicităţii, de

[5] La articolul 2 lit. b) din Legea nr. 544/2001 privind liberul acces la informaţiile de interes public se defineşte informaţia de interes public astfel: „orice informaţie care priveşte activităţile sau rezultă din activităţile unei autorităţi publice sau instituţii publice, indiferent de suportul ori de forma sau de modul de exprimare a informaţiei".

[6] Spre exemplu, articolul 12 alin. (1) lit. a) din Legea nr. 544/2001, exceptează de la accesul liber al cetăţenilor informaţiile din domeniul apărării naţionale, siguranţei şi ordinii publice, dacă fac parte din categoriile informaţiilor clasificate, potrivit legii, astfel că accesul la aceste informaţii va fi permis cetăţeanului doar în urma unei intervenţii a instanţei de judecată, în condiţiile articolului 21 şi urm. din aceeaşi lege.

către cel care ia cunoştinţă de acestea, se pedepseşte cu închisoare de la o lună la un an sau cu amendă". Oricum, această situaţie va genera cel mai probabil în viitor cauze celebre, deoarece trebuie să se lămurească ce înseamnă în acest context „divulgare", din moment ce situaţia este deja publică şi, totodată, trebuie să se lămurească măsura în care o persoană care ia la cunoştinţă în afara atribuţiilor de serviciu, de pe o reţea de socializare, despre asemenea informaţii precum cele puse în discuţie, putea să aibă la cunoştinţă că respectivele informaţii nu sunt destinate publicităţii sau, mai mult decât atât, că ar avea caracter de secret de serviciu.

În concluzie, răspunsul la această a doua întrebare este în sensul că informaţii precum cele medicale, referitoare la starea de sănătate a unei persoane (chiar şi în cazul unui suspect), reprezintă informaţii obţinute în cadrul unei relaţii de confidenţialitate şi sunt supuse secretului profesional. Totuşi, autorităţile trebuie să stabilească cu atenţie nivelul de confidenţialitate acordat acestor informaţii, pentru a nu aduce atingere altor modalităţi de a informa opinia publică în legătură cu aspecte de interes public, precum zona specifică „roşie", potenţialele riscuri etc. În plus, trebuie acordată o atenţie aparte evaluării juridice a infracţiunii asociate divulgării, pentru a nu genera efecte sociale neoportune, inadecvate şi disproporţionate în raport de circumstanţele faptice propriu-zise.

4. O întrebare interesantă ar fi dacă în anumite circumstanţe se poate deroga de la obligaţia de a păstra secretul profesional, atunci când ne referim la date personale cu caracter medical

Pentru a răspunde într-o anumită măsură la această întrebare trebuie făcută o incursiune în cazuistica judiciară şi făcute anumite precizări.

Sub aspect general, intruziunea medicului în viaţa privată a pacientului, prin divulgarea datelor medicale ale acestuia, este interzisă, medicul având obligaţia respectării confidenţialităţii. Totuşi, există situaţii care impun într-o oarecare măsură divulgarea acestora, atât pentru protecţia pacientului cât şi a altor persoane, vorbind astfel de un scop legitim al divulgării.

Stabilirea întinderii acestei obligaţii de confidenţialitate este destul de dificilă. Totuşi, trebuie să ne raportăm la scopul şi necesitatea divulgării. În jurisprudenţa din Statele Unite ale Americii, o cauză celebră, cauza Tarasoff[7] (intrată ulterior în manualele de etică medicală şi de drept din SUA şi apoi din întreaga lume), a schimbat perspectiva abordării problematicii secretului profesional. În această cauză, în urma unor gelozii şi şedinţe de psihoterapie, numitul Poddar intenţiona să o ucidă pe Tarasoff, anunţându-i medicului intenţiile sale. Medicul a informat imediat poliţia, transmiţându-le că Poddar este periculos şi ar trebui internat într-un spital psihiatric. Poliţia l-a arestat şi investigat pe Poddar, dar l-a eliberat în schimbul unei promisiuni a acestuia că nu se va mai apropia de Tatiana. Două luni mai târziu, în octombrie 1969, Poddar a intrat în casa Tatianei Tarasoff, a omorât-o cu un cuţit de bucătărie şi apoi s-a predat poliţiei.

Părinţii Tatianei au acuzat Universitatea Berkeley, psihoterapeutul şi poliţia, de incapacitatea de a preveni o astfel de crimă şi, de asemenea, că nu i-au avertizat în legătură cu pericolul în care se afla fiica lor. Psihoterapeutul s-a apărat invocând obligaţia sa de păstrare a secretului profesional.

[7] A se vedea N. Ploeşteanu, C. Csiszar, *Prelucrarea de date medicale, exercitarea dreptului la liberă exprimare şi protecţia acestor date. Studiu de caz*, în Revista Română de Drept European nr. 1/2020.

Curtea Supremă a statului California a statuat că „o dată ce un terapeut determină sau, în conformitate cu standardele profesionale aplicabile în mod rezonabil, ar fi trebuit să determine, că un pacient reprezintă un pericol grav de violenţă asupra altora, el ***are datoria de a exercita o grijă rezonabilă pentru a proteja victima previzibilă a acestui pericol***. Având în vedere că îndeplinirea acestei obligaţii de diligenţă va varia în mod necesar în funcţie de circumstanţe, în fiecare caz caracterul adecvat al comportamentului terapeutului trebuie măsurat în raport cu standardul de neglijenţă tradiţională a asigurării îngrijirii rezonabile în circumstanţele date".

Curtea a concluzionat că „un medic nu poate înşela încrederea acordată lui în cursul îngrijirii medicale, cu excepţia cazului în care este obligat să facă acest lucru prin lege sau ***cu excepţia cazului în care devine necesar pentru a proteja bunăstarea individului sau a comunităţii***".

Situaţia pandemică din prezent nu este una obişnuită, astfel că obligaţia de confidenţialitate trebuie supusă unui test. Însă, acest test este în primul rând în competenţa autorităţilor publice să îl facă, în special stabilind raportul concret dintre necesitatea informării publice în legătură cu persoane sau zone care prezintă un risc ridicat, pe de o parte şi protecţia vieţii private a celor despre a căror date medicale este vorba, pe de altă parte, raportându-se la circumstanţe precum: capacitatea de intervenţie a instituţiilor publice în combaterea epidemiei într-o zonă determinată, nivelul concret de răspândire a epidemiei în acea zonă, întreprinderea unor măsuri eficiente de diminuare a riscului, numărul de persoane afectate de virus situate pe o zonă determinată, gradul de populare din acea zonă şi necesităţile de circulaţie, gradul de izolare din punct de vedere fizic şi social al unei locuinţe, calitatea de persoană publică, nivelul de panică, tipologia culturală a unei comunităţi etc. Urmare a unei asemenea evaluări se poate înlătura obligaţia de confidenţialitate sau i se poate redefini limitele, mai largi sau dimpotrivă mai restrânse. Oricum aceste chestiuni în situaţii de criză, precum cea de faţă, se găsesc în primul rând în apanajul autorităţilor publice. Este însă semnificativ în acest cadru, faptul că testul final trebuie realizat de o instanţă de judecată[8], astfel cum cer standardele juridice.

5. O chestiune extrem de importantă de cunoscut este aceea dacă odată „publice" anumite date chiar cu caracter medical, acestea angajează vreo formă de răspundere, alta decât cea penală? Iar dacă da, cum ar funcţiona un astfel de mecanism şi dacă el funcţionează identic în toate cazurile?

Trebuie spus că există o legislaţie specifică în domeniul protecţiei datelor personale. În special este vorba despre Regulamentul General privind Protecţia Datelor (GDPR), act legislativ european care are prioritate[9] asupra altor acte normative naţionale, potrivit art. 148 din Constituţia României. GDPR interzice divulgarea datelor cu caracter medical, stabilind câteva excepţii de la această interdicţie. Însă GDPR

[8] A se vedea o idee asemănătoare formulată cu titlu general de autorii prof. univ. dr. D.-M. Şandru, dr. I. Alexe, *Subiectele Regulamentului General privind Protecţia Datelor în caleidoscopul nuanţelor de fericire*, în Pandectele Române nr. 3/2019, p. 79.

[9] A se vedea şi N. Ploeşteanu, R. Miron, *Supremacy of European Law and possible judicial remedies in regard to the issue of Romania's Accession to the Schengen Area*, în Revista Curentul Juridic nr. 1 (56)/2014, p. 14.

stabileşte obligaţii pentru operatorii de date şi în anumite condiţii. Postările pe reţelele de socializare sau transmiterea prin mass media a datelor medicale va angaja răspunderea atât a celor care postează, publică etc., cât şi a reţelelor de socializare, gradul de răspundere variind după numeroşi indicatori, până la exonerare de răspundere, în anumite situaţii: numărul de date divulgate, intenţia frauduloasă, numărul de receptori, măsurile imediat luate după luarea la cunoştinţă în privinţa nerespectării legii, contextul divulgării, aparenta legitimitate etc. Subiectul poate fi extrem de mult dezbătut! Mai mult, în contextul actual, situaţia juridică este complicată de starea de urgenţă, deoarece atrage aplicabilitatea nu doar a GDPR ci şi a legii de transpunere a Directivei europene nr. 680/2016, care permite un regim mai restrictiv, este adevărat că opozabil în special autorităţilor de aplicare a legii, privind prelucrările de date cu caracter personal.

Ca urmare, aparentul răspuns la prima parte a întrebării este că divulgarea pe reţele de socializare sau de către mass media a datelor cu caracter personal medicale, reprezintă o încălcare a GDPR şi poate să angajeze răspunderea administrativă de natură financiară a celor care sunt implicaţi în astfel de divulgări, în conformitate cu prevederile acestui act normativ. Cu toate acestea, s-ar putea argumenta, aşa cum vom vedea la punctul următor, că acesta este doar un răspuns aparent.

6. Există totuşi o „portiţă legislativă" atunci când avem în vederea dezvăluirea datelor cu caracter medical de către mass media sau alte alternative?

Pentru a răspunde la această întrebare trebuie să se ţină cont de regimul libertăţii de exprimare prin presă(în scopuri jurnalistice) stabilit de GDPR şi care este regimul stabilit presei prin actele normative specifice stării de urgenţă.

Cu privire la prima chestiune. Regula generală privind ***raportul dintre dreptul la protecţia datelor cu caracter personal şi libertatea de exprimare*** este stabilită de art. 85 din RGPD. Alin. (1) al acestui articol impune obligaţia statelor membre să asigure „un echilibru între dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament şi dreptul la libertatea de exprimare şi de informare, inclusiv ***prelucrarea în scopuri jurnalistice*** sau în scopul exprimării academice, artistice sau literare" prin intermediul dreptului intern.

Art. 85 cuprinde 3 alineate şi constituie *inter se* o excepţie de la regimul juridic general al GDPR aplicabil în domeniul protecţiei datelor, aspect care reiese din însăşi interpretarea tehnico-legislativă a GDPR şi din conţinutul articolului: raportul dintre drepturile amintite este tratat distinct într-un articol, spre deosebire de multe alte domenii pentru care nu sunt realizate referinţe speciale şi acest aspect se coroborează cu statuările din art. 85 potrivit cărora statele membre pot stabili derogări prin dreptul intern de la mai multe capitole ale RGPD, inclusiv capitolul privind principiile în domeniul protecţiei datelor, ori de câte ori este necesar să se atingă obiectivul justului echilibru. În considerentul 153 al RGPD se evidenţiază o regulă de interpretare necesară identificării sferei de aplicabilitate *rationae materiae* a acestui articol, anume că „Pentru a ţine seama de importanţa dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noţiunile legate de această libertate, cum ar fi *jurnalismul*, să fie interpretate în sens larg".

Pentru a asigura aplicarea RGPD şi a împlini cadrul legislativ din domeniul protecţiei datelor, legiuitorul român a adoptat ***Legea nr. 190/2018*** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al