

CUPRINS

În atenția colaboratorilor.....	9
---------------------------------	---

EDITORIAL

GDPR – 2 ani de aplicare, prezent și viitor Doru Dorobanțu	10
--	----

STUDII ȘI CERCETĂRI

Libertatea de exprimare și protecția datelor cu caracter medical în timpul stării de urgență impuse de pandemia COVID-19 din anul 2020 Nicolae Ploșteanu	15
--	----

Ciocnirea valorilor: legea română privind liberul acces la informațiile de interes public și protecția datelor personale Alexandru Georgescu, Irina Alexe, Daniel-Mihail Șandru	24
---	----

Orientarea nr. 3/2019 a Comitetului european pentru protecția datelor privind prelucrarea datelor cu caracter personal prin dispozitive video și aplicabilitatea acesteia în dreptul român Adriana Akyol	34
--	----

Legea californiană privind protecția datelor consumatorilor Ioan-Luca Vlad	55
--	----

PRAXIS

O scurtă privire critică asupra unei preconizate completări a contractelor de studii universitare de doctorat Silviu-Dorin Șchiopu	63
--	----

Utilizarea mijloacelor de supraveghere video și de geolocalizare în cadrul relațiilor de muncă Georgiana Trifan	70
---	----

OPINII

Folosirea datelor de localizare prin intermediul dispozitivelor mobile în contextul pandemiei COVID-19 Ramona Mihaela Coman	78
---	----

A fost nevoie de acest coronavirus pentru a înțelege mai bine GDPR-UL Marius Dumitrescu	85
---	----

SECTORIAL

Propunere <i>de lege ferenda</i> privind prelucrarea datelor cu caracter personal ale beneficiarului unui contract de asigurare de viață Silviu-Dorin Șchiopu	90
Atacurile cibernetice asupra spitalelor în contextul pandemiei COVID-19 Sonia Bianca Coman	97

STUDII DE CAZ

Dreptul persoanei vizate la informare – între utilitate și obligație Daniela Simionovici	102
De unde provine falsa supremație a consimțământului ca temei legal al prelucrării datelor personale? Marius Dumitrescu, Daniela Cireașă	111

MONITORUL PROTECȚIEI DATELOR

Informare cu privire la amenzile contravenționale aplicate de ANSPDCP în domeniul RGPD, comunicate în perioada 13 decembrie 2019 – 5 mai 2020 Irina Alexe	118
Sinteza amenzilor GDPR aplicate la nivel european, în primele cinci luni ale anului 2020 Marius Dumitrescu, Daniela Cireașă	126

editorial

GDPR – 2 ani de aplicare, prezent și viitor

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

dr. DORU DOROBANȚU¹

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 și viitorului UE, apreciem enorm valoarea extraordinară, în aceste vremuri extraordinare, a celor trei noțiuni fundamentale ale UE: **solidaritatea, libera circulație și protecția datelor**”.

Wojciech Wiewiórowski,
European Data Protection Supervisor

La 25 mai 2018 se pune în aplicare Regulamentul General privind Protecția Datelor, cunoscut sub acronimul GDPR, legislație introdusă la nivelul Uniunii Europene cu scopul principal de uniformizare a normelor de protecție a datelor din statele membre, precum și pentru îmbunătățirea confidențialității și protecția drepturilor persoanelor vizate de prelucrarea acestor date. Este pe bună dreptate considerat un moment de referință privind protecția și confidențialitatea datelor cu caracter personal.

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

Trebuie să spunem că deși intrarea sa în vigoare, în anul 2016, a permis operatorilor și autorităților 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 puțin sau deloc pregătite. Este de discutat dacă aceasta s-a datorat nepăsării și lipsei de interes a operatorilor după ani de aplicare a reglementărilor existente, respectiv Legea

¹ Lector asociat/CS III la Universitatea Politehnica din București, Secretar general de redacție Revista Română pentru Protecția și Securitatea Datelor cu Caracter Personal.

nr. 677/2001, lipsei de înțelegere a noilor reglementări europene ori deficiențelor 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 desemnați să facă acest lucru, fie că vorbim de persoane fizice, fie de anumite firme de consultanță. Chiar și pentru aceia care au avut în atenție preocuparea de a fi pregătiți pentru implementarea cerințelor GDPR înainte de luna mai 2018 și, într-adevăr, companii importante au angajat persoane sau firme specializate pe acest segment juridic, au existat situații în care suportul a fost lipsit de substanță ori nu s-a înțeles pentru că nu a fost adecvat specificului situației lor.

Dacă ne orientăm analiza către amenzi aplicate de autoritățile se supraveghere din statele membre, inclusiv Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), în primul an vom constata că acestea au fost puține (9) și 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 așteptam la altceva, mai ales că investigarea, de exemplu, a unei încălcări a securității datelor necesită timp pentru a putea aprecia și sancționa 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 Protecția Datelor, ANSPDCP menționa pe site: *„Dacă anul 2018 a fost marcat de adoptarea legislației naționale aplicabile (Legea nr. 129/2018, Legea nr. 190/2018), inclusiv a deciziilor normative ale Autorității, putem afirma că, începând cu anul 2019, s-a dat efectivitate deplină monitorizării implementării corecte a noului Regulament și a reglementărilor naționale aferente, la nivelul operatorilor din sectorul public și privat. Afluxul plângerilor și al solicitărilor de puncte de vedere primite în acești doi ani au constituit un important indicator pentru instituția noastră cu privire la existența unei creșteri reale a nivelului de conștientizare a publicului larg referitor la drepturile de care beneficiază, precum și a interesului semnificativ al operatorilor în respectarea noilor reguli europene”.*

O abordare vizibil mai fermă a autorităților am constatat-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 și telecomunicații, hoteluri sau operatori aerieni.

Semnalul privind încheierea perioadei de așteptare pentru îndeplinirea cerințelor de conformitate cu prevederile Regulamentului a fost dat brusc, în ianuarie 2019, de către autoritatea de supraveghere din Franța, Commission nationale de l'informatique et des libertés (CNIL), care după 5 luni de investigație a aplicat gigantului Google o amendă record de 50 milioane de euro pentru încălcarea regulilor de transparență, a informării insuficiente a persoanelor vizate și, nu în ultimul rând, a lipsei unui consimțământ valabil exprimat de către persoanele vizate pentru personalizarea publicității 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 sancționat Marriott International Inc. cu 99 milioane sterline (110.390.200 euro) și 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 îmbunătățire a securității și confidențialității, de apărare a drepturilor și libertăților persoanelor vizate, prin protecția 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 garanțiilor 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 amenziilor prevăzute 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 autorităților de supraveghere, deși nu pare cea mai mare problemă, totuși, notificarea excesivă a situațiilor ipotetic considerate incidente de securitate a condus la supraîncărcarea activității acestora și, prin urmare, la afectarea unor investigații importante. Această situație a fost generată într-o mare măsură de excesul de a nu greși al operatorilor, speriați de potențialul unei sancțiuni contravenționale mari pentru nerespectarea obligației de notificare prevăzută la art. 33 din GDPR. Pe de altă parte, această situație 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 situațiilor care obligă la notificarea autorităților de supraveghere competente. Potrivit raportului Asociației Internaționale a Profesioniștilor în Confidențialitate (IAPP) numai în anul 2018 s-au transmis peste 64.000 de notificări către autoritățile naționale de supraveghere; cu toate acestea doar în 240 cazuri au fost aplicate amenzi.

Pe de altă parte, din analiza sancțiunilor aplicate în perioada 2018-2020 s-a putut constata o oarecare incoerență a acțiunilor diferitelor autorități din statele membre. Dacă unele autorități și-au concentrat activitatea pe două-trei investigații mari, cum este cazul Marii Britanii sau Franței, 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 și transparență în activitățile publice ale acestora, de unde se poate deduce că este nevoie de o mai bună armonizare și o mai strânsă cooperare între aceste autorități.

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, lanțurile de aprovizionare, organizarea evenimentelor și călătoriile sunt deja afectate și există un impact semnificativ asupra cetățenilor și funcționării tuturor organizațiilor. Situația rămâne imprevizibilă, iar organizațiile sunt în situația de a acționa prompt pentru a schimba rapid abordarea cu privire la toate circumstanțe, inclusiv aspectele referitoare la prelucrarea și protecția 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 situației actuale. Domenii până mai ieri considerate incompatibile cu accesul de la distanță, precum învățământul, serviciile publice sau cele de sănătate au fost forțate la transferul on-line.

Creșterea bruscă, fără precedent, a numărului persoanelor angajate care lucrează de acasă reprezintă pe lângă preocupările legate de securitate cibernetică, provocări suplimentare pentru organizații în ceea ce privește protecția datelor. Deoarece o mare parte a organizațiilor nu obișnuiau să lucreze în regim de telemuncă, neavând organizată infrastructura, proceduri ori mecanisme interne pentru a permite un acces securizat și facil la sisteme, baze de date și aplicații, acestea au fost nevoite să se adapteze din mers la noua filozofie, asumându-și de cele mai multe ori riscuri care includ inherent încălcarea confidențialității, integrității sau disponibilității datelor cu caracter personal prelucrate. Lucrurile au fost accelerate iar instituții ale statului au fost nevoite să facă eforturi pentru a oferi acces on-line la servicii, altfel amorțite în prea multă birocrație.

Totodată, necesitatea distanțării sociale a obligat cetățenii să devină mai confortabili cu interacțiunea virtuală, mai toleranți și deschiși la conceptul de partajare a propriilor date personale.

Ceea ce nu trebuie să uităm însă este că dependența de mediul digital și conviețuirea 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* își găsesc adevăratul sens și trebuie să fie obligatoriu parte a noilor strategii dezvoltate de organizații pentru abordarea operațiunilor de prelucrare a datelor personale.

În final, putem aprecia că dată fiind complexitatea și 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 puțin aparent, atât operatorii cât și autoritățile de supraveghere sunt mai degrabă încă în situația de a se obișnui cu exigențele Regulamentului, iar aceasta contribuie la îmbunătățirea treptată a practicilor în domeniul protecției datelor, cu efect direct în reducerea incidentelor care ar putea afecta drepturile și libertățile persoanelor ale căror date sunt prelucrate.

Cel mai mare câștig, la finalul celor doi ani de aplicare a GDPR, este acela al creșterii gradului de conștientizare a problemelor de confidențialitate a publicului larg și cunoașterii drepturilor pe care persoanele vizate de prelucrări le au, esențial pentru o societate din ce în ce mai digitalizată în care amenințările generate de utilizarea ilegală și criminalitatea informatică reprezintă o realitate.

Care va fi evoluția viitoare a reglementărilor?

Schimbările pe care pandemia COVID-19 le-a produs în societate, și în particular în peisajul prelucrării datelor cu caracter personal, reprezintă o oportunitate pentru ca inovația și tehnologia să stimuleze elaborarea unor mecanisme adecvate de creștere a responsabilității și a gradului de conștientizare astfel încât să permită asigurarea protecției drepturilor fundamentale ale cetățenilor.

studii și cercetări

Libertatea de exprimare și protecția datelor cu caracter medical în timpul stării de urgență 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 PLOEȘTEANU¹

□ Rezumat

În perioada pandemiei, o serie de drepturi și libertăți au fost restrânse și supuse unui test de eficiență datorită necesității de a se combate transmiterea virusului și de a fi luate măsuri adecvate pentru gestionarea în ansamblu a comunităților. Fiecare stat a avut propriul său mod de abordare, care a variat la rândul său în funcție de perioadă, de circumstanțele naționale și regionale și de modul de reacție a populației la diferitele măsuri. Printre drepturile cele mai încercate s-au numărat dreptul la liberă circulație, dreptul la ocrotirea sănătății, dreptul la viață privată sau chiar libera exprimare. Studiul își propune să ofere perspective juridice asupra situației în care unele liste cu date cu caracter personal ale celor infectați sau suspecți de infectare au fost divulgate în mod nelegal către public, după care au fost retransmise pe rețele de socializare sau chiar în mass media instituționalizată.

Cuvinte-cheie: Regulamentul General privind Protecția 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 pandemic or the diverse reactions of the people of a specific community. Among the most tried rights were the right to free

¹ Nicolae Ploșteanu este doctor conferențiar în cadrul Universității de Medicină, Farmacie, Științe și Tehnologie „George Emil Palade” din Târgu Mureș, fiind director Centrului de Studii pentru Protecția 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 zile² de angajare a întregii societăți și a întregului aparat de stat în lupta împotriva Covid-19, fiecare corp profesional (inclusiv juriștii, fie ei procurori, judecători, notari, agenți de aplicare a legii, executori, avocați etc.) se confruntă cu numeroase provocări, iar una dintre acestea privește cu certitudine **Libertatea de exprimare**, prin simpla comunicare, prin presa scrisă sau on-line. Adesea au apărut mesaje oficiale adresate de instituții abilitate³, mesaje prin care se anunța 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 suspecti, pot să fie supuși unor sancțiuni, cum ar fi închisoarea sau amenda. În general, asemenea mesaje au pornit de la premisa reală că respectivele informații ar avea fie caracter de secret de serviciu, fie că nu sunt destinate publicității.

Câteva opinii juridice asupra ipotezei aflate în studiu!

2. În această situație de excepție, întrebarea firească este Dacă nu avem dreptul să cunoaștem informații 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 populația are un drept fundamental, prevăzut de art. 31 al Constituției României, anume **dreptul la informație**. Acest articol⁴ 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 Constituția României, dreptul la informație:

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

(2) Autoritățile publice, potrivit competențelor ce le revin, sunt obligate să asigure informarea corectă a cetățenilor asupra treburilor publice și asupra problemelor de interes personal.

(3) Dreptul la informație nu trebuie să prejudicieze măsurile de protecție a tinerilor sau securitatea națională.

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

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

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

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

Nu răspunsul la aceste întrebări este dificil, ci identificarea unei soluții legale asupra situației privită în ansamblul său, deoarece apare cu evidență că asemenea date sunt de interes public⁵, cel puțin identitatea persoanelor și localizarea lor, din multe puncte de vedere: unii nu mai știu de rudele lor și doresc să afle pe orice cale dacă se numără printre cei supuși unei intervenții de acest tip (internare, izolare, carantină etc.); alții doresc să cunoască dacă într-o anumită zonă există un risc mai mare sau mai mic, în funcție de anunțurile făcute. Este foarte adevărat că în anumite situații nu este necesară identificarea persoanei în mod direct, dar precizarea domiciliului poate conduce la identificarea sa. În fine, astfel cum opinam soluția informării este cea delicată și asupra căreia trebuie să se lucreze.

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

Trebuie spus, că în mod obișnuit, datele referitoare la starea medicală a unei persoane intră în categoria datelor sensibile și, de principiu, nu sunt destinate publicității, fiind vorba de protecția vieții private a persoanei despre a cărei sănătate este vorba. Din acest motiv, relația de confidențialitate dintre medic și pacient este supusă unor garanții, precum secretul profesional. Ca urmare, de principiu, asemenea date, precum cele din ipoteza supusă analizei nu se vor divulga și vor angaja răspunderea juridică a celor care sunt supuși obligației de secret profesional.

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

⁵ La articolul 2 lit. b) din Legea nr. 544/2001 privind liberul acces la informațiile de interes public se definește informația de interes public astfel: „orice informație care privește activitățile sau rezultă din activitățile unei autorități publice sau instituții publice, indiferent de suportul ori de forma sau de modul de exprimare a informației”.

⁶ Spre exemplu, articolul 12 alin. (1) lit. a) din Legea nr. 544/2001, exceptează de la accesul liber al cetățenilor informațiile din domeniul apărării naționale, siguranței și ordinii publice, dacă fac parte din categoriile informațiilor clasificate, potrivit legii, astfel că accesul la aceste informații va fi permis cetățeanului doar în urma unei intervenții a instanței de judecată, în condițiile articolului 21 și urm. din aceeași lege.

către cel care ia cunoștință de acestea, se pedepsește cu închisoare de la o lună la un an sau cu amendă”. Oricum, această situație va genera cel mai probabil în viitor cauze celebre, deoarece trebuie să se lămurească ce înseamnă în acest context „divulgare”, din moment ce situația este deja publică și, totodată, trebuie să se lămurească măsura în care o persoană care ia la cunoștință în afara atribuțiilor de serviciu, de pe o rețea de socializare, despre asemenea informații precum cele puse în discuție, putea să aibă la cunoștință că respectivele informații nu sunt destinate publicității 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 informații precum cele medicale, referitoare la starea de sănătate a unei persoane (chiar și în cazul unui suspect), reprezintă informații obținute în cadrul unei relații de confidențialitate și sunt supuse secretului profesional. Totuși, autoritățile trebuie să stabilească cu atenție nivelul de confidențialitate acordat acestor informații, pentru a nu aduce atingere altor modalități de a informa opinia publică în legătură cu aspecte de interes public, precum zona specifică „roșie”, potențialele riscuri etc. În plus, trebuie acordată o atenție aparte evaluării juridice a infracțiunii asociate divulgării, pentru a nu genera efecte sociale neoportune, inadecvate și disproporționate în raport de circumstanțele faptice propriu-zise.

4. O întrebare interesantă ar fi dacă în anumite circumstanțe se poate deroga de la obligația 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 și făcute anumite precizări.

Sub aspect general, intruziunea medicului în viața privată a pacientului, prin divulgarea datelor medicale ale acestuia, este interzisă, medicul având obligația respectării confidențialității. Totuși, există situații care impun într-o oarecare măsură divulgarea acestora, atât pentru protecția pacientului cât și a altor persoane, vorbind astfel de un scop legitim al divulgării.

Stabilirea întinderii acestei obligații de confidențialitate este destul de dificilă. Totuși, trebuie să ne raportăm la scopul și necesitatea divulgării. În jurisprudența din Statele Unite ale Americii, o cauză celebră, cauza Tarasoff⁷ (intrată ulterior în manualele de etică medicală și de drept din SUA și apoi din întreaga lume), a schimbat perspectiva abordării problematicei secretului profesional. În această cauză, în urma unor gelozii și ședințe de psihoterapie, numitul Poddar intenționa să o ucidă pe Tarasoff, anunțându-i medicului intențiile sale. Medicul a informat imediat poliția, transmitându-le că Poddar este periculos și ar trebui internat într-un spital psihiatric. Poliția l-a arestat și 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 Tatiane Tarasoff, a omorât-o cu un cuțit de bucătărie și apoi s-a predat poliției.

Părinții Tatiane au acuzat Universitatea Berkeley, psihoterapeutul și poliția, de incapacitatea de a preveni o astfel de crimă și, de asemenea, că nu i-au avertizat în legătură cu pericolul în care se afla fiica lor. Psihoterapeutul s-a apărat invocând obligația sa de păstrare a secretului profesional.

⁷ A se vedea N. Ploșteanu, C. Csiszar, *Prelucrarea de date medicale, exercitarea dreptului la liberă exprimare și protecția 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 violență 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 obligații de diligență va varia în mod necesar în funcție de circumstanțe, în fiecare caz caracterul adecvat al comportamentului terapeutului trebuie măsurat în raport cu standardul de neglijență tradițională a asigurării îngrijirii rezonabile în circumstanțele date”.

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

Situația pandemică din prezent nu este una obișnuită, astfel că obligația de confidențialitate trebuie supusă unui test. Însă, acest test este în primul rând în competența autorităților 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 și protecția vieții private a celor despre a căror date medicale este vorba, pe de altă parte, raportându-se la circumstanțe precum: capacitatea de intervenție a instituțiilor 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 și necesitățile de circulație, gradul de izolare din punct de vedere fizic și social al unei locuințe, calitatea de persoană publică, nivelul de panică, tipologia culturală a unei comunități etc. Urmare a unei asemenea evaluări se poate înlătura obligația de confidențialitate sau i se poate redefini limitele, mai largi sau dimpotrivă mai restrânse. Oricum aceste chestiuni în situații de criză, precum cea de față, se găsesc în primul rând în apanajul autorităților publice. Este însă semnificativ în acest cadru, faptul că testul final trebuie realizat de o instanță de judecată⁸, 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 funcționa un astfel de mecanism și dacă el funcționează identic în toate cazurile?

Trebuie spus că există o legislație specifică în domeniul protecției datelor personale. În special este vorba despre Regulamentul General privind Protecția Datelor (GDPR), act legislativ european care are prioritate⁹ asupra altor acte normative naționale, potrivit art. 148 din Constituția României. GDPR interzice divulgarea datelor cu caracter medical, stabilind câteva excepții de la această interdicție. Însă GDPR

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

⁹ A se vedea și N. Ploșteanu, 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.

stabilește obligații pentru operatorii de date și în anumite condiții. Postările pe rețelele de socializare sau transmiterea prin mass media a datelor medicale va angaja răspunderea atât a celor care postează, publică etc., cât și a rețelelor de socializare, gradul de răspundere variind după numeroși indicatori, până la exonerare de răspundere, în anumite situații: numărul de date divulgate, intenția frauduloasă, numărul de receptori, măsurile imediat luate după luarea la cunoștință în privința nerespectării legii, contextul divulgării, aparenta legitimitate etc. Subiectul poate fi extrem de mult dezbătut! Mai mult, în contextul actual, situația juridică este complicată de starea de urgență, deoarece atrage aplicabilitatea nu doar a GDPR ci și a legii de transpunere a Directivei europene nr. 680/2016, care permite un regim mai restrictiv, este adevărat că opozabil în special autorităților de aplicare a legii, privind prelucrările de date cu caracter personal.

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

6. Există totuși o „porțiță legislativă” atunci când avem în vedere dezvoltarea datelor cu caracter medical de către mass media sau alte alternative?

Pentru a răspunde la această întrebare trebuie să se țină cont de regimul libertății de exprimare prin presă (în scopuri jurnalistice) stabilit de GDPR și care este regimul stabilit presei prin actele normative specifice stării de urgență.

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

Art. 85 cuprinde 3 alineate și constituie *inter se* o excepție de la regimul juridic general al GDPR aplicabil în domeniul protecției datelor, aspect care reiese din însăși interpretarea tehnico-legislativă a GDPR și din conținutul articolului: raportul dintre drepturile amintite este tratat distinct într-un articol, spre deosebire de multe alte domenii pentru care nu sunt realizate referințe speciale și 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 protecției datelor, ori de câte ori este necesar să se atingă obiectivul justului echilibru. În considerentul 153 al RGPD se evidențiază o regulă de interpretare necesară identificării sferei de aplicabilitate *rationae materiae* a acestui articol, anume că „Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi *jurnalismul*, să fie interpretate în sens larg”.

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