

# Tipologia protecției datelor cu caracter personal în situații de criză medicală: coronavirus COVID-19

Prof. univ. dr. **Daniel-Mihail ȘANDRU**<sup>[1]</sup>

*Motto:*

Și brusc trecutu-mi pare viitor  
și urc spre secole latine  
și-aud un ding, un dang sonor  
al frunzelor foșnind prin mine.  
Aerul, Nichita Stănescu

## ABSTRACT

Data protection (Art. 8), the right to life (Art. 2), the right to privacy (Art. 8) and the protection of health (Art. 35) are fundamental rights protected by the Charter of Fundamental Rights of the European Union (CDFUE) as well, and by similar or even identical provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). The General Data Protection Regulation (GDPR) primarily protects personal data, emphasizing that this right is not absolute (recital 4). On a case-by-case basis, the context of applying special rules regarding personal data of has to be assessed. Data protection in medical crisis situations involves several research directions and typologies in application. First of all, the situation of humanitarian and medical crisis and the restriction of the rights of natural persons, respectively the legislative reaction of the states and organizations, must be taken into account. A critical approach on the „unity in diversity” of the reaction of the member states of the European Union and the European Committee for Data Protection is needed. Secondly, the rights of data subjects as patients or subjects likely to be patients, infected or suspected to be carrying the new SARS-CoV-2 virus (severe acute respiratory syndrome coronavirus 2) must be taken into consideration that triggers COVID-19 disease. Third, the article discusses

<sup>[1]</sup> Daniel-Mihail Șandru este cercetător științific gradul I, a fondat și coordonează Centrul de Studii de Drept European al Institutului de Cercetări Juridice „Acad. Andrei Rădulescu” al Academiei Române, este profesor universitar la Universitatea Creștină Dimitrie Cantemir și Universitatea din București. Judecător ad hoc la Curtea Europeană a Drepturilor Omului și arbitru la Curtea de Arbitraj Comercial Internațional de pe lângă Camera de Comerț și Industrie a României. Președinte al Societății de Științe Juridice (SSJ) și al Asociației Române de Drept și Afaceri Europene (ARDAE). Poate fi contactat la adresa [contact@mihaisandru.ro](mailto:contact@mihaisandru.ro) Pagina web: [www.mihaisandru.ro](http://www.mihaisandru.ro) Materialul face parte din volumul „Protecția datelor în România. Conformare și sancțiuni GDPR” în curs de publicare la Editura Universitară și a fost pregătit pentru Conferința internațională „Challenges of Doing Business in the Global Economy” (CBGE 2020), ed. a VIII-a, organizată de Facultatea de Administrarea Afacerilor Internaționale – Universitatea Creștină Dimitrie Cantemir. La data de 15 aprilie 2020 au fost verificate sau/și accesate ultima dată trimerile web.

limiting the rights of individuals in exceptional situations and their application to data protection, including the right to information and the emergence of fake news. Fourth, the relationship between the employee and the employer is modified by establishing procedures for informing the employee, measures to protect him and his protection in relation to the clients, measures that lead to the protection of the other employees and the taking of other technical and organizational measures for data protection. The application of the principles, especially regarding the basis of processing, respectively art. 6 paragraph 1 letter d – „the processing is necessary to protect the vital interests of the data subject or of another natural person” is analyzed in this framework. Fifth, the article addresses data security and the risks associated with using home-based and telework. In conclusions, the need to develop a single guide by the European Data Protection Committee is underlined and references are made to all European Committee guidelines or guidelines or national supervisory authorities as the General Regulation provides few specific interpretation resources. These guidelines are necessary both for the establishment of the operators' actions and for the avoidance of sanctions, the author analyzing the sanctions that refer to the COVID-19 phenomenon or that could involve situations of medical crisis.

**Keywords:** *data protection, health protection, COVID19, rights of the data subject, obligations controller, medical crisis.*

## REZUMAT

---

Protecția datelor (art. 8), dreptul la viață (art. 2), dreptul la viață privată (art. 8) și protecția sănătății (art. 35) sunt drepturi fundamentale protejate deopotrivă în Carta drepturilor fundamentale a Uniunii Europene (CDFUE) precum și în dispoziții asemănătoare ori chiar identice din Convenția pentru apărarea Drepturilor Omului și a Libertăților Fundamentale (CEDO). Regulamentul general privind protecția datelor (RGPD) protejează în primul rând datele cu caracter personal, dar subliniază că acest drept nu este absolut (consid. 4). De la caz la caz va trebui să se aibă în vedere contextul aplicării normelor speciale referitoare la datele personale ale persoanelor vizate. Protecția datelor în situații de criză medicală are în vedere mai multe direcții de cercetare și tipologii în aplicare. În primul rând, trebuie avute în vedere situația de criză umanitară și medicală și restrângerea drepturilor persoanelor fizice, respectiv reacția legislativă a statelor și organizațiilor. Este necesară o abordare critică privind „unitatea în diversitate” a reacției statelor membre ale Uniunii Europene și a Comitetului European pentru Protecția Datelor. În al doilea rând, trebuie să fie avute în vedere drepturile persoanelor vizate în calitatea acestora de pacienți sau de subiecte susceptibile de a fi pacienți, infectate sau suspecte de a fi purtării noului virus SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2 – sindrom sever respirator acut coronavirus 2) care declanșează boala COVID-19. În al treilea rând, articolul discută despre limitarea

drepturilor persoanelor fizice în situații excepționale și aplicarea acestora protecției datelor, inclusiv dreptul la informare și apariția fake news. În al patrulea rând, relația dintre angajat și angajator se modifică prin instituirea unor proceduri de informare a angajatului, măsuri de protecție a acestuia și de protecția acestuia în raport cu clienții, măsuri care să conducă la protecția celorlalți angajați și luarea altor măsuri tehnice și organizatorice de protecție a datelor. Aplicarea principiilor, în special în ceea ce privește temeiul prelucrării, respectiv art. 6 alin. (1) lit. d) – „prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice” este analizată în acest cadru. În al cincilea rând, articolul are în vedere securitatea datelor și riscurile asociate utilizării muncii la domiciliu și a telemuncii. În concluzii, se subliniază necesitatea elaborării unui ghid unic de către Comitetul european de protecția datelor și se fac trimiteri la lista tuturor ghidurilor și orientărilor Comitetului european ori ale autorităților naționale de supraveghere întrucât Regulamentul general oferă puține resurse specifice de interpretare. Aceste orientări sunt necesare atât pentru întemeierea acțiunilor operatorilor dar și pentru evitarea sancțiunilor, autorul analizând sancțiunile care se referă la fenomenul COVID-19 sau care ar putea implica situații de criză medicală.

**Cuvinte-cheie:** *protecția datelor, protecția sănătății, COVID-19, drepturile persoanei vizate, obligațiile operatorului, criza medicală.*

#### Legislație relevantă:

Carta Drepturilor Fundamentale a Uniunii Europene, art. 2, art. 7, art. 8, art. 35, art. 51, art. 52; Regulamentul UE 679/2016, art. 5, art. 6, art. 21, art. 30, art. 35

## I. Introducere

Sistemul de Clasificare Internațională a Bolilor (International Classification of Diseases – ICD) s-a modificat în 2020 prin introducerea unei noi boli: COVID-2019<sup>[2]</sup>. De la apariția acestei boli, la sfârșitul anului 2019 și până în 11 martie 2020 când a fost declarată pandemia la nivel mondial<sup>[3]</sup>, transmiterea coronavirusului a evoluat fulgerător. În prezent datele au căpătat o amploare și mai mare<sup>[4]</sup>. Fiecare stat și-a luat propriile măsuri și a elaborat propriile strategii în legătură cu combaterea efectelor contagiunii. Pe 13 martie 2020 Comisia Europeană a avut în vedere un prim răspuns și o strategie sub denumirea de „răspuns coordonat”<sup>[5]</sup> care a avut în vedere declanșarea

<sup>[2]</sup> Organizația Mondială a Sănătății, *Coronavirus disease (COVID-19) outbreak*, disponibil la adresa <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>

<sup>[3]</sup> WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020, disponibil la adresa <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19--11-march-2020>

<sup>[4]</sup> Pentru situația la zi a se vedea site-ul Organizației Mondiale a Sănătății: <https://www.who.int/emergencies/diseases/novel-coronavirus-2019>

<sup>[5]</sup> Comisia Europeană, *Răspunsul coordonat la nivel european cu privire la coronavirus: Întrebări și răspunsuri*, 13 martie 2020, Bruxelles disponibil la adresa [https://ec.europa.eu/commission/presscorner/detail/ro/qanda\\_20\\_458](https://ec.europa.eu/commission/presscorner/detail/ro/qanda_20_458)

unei proceduri comune accelerate de achiziții publice, împreună cu 26 de state membre, orientări privind culoarele verzi sau repatrierea cetățenilor europeni.

Libera circulație a persoanelor, libertatea religiei, nediscriminarea, libera circulație a mărfurilor, libertatea de exprimare și de informare, libertatea de întrunire și de asociere, dreptul la educație, libertatea de a desfășura o activitate comercială, protecția sănătății – sunt drepturi afectate de noul coronavirus<sup>[6]</sup>. În acest articol particularizăm efectele pandemiei, ale restricțiilor autorităților și ale desfășurării activităților, în privința dreptului la protecția datelor.

Declarația comună a membrilor Consiliului European din 26 martie 2020 a menționat cinci direcții de acțiune: (1) limitarea răspândirii virusului, acțiuni fundamentate pe orientările Centrului European de Prevenire și Control al Bolilor (ECDC), precum și pe recomandările Grupului consultativ privind Covid-19 din cadrul Comisiei și monitorizarea în continuare a evoluțiilor prin intermediul mecanismului integrat al UE pentru un răspuns politic la crize (IPCR), (2) furnizarea de echipament medical, potrivit căreia Comisia „va majora, după caz, bugetul inițial pentru rezerva strategică rescEU de echipamente medicale, inclusiv pentru terapie intensivă, precum și de vaccinuri și tratamente”, (3) promovarea cercetării, care se reflectă atât în finanțare cât și în colaborarea cu partenerii din G7 și G20, precum și inițiativele Comisiei Europene, ale Consiliului European pentru Inovare și ale Grupului Băncii Europene de Investiții (BEI) de a acorda sprijin financiar acțiunilor din domeniul sănătății publice, (4) combaterea consecințelor socioeconomice prin acțiunile Băncii Centrale Europene, ale Eurogrupului și ale Băncii Europene de Investiții și (5) situația cetățenilor blocați în țări terțe „cu sprijinul activ al Înaltului Reprezentant și al Comisiei. Comisia va transmite un addendum la Orientările privind gestionarea frontierelor pentru a facilita măsurile de tranzit pentru cetățenii UE repatriați.”<sup>[7]</sup>

În domeniul ajutoarelor de stat Comisia a realizat mai multe comunicări cu forță juridică,<sup>[8]</sup> indicând și scopul acestora: „aplicarea clar direcționată și proporțională a controlului UE privind ajutoarele de stat are rolul de a asigura eficacitatea măsurilor naționale de sprijin în ajutarea întreprinderilor afectate în cursul epidemiei de COVID-19, dar și să le permită acestor întreprinderi să se redreseze odată ce situația actuală este depășită, ținând seama de importanța realizării dublei tranziții verzi și digitale în conformitate cu obiectivele UE.”<sup>[9]</sup> În ceea ce privește cercetarea și dezvoltarea sunt considerate costuri eligibile inclusiv cele ce se referă la „instrumentele de colectare și prelucrare a datelor”.

<sup>[6]</sup> Pentru o reflecție privind impactul coronavirus în domeniul juridic: M. Duțu, *Dreptul și Justiția în zodia coronavirusului COVID-19*, Juridice.ro, 17 aprilie 2020 disponibil la adresa <https://www.juridice.ro/essentials/3658/dreptul-si-justitia-in-zodia-coronavirusului-covid-19>. „O situație care s-a extins cu rapiditate, odată cu pandemia, în ultimele luni la nivelul întregii planete, mai în toate statele indiferent de sistemul de drept și de justiție, în numele „interesului public general”, pentru evitarea „riscului de sănătate publică” și ca „măsuri urgente cu caracter excepțional”. Pentru sistemul juridic și cel de justiție o atare evoluție se manifestă în două sensuri principale: pe de o parte, emergența și propagarea fulgurantă a unui drept de excepție, chemat să răspundă unor aspecte noi, care marchează transversal marea majoritate a sectoarelor de activitate economico-socială și reglementare juridică, iar, pe de alta, paralizia, aproape totală, a funcționării autorității judiciare, deopotrivă, în privința activității de înfăptuire, precum și de administrare a justiției.”

<sup>[7]</sup> *Declarația comună a membrilor Consiliului European*, 26 martie 2020 disponibilă la adresa <https://www.consilium.europa.eu/ro/press/press-releases/2020/03/26/joint-statement-of-the-members-of-the-european-council-26-march-2020/>

<sup>[8]</sup> Comisia Europeană, Comunicarea „Cadru temporar pentru măsuri de ajutor de stat de sprijinire a economiei în contextul actualei epidemii de COVID-19”, C(2020)1863, JO C 0911, 20 martie 2020, p. 1.

<sup>[9]</sup> Comisia Europeană, *Comunicare a Comisiei Modificare a Cadrelor temporare pentru măsuri de ajutor de stat de sprijinire a economiei în contextul actualei epidemii de COVID-19*, Bruxelles, 3.4.2020 C(2020) 2215 final.

## II. Drept internațional, crize medicale, crize umanitare, restrângerea drepturilor

Din perspectiva dreptului internațional<sup>[10]</sup> și a dreptului european, fie din dreptul Uniunii Europene, prin Declarația Comitetului European pentru Protecția Datelor (CEPD)<sup>[11]</sup> fie norme ale Consiliului Europei<sup>[12]</sup>, sintetic se poate evidenția o activitate mai degrabă de observare și de coordonare generală decât una implicată, cu reguli profunde. Aceasta și pentru că Uniunea Europeană are competențe limitate în domeniul sănătății. De altfel, toate entitățile de supraveghere a prelucrării datelor, atât cele de la nivel european cât și autoritățile naționale au fost afectate în privința activităților curente. Dintre preocupările la nivel european cea mai importantă este aceea a prelucrării *localizării persoanelor vizate* în scopul evitării transmiterii coronavirusului.

În Uniunea Europeană, Regulamentul general privind protecția datelor<sup>[13]</sup> este aplicabil. Regulamentul nu este nici suspendat și nici anulat de vreo altă legislație, națională sau europeană<sup>[14]</sup>. Sunt două acțiuni importante luate până în acest moment, în afara unora particulare, în diferite state membre: a) acțiunea Uniunii Europene privind schimbul de metadate anonimizate cu scopul de a modela și anticipa propagarea virusului și b) proiectul de soft pentru telefoane promovat de Apple și Google.

Comisarul pentru piața internă împreună cu directorii executivi ai companiilor europene de telecomunicații și ai GSMA – asociația operatorilor de telecomunicații mobile –, au discutat despre „reziliența rețelei și despre schimbul de metadate anonimizate cu scopul de a modela și

[10] Armin von Bogdandy, Pedro A. Villarreal, *International Law on pandemic response: a first stocktaking in light of the Coronavirus crisis*, Max Planck Institute for Comparative Public Law and International Law, Research Paper no. 2020-07, Heidelberg, 26 martie 2020. A.M. Șandru, D.-M. Șandru, *Dreptul umanitar și protecția datelor personale*, în *Pandectele române* nr. 6/2018, p. 58-66. D. Giri, *Responsibility of China for the Spread of Covid-19: Can China Be Asked to Make Reparations?*, JURIST – Student Commentary, 10 aprilie 2020, <https://www.jurist.org/commentary/2020/04/devashshish-giri-china-covid19-reparations/>

[11] Comitetul European pentru Protecția Datelor, *Declarație privind prelucrarea datelor cu caracter personal în contextul pandemiei COVID-19*, adoptată la 19 martie 2020 disponibilă aici <https://www.dataprotection.ro/servlet/ViewDocument?id=1859> sau [https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en)

A se vedea: N.-J. Brehon, *The European Union and the Coronavirus*, European Issue, no. 553, 6 aprilie 2020, disponibil la adresa <https://www.robert-schuman.eu/en/european-issues/0553-the-european-union-and-the-coronavirus>; Raportul Agenției pentru Drepturi Fundamentale, *Fundamental rights implications of COVID-19*, disponibil atât la nivelul UE cât și pentru statele membre la adresa <https://fra.europa.eu/en/themes/covid-19>

[12] A se vedea: *Respecting democracy rule of law and human rights in the framework of the COVID-19 sanitary crisis. Toolkit for member states*, SG Inf(2020)11, 7 aprilie 2020 disponibil la adresa <https://www.coe.int/en/web/belgrade/-/coronavirus-guidance-to-governments-on-respecting-human-rights-democracy-and-the-rule-of-law> Pe larg: A.M. Șandru, D.-M. Șandru, *Reforma protecției datelor din perspectiva Consiliului Europei*, în *Studii și cercetări juridice* nr. 3/2019, p. 311-325.

[13] Regulamentul (UE) nr. 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 nr. 95/46/CE (Regulamentul general privind protecția datelor) a fost publicat în Jurnalul Oficial L 119, 4 mai 2016, p. 1-88. I. Alexe, C.M. Banu, *De la directivă la regulament în reglementarea, la nivelul Uniunii Europene, a protecției datelor cu caracter personal*, în vol. I. Alexe, N.-D. Ploșteanu, D.-M. Șandru (coordonatori), *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești și noile provocări ale Regulamentului (UE) 2016/679*, Ed. Universitară, 2017, p. 14 și urm.

[14] I. Alexe, C.-M. Banu, *op. cit.*, pp. 14-40.

anticipa propagarea virusului.”<sup>[15]</sup> Probabil aceasta va face obiectul unor cercetări viitoare, fiind desigur unul dintre aspectele care vor pune probleme pe termen lung, bineînțeles în măsura în care viața privată a cetățenilor va fi afectată de deciziile privind localizarea. Până în acest moment, geolocalizarea este considerată o soluție, dar sunt și opinii potrivit cărora nu trebuie înlăturate dispozițiile de protecție din RGPD<sup>[16]</sup>.

„Sistemul de alertă precoce și de reacție” (SAPR) instituit prin Decizia nr. 1083/2013<sup>[17]</sup> are în vedere un sistem de protecție a datelor cu caracter personal, atât în privința unui circuit securizat al acestora cât și al mijloacelor de comunicare. Recomandarea Comisiei Europene din 8 aprilie 2020<sup>[18]</sup> „stabilește un proces în vederea adoptării împreună cu statele membre a unui set de instrumente, axat pe două dimensiuni: [a]) o abordare paneuropeană coordonată privind utilizarea aplicațiilor mobile pentru a permite cetățenilor să ia măsuri eficace și mai specifice de distanțare socială, precum și pentru avertizare, prevenire și localizare a contactilor și [b]) o abordare comună pentru modelarea și anticiparea evoluției virusului prin date anonimizate și agregate privind localizarea mobilă.” Se au în vedere următoarele aspecte tehnice și juridice care să asigure scopul unei asemenea prelucrări:

- specificații pentru asigurarea eficacității aplicațiilor mobile de informare, avertizare și localizare din punct de vedere medical și tehnic;
- măsuri de evitare a proliferării aplicațiilor incompatibile, de sprijinire a cerințelor de interoperabilitate și de promovare a soluțiilor comune;
- mecanisme de guvernare care trebuie aplicate de autoritățile din domeniul sănătății publice și cooperarea cu Centrul European de Prevenire și Control al Bolilor;
- identificarea bunelor practici și a mecanismelor pentru schimbul de informații cu privire la funcționarea aplicațiilor și
- schimbul de date cu organismele publice epidemiologice relevante, inclusiv transmiterea de date agregate către ECDC.

Pentru datele prelucrate prin intermediul SAPR se aplică Decizia (UE, Euratom) 2017/46 a Comisiei din 10 ianuarie 2017 privind securitatea sistemelor informatice și de comunicații în cadrul Comisiei Europene<sup>[19]</sup>.

În continuarea acestor documente și acte normative va trebui să avem în vedere interpretarea din Declarația privind prelucrarea datelor cu caracter personal în contextul pandemiei COVID-19,

<sup>[15]</sup> Comisia [europeană] colaborează cu operatorii telecom pentru a limita răspândirea COVID-19, [https://ec.europa.eu/romania/news/20200324\\_operatori\\_telecom\\_covid19\\_ro](https://ec.europa.eu/romania/news/20200324_operatori_telecom_covid19_ro)

<sup>[16]</sup> Autoritatea europeană pentru protecția datelor, prin publicarea unei scrisori a președintelui său a asigurat că se vor lua măsuri de anonimizare, securitatea datelor și accesul la acestea, precum și rolul responsabilului cu protecția datelor. A se vedea scrisoarea „*Monitoring spread of COVID-19*” către Roberto Viola, Director-General DG CNECT, Comisia Europeană, WRW/VC/mt/D(2020)0724 C2020-0337 disponibil [https://edps.europa.eu/sites/edp/files/publication/20-03-25\\_edps\\_comments\\_concerning\\_covid-19\\_monitoring\\_of\\_spread\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf), publicată pe site la 25.03.2020.

<sup>[17]</sup> Decizia nr. 1082/2013/UE a Parlamentului European și a Consiliului din 22 octombrie 2013 privind amenințările transfrontaliere grave pentru sănătate și de abrogare a Deciziei nr. 2119/98/CE (JO L 293, 5 noiembrie 2013, pp. 1-15)

<sup>[18]</sup> Recomandarea Comisiei privind un set de instrumente al Uniunii Europene pentru utilizarea tehnologiei și a datelor pentru a combate criza provocată de pandemia de COVID-19 și pentru a ieși din această criză Brussels, 8 aprilie 2020, C(2020) 2296 final, disponibilă la adresa [https://ec.europa.eu/info/sites/info/files/recommendation\\_on\\_apps\\_for\\_contact\\_tracing\\_4.pdf](https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf) a se vedea și Comunicatul „Comisia adoptă o recomandare de sprijinire a strategiilor de ieșire din criză prin intermediul datelor și al aplicațiilor mobile”, 8 aprilie 2020.

<sup>[19]</sup> JO L 6, 11.1.2017, p. 40-51.

adoptată la 19 martie 2020. În privința legalității prelucrării, CEPD nu recomandă utilizarea consimțământului, ceea ce este firesc: „RGPD reprezintă o legislație largă și prevede reguli care se aplică și prelucrării datelor cu caracter personal într-un context precum cel referitor la COVID-19. RGPD permite autorităților competente de *sănătate publică* și angajatorilor să prelucreze datele cu caracter personal în contextul unei epidemii, în conformitate cu legislația națională și în condițiile prevăzute de aceasta. De exemplu, atunci când prelucrarea este necesară din motive de interes public important în domeniul *sănătății publice*. În aceste condiții, nu este necesar să vă bazați pe consimțământul persoanelor.” După care se precizează că „în ceea ce privește prelucrarea datelor de telecomunicații, cum ar fi datele privind locația, trebuie respectate și legile naționale care pun în aplicare Directiva privind viața privată și comunicațiile electronice. În principiu, datele privind locația pot fi utilizate numai de operator atunci când sunt făcute anonime sau cu acordul persoanelor fizice. Cu toate acestea, art. 15 din Directiva privind viața privată și comunicațiile electronice permite statelor membre să introducă măsuri legislative pentru a proteja securitatea publică. O astfel de legislație excepțională este posibilă numai dacă constituie o măsură necesară, adecvată și proporțională în cadrul unei societăți democratice. Aceste măsuri trebuie să fie în conformitate cu Carta Drepturilor Fundamentale și Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale. Mai mult, aceasta este supusă controlului judiciar al Curții Europene de Justiție și al Curții Europene a Drepturilor Omului. În cazul unei situații de urgență, aceasta ar trebui, de asemenea, să fie strict limitată la durata de urgență.” Sunt două aspecte: Directiva privind viața privată și comunicațiile electronice ar fi trebuit să fi fost modificată de mult printr-un nou Regulament cu un astfel de obiect de reglementare, aflat doar în stadiu de proiect, și precizările Comitetului sunt în sensul utilizării geo-locației fără consimțământul persoanelor vizate cu instituirea unor măsuri de securitate specifice. Declarația nu soluționează distincțiile existente deja la nivelul jurisprudenței CJUE dintre „securitate publică” și „sănătate publică” („public security” și „public health”) fiind folosite mai degrabă ca sinonime<sup>[20]</sup>. Declarația se referă la obligațiile autorităților publice, respectiv „să prelucreze datele locației într-un mod anonim (adică prelucrarea datelor agregate într-un mod în care persoanele nu pot fi reidentificate), ceea ce ar putea permite generarea de rapoarte privind concentrarea dispozitivelor mobile într-o anumită locație („cartografie”).” Dar chiar și așa, „nu este posibilă doar prelucrarea datelor anonime, Directiva privind viața privată și comunicațiile electronice permite statelor membre să introducă măsuri legislative pentru salvagardarea *securității publice* (art. 15).” În fine, o ultimă precizare se referă la necesitatea aplicării principiului proporționalității. „Soluțiile cele mai puțin intruzive ar trebui să fie întotdeauna preferate, ținând cont de scopul specific care trebuie atins. Măsurile invazive, cum ar fi „urmărirea” persoanelor (adică prelucrarea datelor istorice despre locațiile ne-anonimizate) ar putea fi considerate proporționale în circumstanțe excepționale și în funcție de modalitățile concrete ale prelucrării. Cu toate acestea, ar trebui să se supună unui control și unor garanții îmbunătățite pentru a asigura respectarea principiilor de protecție a datelor (proporționalitatea măsurii în ceea ce privește durata și domeniul de aplicare, păstrarea datelor limitate și limitarea scopului).”

Pentru coloșii prelucrării datelor această prelucrare este o mană cerească<sup>[21]</sup> însă înainte de a trece la prelucrarea pe o scară largă a unor date sensibile ar trebui avute în vedere măsuri de protecție,

<sup>[20]</sup> A se vedea, de exemplu: cauzele C-331/16 și C-366/16, *K.*, hotărârea din 2 mai 2018, ECLI:EU:C:2018:296, pct. 42, 52.

<sup>[21]</sup> Comunicat Apple and Google partner on COVID-19 contact tracing technology, 10 aprilie 2020, <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>, precum și documente de detaliu privind mijloacele tehnice utilizate „Privacy-Preserving Contact Tracing”, disponibile la adresa <https://www.apple.com/covid19/contacttracing/>

având în vedere art. 25 din Regulament, referitor la asigurarea protecției datelor din momentul conceperii și în mod implicit, și art. 32, referitor la securitatea datelor<sup>[22]</sup>.

Una dintre probleme ridicate în mediul jurnalistic este aceea a menținerii unei supravegheri ridicate și după pandemie<sup>[23]</sup>. Dar aceasta este doar o speculație, peste câțiva ani se va observa cu certitudine care a fost „traectoria” localizării după molimă. Cu toate acestea, apreciem că măsurile excepționale care permit o astfel de supraveghere ar trebui să înceteze la momentul încetării situației excepționale care le-au generat.

### III. Drepturile persoanelor vizate în România. Studii de caz

Principalele acte adoptate în România, care afectează și drepturile persoanelor vizate, au fost Decretul nr. 195/2020 privind instituirea stării de urgență<sup>[24]</sup>, ordonanțele de urgență<sup>[25]</sup>, ordonanțele militare,<sup>[26]</sup> ordine ale ministrului sănătății legate strict de răspândirea COVID-19<sup>[27]</sup>, ordine ale comandatului acțiunii<sup>[28]</sup> precum și punctele de vedere<sup>[29]</sup> ori comunicate oficiale, unele cu rol interpretativ. O primă analiză a decretului și a ordonanțelor militare, precum și a actelor subsecvente<sup>[30]</sup> din perspectiva restrângerii drepturilor poate indica că nu există o mențiune expresă cu privire la suspendarea dreptului la protecția datelor cu caracter personal.

---

<sup>[22]</sup> Pentru studiul comparativ al diferitelor aplicații mobile (app), provenite de la firme mai puțin cunoscute, dar care prelucrează date pe scară largă: P. Sanderson, *FPF Charts the Role of Mobile Apps in Pandemic Response*, Future of Privacy Forum, 3 aprilie 2020, disponibil la adresa <https://fpf.org/2020/04/03/fpf-charts-the-role-of-mobile-apps-in-pandemic-response-chart/>

<sup>[23]</sup> A. Kharpal, *Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends*, CNBS, 26 martie 2020 <https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html>

<sup>[24]</sup> Decretul nr. 195/2020 privind instituirea stării de urgență pe teritoriul României, publicat în M. Of. nr. 212 din 16 martie 2020; Hotărârea Parlamentului României nr. 3/2020 pentru încuviințarea măsurii adoptate de Președintele României privind instituirea stării de urgență pe întreg teritoriul României.

<sup>[25]</sup> Ordonanța de urgență nr. 29/2020 privind unele măsuri economice și fiscal-bugetare, M. Of. nr. 230/2020; Ordonanța de urgență nr. 30/2020 pentru modificarea și completarea unor acte normative, precum și pentru stabilirea unor măsuri în domeniul protecției sociale în contextul situației epidemiologice determinate de răspândirea coronavirusului SARS-CoV-2, M. Of. nr. 231/2020.

<sup>[26]</sup> Ordonanța militară nr. 1 din 18 martie 2020 privind unele măsuri de primă urgență care privesc aglomerările de persoane și circulația transfrontalieră a unor bunuri, M. Of. nr. 219/2020; Ordonanța militară nr. 2 din 21 martie 2020 privind măsuri de prevenire a răspândirii COVID-19, M. Of. nr. 232/2020; Ordonanța militară nr. 3 a ministrului afacerilor interne privind măsuri de prevenire a răspândirii COVID-19, M. Of. nr. 242 din 24 martie 2020. Ordonanțe militare, acte legislative cu o natură constituțională imprecisă, de fapt neprevăzute în Constituție, dar indicate ca temei în Ordonanța de urgență nr. 1/1999 (art. 23 și urm.).

<sup>[27]</sup> Ordinul Ministerului Sănătății nr. 487/2020 privind aprobarea protocolului de tratament al infecției cu virusul SARS-Cov-2, M. Of. nr. 242 din 24 martie 2020.

<sup>[28]</sup> Ordinul Comandantului Acțiunii Secretar de stat, șef al Departamentului pentru Situații de Urgență nr. 74527 din 23 martie 2020 privind instituirea unor măsuri necesare pentru limitarea răspândirii infecției cu virusul SARS-COV-2 la nivelul unităților sanitare publice și private, cu modificările și completările aduse prin Ordinul Comandantului Acțiunii Secretar de stat, șef al Departamentului pentru Situații de Urgență nr. 74553 din 7 aprilie 2020, disponibil la [https://www.cnsctb.ro/index.php/legislatie\\_cov/1638-ordinul-comandantului-actiunii-74553-07-04-2020/file](https://www.cnsctb.ro/index.php/legislatie_cov/1638-ordinul-comandantului-actiunii-74553-07-04-2020/file)

<sup>[29]</sup> Cu titlu de exemplu, a se vedea Punctul de vedere privind aplicarea art. 1 din Ordinul Comandantului Acțiunii Secretar de stat, șef al Departamentului pentru Situații de Urgență nr. 74527 din 23 martie 2020, disponibil la [https://www.cnsctb.ro/index.php/legislatie\\_cov/1640-punct-de-vedere-art-1-ordin-comandant-actiune-nr-74527-din-23-03-2020/file](https://www.cnsctb.ro/index.php/legislatie_cov/1640-punct-de-vedere-art-1-ordin-comandant-actiune-nr-74527-din-23-03-2020/file)

<sup>[30]</sup> Hotărârea nr. 3 din 24 februarie 2020 a Grupului de suport tehnico-științific privind gestionarea bolilor înalt contagioase pe teritoriul României.



Pe de altă parte, România a formulat o cerere la Consiliul Europei în virtutea art. 15 din Convenția pentru apărarea Drepturilor Omului și a Libertăților fundamentale (CEDO), potrivit căruia în cazul în care a) există un pericol public care amenință viața națiunii, b) orice stat membru poate lua măsuri care derogă de la obligațiile prevăzute de Convenție, c) în măsura strictă în care situația o impune și d) cu condiția ca aceste măsuri să nu fie în contradicție cu alte obligații care decurg din dreptul internațional, având în vedere că e) nu se poate deroga de la art. 2, 3, 4 și 7 și cu obligația statului membru de a informa Secretarul General al Consiliului Europei de momentul încetării măsurilor. Această cerere de derogare trebuie văzută în contextul respectării principiilor CEDO, în special principiul proporționalității, și al jurisprudenței stabilite de Curte<sup>[31]</sup>.

### ***Prelucrarea și transmiterea datelor persoanelor implicate în situații medicale (izolate, în carantină, infestate, decedate)***

Autoritățile statului trebuie să respecte toate drepturile persoanelor vizate<sup>[32]</sup>, chiar dacă acestea au devenit subiect al infecției cu coronavirus SARS-CoV-2.

Interoperabilitatea din cadrul instituțiilor statului care desfășoară activități medicale sau de urgență privind persoane care au legătură cu virusul este neclară. Transmiterea datelor cu privire la aceste persoane este ilegală către operatori privați, care nu au legătură cu sistemul medical<sup>[33]</sup>.

Publicarea unor liste cu persoanele carantinate, izolate sau infectate, de către autoritățile administrației publice locale, pe rețele de socializare, fie pe site-ul primăriei, pe pagina de rețea socială a primăriei sau pe pagina primarului, ori a listei doctorilor infectați, publicată de un consilier local sau județean – toate constituind exemple din România, dar exemple negative întrucât nu există nicio proporționalitate în aceste măsuri, care nu ar putea fi justificate nici măcar de frica persoanelor care au trecut la asemenea divulgări de date cu caracter personal.

Fotografierea declarațiilor cu telefonul polițistului a fost o altă modalitate de încălcare a protecției datelor personale, care a încetat la aproape două săptămâni de la declararea stării de urgență, după ce aceste practici nelegale au fost sesizate de mai mulți actori implicați, iar autoritățile ierarhic-superioare ale polițiștilor au emis îndrumări pentru aplicarea corectă a normelor legale.

### ***Utilizarea platformelor on-line pentru cursuri universitare și școlare***

Utilizarea platformelor on-line pentru cursuri universitare și școlare trebuie să fie analizată din perspectiva a) persoanelor vizate implicate, respectiv a școlărilor care sunt minori și a drepturilor

<sup>[31]</sup> A se vedea cauzele CEDO: *Lawless împotriva Irlandei*, cererea 332/57; *cauza grecească*, cererea 176/56 (Regatul Greciei împotriva Regatului Marii Britanii); A se vedea și Ghidul privind aplicarea art. 15 din Convenția Europeană a Drepturilor Omului, ultima modificare decembrie 2019, disponibil la adresa [https://www.echr.coe.int/Documents/Guide\\_Art\\_15\\_ENG.pdf](https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf) Notificarea este foarte importantă, întrucât în absența acesteia Articolul 15 nu se aplică măsurilor luate de statul pârât. A se vedea: Cipru împotriva Turciei, Raportul Comisiei din 4 October 1983, par. 66-68.

<sup>[32]</sup> A.-M. Șandru, *Inovări și reevaluări în privința drepturilor persoanei vizate în Regulamentul 2016/679*, în *Revista Română de Drept al Afacerilor* nr. 4/2018, p. 42-48.

<sup>[33]</sup> Cauza Bara (C-201/14, *Bara și alții*, hotărârea din 1 octombrie 2015, ECLI:EU:C:2015:638) se aplică chiar în situații de urgență. Cu privire la cauza Bara, a se vedea A.-M. Șandru, *Privire critică asupra jurisprudenței Curții de Justiție a UE referitoare la interpretarea art. 8 privind protecția datelor cu caracter personal din Carta drepturilor fundamentale a Uniunii Europene (CDFUE)*, în *Pandectele Române* nr. 1/2018, p. 26-33. Pe larg: Pentru o știre care nu a fost confirmată de surse independente: T. Leahu, *RCS-RDS deține ilegal o listă a persoanelor izolate la domiciliu. DSP și Poliția neagă că au furnizat baza de date*, 7Iași, 28 martie 2020, <https://www.7iasi.ro/rcs-rds-detine-ilegal-o-lista-a-persoanelor-izolate-la-domiciliu-dsp-si-politia-neaga-ca-au-furnizat-baza-de-date/>

care trebuie respectate de către școli și universități, b) a operatorului, respectiv între școli și universități, din perspectiva autonomiei universitare și a subordonării școlilor, dar și a accesului la educație și c) a platformelor utilizate și a raporturilor juridice stabilite între operatori și aceste platforme on-line.

Implicațiile utilizării platformelor on-line sunt importante pentru că pe această cale s-a făcut un transfer masiv de date cu caracter personal fără măsuri de protecția datelor cu caracter personal. Nume ale elevilor din numeroase școli au fost utilizate pentru a li se constitui conturi în Google Classroom sau Microsoft Team fără să existe o minimă informare cu privire la prelucrarea datelor, modalitățile de ștergere a datelor și perioada pentru care sunt prelucrate datele. Mai mult, prin acești operatori s-au desfășurat cursuri on-line fără ca profesorii sau elevii să fie pregătiți din punctul de vedere al securității datelor.

În mediul universitar s-au utilizat alte platforme, cea mai cunoscută fiind Zoom, dar și Moodle sau platforme ale universităților în care au fost integrate softuri asemănătoare (jitsi, sakai) sau pur și simplu google. În unele situații, pentru a se dovedi activitatea cadrelor didactice cursurile on-line au fost înregistrate în cloud sau în calculatorul acestora. Sunt atât de multe elemente care ar trebui avute în vedere, de la saga zoom care având în vedere succesul mondial de care s-a bucurat și-a îmbunătățit securitatea, la modalitatea de informare de prelucrare a datelor, ori la transferul de date. Desigur, având în vedere spectrul de anulare/înghețare a anului școlar/universitar atât elevii și studenții cât cadrele didactice au considerat un rău mai mic utilizarea acestor platforme. În cele mai multe situații nu ar fi fost vorba de consimțământul participanților întrucât dată fiind starea de urgență ar fi fost o procedură nejustificată și greoaie dacă nu imposibil, dar temeiul legitim al operatorului ar fi trebuit documentat.

În toate aceste cazuri menționate, fiind vorba despre date prelucrate de organisme publice sau autorități ce, potrivit Regulamentului, au obligația de a desemna un responsabil cu protecția datelor<sup>[34]</sup> care să îi ajute să își conformeze activitatea cu dispozițiile RGPD, acest responsabil ar fi trebuit consultat și implicat, în timp util, în toate activitățile ce vizează protecția datelor. Chiar dacă regimul sancționator aplicabil operatorilor din sectorul public diferă de cel aplicabil operatorilor din sectorul privat, în ceea ce privește procedura de constatare și aplicare a amenzilor contravenționale<sup>[35]</sup>, este probabil ca, după ce lucrurile vor reintra în ordinea firească, autoritatea de supraveghere să analizeze cu atenție și toate aceste practici susceptibile de încălcare a Regulamentului.

<sup>[34]</sup> Pentru analiza instituției responsabilului cu protecția datelor a se vedea: I. Alexe, *Principalele noutăți privind responsabilul cu protecția datelor, incluse în GDPR*, în *Pandectele Române* nr. 1/2018, p. 34-45; I. Alexe, *Responsabilul cu protecția datelor (DPO) – funcționar public sau personal contractual?*, în *Revista Română de Dreptul Muncii*, nr. 2/2018, p. 53-65; I. Alexe, *Rolul responsabilului cu protecția datelor în respectarea drepturilor persoanei vizate*, în *Revista Română de Drept al Afacerilor* nr. 3/2019, p. 23-34; I. Alexe, D.-M. Șandru, *Desemnarea unui responsabil cu protecția datelor unic de către mai multe autorități sau organisme publice*, în *Revista de Drept Public* nr. 2/2019, p. 47-56; D.-M. Șandru, I. Alexe, *Subiectele Regulamentului General privind Protecția Datelor în caleidoscopul nuanțelor de ferice*, în *Pandectele române* nr. 3/2019, p. 74-80.

<sup>[35]</sup> Referitor la particularitățile aplicării regimului sancționator în România a se vedea I. Alexe, *Regimul sancționator prevăzut de Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal*, în *Curierul Judiciar* nr. 1/2018, p. 36-42; I. Alexe, D.-M. Șandru, *Reglementări naționale ce vizează aplicarea, în România, a Regulamentului General privind protecția datelor*, în volumul I. Alexe, D.-M. Șandru (editori), *Legislația privind protecția datelor în România*, Ed. Rosetti International, București, 2018, p. 7-25; I. Alexe, *Experiențe ale aplicării amenzilor administrative din România în domeniul GDPR*, în *Pandectele Române* nr. 5/2019, p. 79-95; I. Alexe, *Particularitățile procedurii de efectuare a investigațiilor ce vizează protecția datelor*, în *Pandectele Române* nr. 4/2019, p. 62-75.

## Utilizarea formularelor on-line pentru completarea declarațiilor

*Utilizarea formularelor on-line pentru completarea declarațiilor prevăzute de Ordonanțele militare nr. 2/2020 și 3/2020.* Restrângerea drepturilor persoanelor fizice s-a realizat prin ordonanțe militare. Între alte măsuri, ordonanțele militare nr. 2 și nr. 3 au restrâns dreptul la liberă circulație al cetățenilor. Urmare a acestor acte, mai multe site-uri au realizat formulare care să fie completate de către utilizatori on-line și apoi să fie imprimare sau să fie salvate într-un document de forma pdf. Se poate menționa o lipsă de etică în promovarea acestor site-uri pentru că fie au nume de domenii care să atragă utilizatorii și fac trimitere la guvern/are, fie sunt site-uri ad-hoc care fac trimitere la situația de urgență. Se remarcă și o contradicție în ceea ce se menționează pe site, respectiv faptul că acesta „nu stochează datele dvs. personale, care doar tranzitează server-ul nostru pentru a vă genera documentele”. Așadar, se recunoaște o prelucrare a datelor cu caracter personal („tranzitarea” este tot o modalitate de prelucrare), unele sensibile, fără a exista proceduri publicate pe site privind protecția datelor. Fără a nega utilitatea unor astfel de instrumente, din perspectiva comodității utilizatorilor, trebuie remarcat faptul că acestea nu trebuie să încalce reglementarea privind protecția datelor, pentru că nu există niciun temei în a prelucra date fără a respecta drepturile persoanelor vizate. În aceste situații ar trebui utilizate formulare deja existente pe site-urile publice cum ar fi site-ul Guvernului <https://gov.ro/masuri> sau site-ul [stirioficiale.ro](http://stirioficiale.ro) realizat în „parteneriat cu Guvernul României prin Autoritatea pentru Digitalizarea României”.<sup>[36]</sup>

Măsuri practice pentru site-urile care constituie formulare on-line, fie și pentru situațiile menționate de ordonanțele militare:

- Crearea politicii de confidențialitate;
- Informații privind prelucrarea datelor, în special în ceea ce privește stocarea și distrugerea datelor;
- Informații referitoare la transferul de date către state terțe;
- Informații referitoare la politica cookies;
- Măsurile tehnice și organizatorice pentru prelucrarea datelor;
- Celelalte elemente obligatorii (referitoare la identificarea operatorului, autoritatea de supraveghere etc.).

Încălcarea elementelor enumerate conduce la încălcarea mai multor principii ale Regulamentului general privind protecția datelor. În primul rând este încălcat principiul responsabilității prin inocularea ideii că operatorul respectiv nu prelucrează date cu caracter personal, în al doilea rând

<sup>[36]</sup> CERT-RO a menționat în comunicatul „Echipa CERT-RO recomandă folosirea surselor oficiale în completarea documentelor necesare pentru activitățile din afara locuinței, în perioada restricțiilor determinate de COVID-19, publicat la adresa <https://cert.ro/citeste/recomandare-cert-ro-declaratie-activitate-covid>: „Echipa CERT-RO a primit în ultimele ore numeroase întrebări legate de legitimitatea site-urilor care oferă posibilitatea de a genera, online, declarația pe propria răspundere necesară pentru justificarea prezenței în afara locuinței, în contextul restricțiilor impuse din cauza COVID-19. Pentru generarea unei astfel de declarații este solicitată introducerea unor date cu caracter personal pe site.

Deși unele dintre site-urile semnalate au elementele de securitate necesare și menționează inclusiv faptul că nu colectează și nu procesează date cu caracter personal, CERT-RO nu poate garanta că acest lucru se întâmplă cu respectarea Regulamentului pentru Protecția Datelor cu Caracter Personal sau că respectivele site-uri au autorizarea de a prelucra date cu caracter personal, din partea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Din acest motiv, recomandăm utilizatorilor să folosească doar surse OFICIALE pentru obținerea acestui tip de declarație, în principal cele disponibile pe site-urile MAI, al Guvernului sau stirioficiale.ro.”

principiile proporționalității și echității prelucrării datelor, în al treilea rând, chiar dacă suntem în fața unor formulare oficiale, comoditatea nu poate fi justificată prin încălcarea legislației referitoare la protecția datelor.

Măsuri practice pentru ceilalți operatori: interzicerea utilizării unor astfel de site-uri de pe calculatoarele (device-urile) de serviciu și chiar personale având în vedere impredictibilitatea prelucrării datelor și al transferului către terți a unor date sensibile (inclusiv IP-ul și alte elemente tehnice).

Au fost implicate mai multe tipuri de site-uri:

a) situri situate în afara Uniunii Europene având în vedere domeniul de internet de nivel superior (ccTLD), pentru Muntenegru „.me” sau „.in” pentru India.

b) site-uri cu domeniul „.ro”, de altfel unul închis și altul încă funcțional;

Cu privire la site-ul care până la urmă a închis formularul (și care se apropia cel mai mult de condițiile de conformare cu Regulamentul) ca urmare a sesizării autorității de protecția datelor, aceasta reacționând și anunțând că va demara o investigație<sup>[37]</sup>, site-ul a revenit prin publicarea integrală a politicii de confidențialitate, precizând că poate pune la dispoziția instituțiilor abilitate codul sursă pentru a se verifica inexistența stocării datelor (o zi mai târziu a pus public la dispoziția tuturor codul sursa). Grupul pentru Comunicare Strategică s-a delimitat de aceste aplicații și a arătat că nu lucrează cu ele<sup>[38]</sup>, furnizorii de antivirus au indicat breșe de securitate<sup>[39]</sup> iar CERT-RO a sfătuit cetățenii să utilizeze sursele oficiale<sup>[40]</sup>.

c) site oficial, asumat de autoritățile din România

În fine, un alt formular, dezvoltat de Serviciul de Telecomunicații Speciale, a fost pus la dispoziție, pe site (<https://formular.sts.ro/>) fiind publicate atât „Termeni și condiții. Confidențialitate” cât

<sup>[37]</sup> „Totodată, având în vedere aspectele semnalate, referitoare la posibile prelucrări de date prin intermediul site-ului [...], vă informăm că Autoritatea de Supraveghere a reținut situația prezentată, în vederea exercitării competențelor sale.” Autoritatea face de altfel referire la temeiurile prelucrării și la investigație. Adresa autorității este disponibilă la adresa [https://media.hotnews.ro/media\\_server1/document-2020-03-25-23751738-0-demarare-investigatie.pdf](https://media.hotnews.ro/media_server1/document-2020-03-25-23751738-0-demarare-investigatie.pdf)

<sup>[38]</sup> Ministerul Afacerilor Interne, Actualizarea modelului declarației pe proprie răspundere, 26 martie 2020, <https://www.mai.gov.ro/actualizarea-modelului-declaratiei-pe-proprie-raspundere/>, „Precizăm faptul că orice alte inițiative de a dezvolta platforme electronice folosite pentru completarea declarațiilor pe proprie răspundere/adeverințe de angajator NU beneficiază de acordul autorităților guvernamentale și nu se realizează în colaborare cu acestea. În acest sens, avertizăm asupra riscului folosirii, în mod nejustificat, a unor astfel de instrumente electronice pentru prelucrarea și folosirea fără drept a datelor personale.” Desigur, s-ar putea discuta despre răspundere (juridică, a tuturor cetățenilor) și responsabilitatea juridică și morală, în care rolul important revine autorităților atât în ceea ce privește reglementarea, interpretarea și aplicarea fără abuzuri a dreptului. Despre responsabilitate, a se vedea: C. Ignătescu, *The Premises of Responsibility*, Romanian Journal for Multidimensional Education / Revista Românească pentru Educație Multidimensională, Volume 5, Issue 2, Suplimentary 1, December, Year 2013, p. 41-50; cu privire la domeniul contravențional și abuzul de drept se va scrie mult timp după trecerea pandemiei. Cu privire la abuzul de drept a se vedea: C. Ignătescu, *Abuzul de drept*, Ed. Lumen, 2013, p. 73 referitor la exercițiul drepturilor subiective, în condiții excepționale.

<sup>[39]</sup> V. Barza, *Descărcați declarația pe proprie răspundere doar de pe site-ul Guvernului, avertizează Bitdefender. Compania a blocat pagini neoficiale pentru tentativă de fraudă*, 26 martie 2020, HotNews.ro. De altfel, s-au și demonstrat breșe de securitate: C. Iosub, *Atentie! Declaratiepr.ro a stocat datele personale* <https://www.cristianiosub.com/atentie-declaratiepr-stocat-datele-personale/>

<sup>[40]</sup> *Echipa CERT-RO recomandă folosirea surselor oficiale în completarea documentelor necesare pentru activitățile din afara locuinței, în perioada restricțiilor determinate de COVID-19*, comunicat din 25 martie 2020.

și „ Nota de informare privind prelucrarea datelor cu caracter personal” în care sunt menționate toate elementele obligatorii de informare<sup>[41]</sup>.

#### IV. Efectele coronavirus în domeniul relațiilor de muncă

Angajatorul poate solicita date despre sănătate angajatului? Îi poate măsura temperatura? Dar informații cu privire la starea de sănătate a familiei? În toate situațiile, răspunsul este dat de aplicarea principiului proporționalității. În sprijinul aplicării avem în vedere două documente provenind de la Comitetul European pentru Protecția Datelor și de la autoritatea națională de protecția datelor.<sup>[42]</sup>

În privința Declarației CEPD aceasta nu aduce lămuriri suplimentare față de opiniile și ghidurile anterioare. Nici în documentele adoptate anterior consimțământul nu era favorizat în relația angajat angajator și nici în această declarație.<sup>[43]</sup> „Un angajator poate să solicite vizitatorilor sau angajaților să furnizeze informații specifice de sănătate în contextul COVID-19. Aplicarea principiului proporționalității și reducerii la minimum a datelor este deosebit de relevantă aici. Angajatorul trebuie să solicite informații despre starea de sănătate numai în măsura în care legislația națională o permite.” Curtea Europeană a Drepturilor Omului a pronunțat o decizie<sup>[44]</sup> în care distinge între dreptul la viață privată și dreptul la protecția datelor cu caracter personal. Distincția aceasta trebuie avută în vedere și în contextul pandemiei, întrucât după ce efectele sale se vor fi risipit, angajații vor putea introduce acțiune împotriva angajatorilor sau vor face plângeri la autoritățile de protecția datelor.

[41] Formular.sts.ro – platforma electronică pentru completarea online a declarațiilor pe proprie răspundere și a adeverințelor de angajator, 28 martie 2020, comunicat disponibil la adresa <https://www.mai.gov.ro/formular-sts-ro-platforma-electronica-pentru-completarea-online-a-declaratiilor-pe-proprie-raspundere-si-a-adeverintelor-de-angajator/>: „Platforma operaționalizată pe site-ul Serviciului de Telecomunicații Speciale le permite cetățenilor să completeze de pe telefon sau calculator câmpurile predefinite și, ulterior, să salveze documentele în format PDF. Menționăm că documentele necesită semnătura olografă pentru autentificarea acestora. Este foarte important de menționat că datele personale nu sunt prelucrate de către STS, acestea rămân în telefonul/calculatorul utilizatorului. Pe timpul verificărilor făcute de autorități, persoanele pot prezenta declarația pe proprie răspundere/adeverința de angajator direct de pe telefon (cu semnătură olografă aplicată) împreună cu actul de identitate, pe care personalul abilitat cu verificarea acestora le va putea fotografia.

Precizăm faptul că formular.sts.ro este singura platformă electronică avizată pentru completarea declarațiilor pe proprie răspundere/adeverințe de angajator. Orice alte astfel de platforme online NU beneficiază de acordul autorităților guvernamentale și nu se realizează în colaborare cu acestea. În acest sens, avertizăm asupra riscului folosirii, în mod nejustificat, a unor astfel de instrumente electronice pentru prelucrarea și folosirea fără drept a datelor personale. În baza colaborării cu Guvernul României, platforma formular.sts.ro a fost dezvoltată de compania (...) cu suportul juridic din partea (...) și cu sprijinul Serviciului de Telecomunicații Speciale.”

[42] A.N.S.P.D.C.P., Prelucrarea datelor privind starea de sănătate, comunicat din data de 18 martie 2020 disponibil la adresa [https://www.dataprotection.ro/?page=Prelucrarea\\_datelor\\_privind\\_starea\\_de\\_sanatate&lang=ro](https://www.dataprotection.ro/?page=Prelucrarea_datelor_privind_starea_de_sanatate&lang=ro)

[43] D.-M. Șandru, *Protecția datelor personale în relațiile de muncă. Considerații privind temeiul prelucrării*, în *Pandectele române nr. 5/2019*. D.-M. Șandru, *Curtea de Justiție a Uniunii Europene și protecția datelor personale ale angajaților în relațiile de muncă*, în *Revista Română de Drept European nr. 4/2017*, p. 92-101.

[44] A.A. Ionescu Dumitrache, *Viața privată și datele cu caracter personal. Considerații privind jurisprudența CEDO*, în *PR nr. 6/2019*, p. 75.

Au fost elaborate ghiduri și recomandări ale autorităților de supraveghere a protecției datelor<sup>[45]</sup> sau ale Organizației Mondiale a Sănătății<sup>[46]</sup> cu grade diferite de complexitate care trebuie analizate distinct față de prezentul material.

Prelucrarea datelor celuilalt părinte al copilului în scopul aplicării Legii nr. 19/2020 privind acordarea unor zile libere părinților pentru supravegherea copiilor<sup>[47]</sup>, în situația închiderii temporare a unităților de învățământ se realizează în baza unui temei legal, întrucât este prevăzută expres procedura în hotărârea Guvernului de punere în aplicare<sup>[48]</sup>.

Potrivit Declarației CEPD „angajatorii ar trebui să informeze personalul despre cazurile COVID-19 și să ia măsuri de protecție, dar nu ar trebui să comunice mai multe informații decât este necesar.” Această situație de divulgare a datelor unei persoane fizice este avută în vedere și de jurisprudența CEDO<sup>[49]</sup>.

În aplicarea dispozițiilor privind protecția datelor un rol important îl are responsabilul cu protecția datelor, care înțelege necesitățile operatorului și adaptarea la cerințele externe impuse de restricțiile autorităților. Cuvântul de ordine, „proporționalitate”, este destul de vag, dar tocmai de aceea, DPO este esențial.

## V. Securitatea datelor

Desfășurarea activității de la domiciliu sau din alte locuri în afara locului de muncă aduce avantaje în privința securității sănătății lucrătorilor, dar aceste situații aduc și riscuri pentru operator și pentru persoanele vizate din perspectiva protecției datelor<sup>[50]</sup>.

Telemunca sau desfășurarea activității de la domiciliu trebuie să ia în considerare și probleme care nu implică doar viața intimă și privată a persoanei fizice, ci și creșterea riscurilor cu privire la datele personale din documentele și activitatea profesională. Altfel spus, dacă încălcarea securității datelor referitoare la persoanele fizice are impact redus, deși se referă la viața privată a acestora, așadar vizează date importante, cu atât mai mult prelucrarea datelor din documentele operatorului ar putea crește riscurile, atât cantitativ cât și calitativ.

Măsurile tehnice și organizatorice pe care trebuie să le ia lucrătorii pentru activitățile la calculator sau alte instrumente, pe care le desfășoară acasă<sup>[51]</sup>, se referă în special la informarea de către

<sup>[45]</sup> Lista completă a acestora este disponibilă la adresa <https://www.mihaisandru.ro/daniel-mihail-sandru-protectia-dator-cu-caracter-personal-in-situatii-de-criza-medicala-coronavirus-covid-19/>

<sup>[46]</sup> World Health Organization, „*Getting your workplace ready for COVID-19*”, Geneva, 3 martie 2020 [https://www.who.int/docs/default-source/coronaviruse/getting-workplace-ready-for-covid-19.pdf?sfvrsn=359a81e7\\_6](https://www.who.int/docs/default-source/coronaviruse/getting-workplace-ready-for-covid-19.pdf?sfvrsn=359a81e7_6)

<sup>[47]</sup> M. Of. nr. 209/2020.

<sup>[48]</sup> Hotărârea Guvernului nr. 217/2020 pentru aplicarea prevederilor Legii nr. 19/2020 privind acordarea unor zile libere părinților pentru supravegherea copiilor, în situația închiderii temporare a unităților de învățământ, M. Of. nr. 230/2020.

<sup>[49]</sup> A se vedea cauza CEDO *Y împotriva Turciei*, hotărârea din 17 februarie 2015 (cererea 648/10).

<sup>[50]</sup> P. Otto, P. Marta, N. Salmien, J. Flamant, *Employers Take Notice: Increased Cybersecurity Threats Amid Coronavirus Precautions*, Chronicle of data protection, 13 martie 2020, <https://www.hldataprotection.com/2020/03/articles/cybersecurity-data-breaches/employers-take-notice-increased-cybersecurity-threats-amid-coronavirus-precautions/>; I.N. Kolochenko, *5 Reasons Why COVID-19 Will Bolster the Cybersecurity Industry*, ImmuniWeb, 10 martie 2020, disponibil la adresa <https://www.immuniweb.com/blog/5-reasons-why-covid-19-will-bolster-the-cybersecurity-industry.html>

<sup>[51]</sup> A se vedea lista elaborată de Information Commissioner's Office (ICO) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>

angajator și respectarea regulilor impuse în special cu privire la adrese de e-mail utilizate, posibilitatea utilizării unor stick-uri USB, închiderea sau blocarea tuturor softurilor care ar putea interfera cu datele prelucrate prin instrumentul la care se lucrează (calculator, laptop orice device)<sup>[52]</sup> și utilizarea rețelei private virtuale (virtual private network, prescurtat VPN).

## VI. Fake news, libertatea de exprimare și protecția datelor

Libertatea de exprimare este importantă într-un context de situație excepțională încă de la momentul inițial, respectiv stadiul incipient al apariției virusului în China și comunicarea de către autoritățile chineze și Organizația Mondială a Sănătății și până la cele mai mici detalii de comportament, norme și măsuri insituite de fiecare stat membru în parte. Autoritățile naționale au făcut apel la utilizarea surselor oficiale, înființând chiar site-uri noi în acest sens, Autoritatea pentru Digitalizarea României fiind cea care a garantat caracterul oficial al acestor site-uri<sup>[53]</sup>.

În timpul pandemiei de coronavirus SARS-CoV-2 fenomenul fake news a avut mai multe tipologii:

- cadrul factual (denaturări cu privire la elemente concrete, numărul persoanelor infectate);
- publicitar – în scop de marketing privind un anumit produs (farmaceutic, medicamentos);
- legislativ – prin prezentarea denaturată a unor acte legislative sau
- politic – cu privire la acțiunile statelor implicate.<sup>[54]</sup>

Comisia Europeană și-a asigurat colaborarea platformelor Google, Facebook, Twitter, Microsoft, Mozilla și a asociației comerciale EDiMA, pentru a lupta împotriva răspândirii dezinformării legate de pandemia de coronavirus<sup>[55]</sup>.

La nivel internațional se fac eforturi pentru a disemina doar informații științific confirmate<sup>[56]</sup>, iar informațiile factuale să fie cât mai aproape de adevăr, fără distorsionări în interpretare. Fenomenul de dezinformare sau fake news se poate fundamenta și pe date cu caracter personal impropriu utilizate. Trebuie subliniat că prelucrarea datelor personale, cel puțin forma divulgării identității persoanei vizate, rareori este utilă pentru comunitate sau pentru societate în ansamblul acesteia. În România au existat încălcări ale securității datelor prin prezentarea unor evenimente referitoare la persoane (cum ar fi decesul inexistent, o știre neverificată fiind adusă la cunoștință publică de către un oficial, publicată pe site-ul unui operator importat, preluată de mass-media și mai apoi retractată/dezmințită/ștearsă). Modalitățile în care au reacționat autoritățile, inclusiv prin ștergerea unor pagini de internet sau închiderea unor site-uri vor declanșa dezbateri

<sup>[52]</sup> C. Matyszczyk, *Working from home? Switch off Amazon's Alexa (say lawyers)*, 24 martie 2020, <https://www.zdnet.com/article/working-from-home-switch-off-amazons-alexa-say-lawyers/>

<sup>[53]</sup> <https://datelazi.ro/>, <https://stirioficiale.ro/informatii>, <https://fiipregatit.ro/>. Pe larg: N. Ploeșteanu, R. Miron, *Fakenews și Regulamentul General privind Protecția Datelor*, în *Pandectele române* nr. 5/2019, p. 105-107.

<sup>[54]</sup> Uniunea Europeană a realizat un raport disponibil la adresa <https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/>

<sup>[55]</sup> Pe larg: COVID-19: Comisia colaborează cu platformele online pentru combaterea dezinformării și lansează o pagină web dedicată demontării miturilor și verificării factuale în ceea ce privește pandemia, 30 martie 2020, comunicat disponibil la adresa [https://ec.europa.eu/romania/news/20200330\\_platforma\\_dezinformare\\_coronavirus\\_ro](https://ec.europa.eu/romania/news/20200330_platforma_dezinformare_coronavirus_ro)

<sup>[56]</sup> Google – <https://sites.google.com/fpf.org/covid-19-privacy-resources/>

reeritoare la balansul dintre dreptul la informare (prin modalitatea dezinformării) și libertatea de exprimare, ca drept fundamental<sup>[57]</sup>.

## Concluzii

Coronavirusul SARS-CoV-2 care declanșează boala COVID-19 a provocat intense efecte politice, economice și juridice.

În acest articol am observat tipologia efectelor crizei medicale din 2020 cu privire la principalele aspecte ale vieții sociale și afectarea drepturilor omului având ca punct central dreptul la protecția datelor cu caracter personal. Decretul care instituie starea de urgență nu limitează dreptul la protecția datelor cu caracter personal, cel puțin nu în mod direct, întrucât ar putea fi avută în vedere în referirea la afectarea dreptului la viața privată din Convenția Europeană a Drepturilor Omului. Chiar și în aceste condiții și luând în considerare și declarația României la Consiliul Europei, în temeiul art. 15 din Convenție, statul român trebuie să respecte tratatele la care este parte, inclusiv Carta drepturilor fundamentale a UE, text cu valoare de tratat potrivit art. 6 din Tratatul privind Uniunea Europeană, tratat în care dreptul la respectarea datelor cu caracter personal este prevăzut distinct de dreptul la viața privată. De asemenea trebuie subliniat că nicio instituție a Uniunii Europene, Agenția Drepturilor Fundamentale, Comitetul european pentru protecția datelor, Autoritatea europeană pentru protecția datelor sau vreo autoritate națională nu au comunicat suspendarea sau restrângerea dreptului la protecția datelor pe perioada pandemiei. Toate aceste entități au făcut eforturi de a consilia prin ghiduri, orientări, opinii, comunicate operatorii, persoanele împuternicite de operator și persoanele vizate în respectarea GDPR, în scopul aplicării reglementărilor privind protecția datelor la noua situație.

Sunt discutate exemple concrete din România, cum ar fi formulare de declarații on-line, fotografierea de către polițiști a declarațiilor persoanelor fizice dar și problematice de angajare cum ar fi strategiile autorităților privind localizarea persoanelor infectate sau suspectate a fi purtătorii virusului. Impactul cel mai mare îl au două aspecte care se dezvoltă la nivel mondial: transferul de date, inclusiv transfer de date către state terțe (China, Statele Unite ale Americii) și localizarea.

Acțiunile autorităților de supraveghere a protecției datelor au fost în diferite modalități: cele mai multe au oferit ghiduri, orientări privind aplicarea normelor privind protecția datelor în contextul relațiilor de muncă, unele au realizat colaje cu normele juridice adoptate în timpul situației de urgență (autoritatea de protecția datelor din Italia) iar altele au sancționat operatorii pentru nerespectarea unor norme privind protecția datelor (Polonia).

Fără îndoială că după pandemie vor fi plângeri ale persoanelor vizate pentru nerespectarea legislației privind protecția datelor. Istoria tipologiei protecției datelor în timpul coronavirusului este la început.

În acest material am realizat o sinteză și am oferit sursele de informare directă la ghidurile și orientările elaborate de autoritățile de protecția datelor precum și observații practice privind securitatea informatică mai ales în contextul muncii la domiciliu.

---

<sup>[57]</sup> D.-M. Șandru, *Ierarhizarea valorilor și drepturilor fundamentale în activitatea jurnalistică*, în curs de publicare în *Dreptul nr. 4/2020*; A. Georgescu, I. Alexe, D.-M. Șandru, *Ciocnirea valorilor: legea română privind liberul acces la informațiile de interes public și protecția datelor personale*, în *Revista Română pentru Protecția și Securitatea Datelor cu Caracter Personal (RRPSDCP) nr. 2/2020*.