

**Revista română pentru protecția
și securitatea datelor cu caracter personal
(RRPSDCP)[®]**

1/2022

În atenția colaboratorilor	9
EDITORIAL	
În căutarea unui responsabil cu protecția datelor Silviu-Dorin Șchiopu	10
In Search of a Data Protection Officer Silviu-Dorin Șchiopu	13
STUDII ȘI CERCETĂRI	
Registrul național al persoanelor care au comis infracțiuni sexuale, de exploatare a unor persoane sau asupra minorilor din perspectiva protecției datelor cu caracter personal Bogdan Bodea	15
Elemente jurisprudențiale privind accesul la datele cu caracter personal prelucrate în activitatea parlamentară Nicolae Ploșteanu	22
Datele personale – o veritabilă monedă de plată. Evoluție firească sau abuz? Mihaela Bălău	26
PRAXIS	
Implementarea GDPR – o formă fără fond? Bogdan Panait	35
Prelucrarea datelor de către angajatori în contextul pandemiei de Covid-19 Cristina Bojică	41
OPINII	
De ce breșele de confidențialitate sunt un sport de echipă Amalia Barthel	47
STUDII DE CAZ	
Clearview AI Inc. și puterea celor lipsiți de putere Lorena-Elena Stănescu, Raluca Onufreiciuc	54

MONITORUL PROTECȚIEI DATELOR

Sanțiuni aplicate în perioada ianuarie-iunie 2022 de către autoritățile de supraveghere din Uniunea Europeană

Doru Dorobanțu, Mihaela Mihai..... 73

SECȚIUNEA AUTORITĂȚILOR

Activitatea ANSPDCP în anul 2021113

Registrul național al persoanelor care au comis infracțiuni
sexuale, de exploatare a unor persoane sau asupra
minorilor din perspectiva protecției datelor cu caracter
personal

*National automated Register regarding the persons who
have committed sexual crimes, exploitation of persons or on
minors from the perspective of the protection of personal
data*

BOGDAN BODEA*

▣ Rezumat

La data de 20 iunie 2019 legiuitorul român a adoptat Legea nr. 118/2019 privind Registrul național automatizat cu privire la persoanele care au comis infracțiuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum și pentru completarea Legii nr. 76/2008 privind organizarea și funcționarea Sistemului Național de Date Genetice Judiciare.

Scopul declarat al adoptării acestui act normativ a fost acela al prevenirii și combaterii faptelor de natură sexuală, de exploatare a unor persoane sau asupra minorilor, prevăzute și pedepsite de legea penală, precum și cel de a evita riscul recidivei persoanelor condamnate pentru săvârșirea acestui tip de infracțiuni.

Actul normativ astfel cum a fost adoptat de Parlament prezintă în opinia noastră unele deficiențe incompatibile cu drepturile fundamentale ale persoanei, în special cu dreptul de a fi dat uitării, fapt ce impune o analiză a conformității sale cu exigențele ce decurg din acest drept precum și din necesitatea protecției datelor cu caracter personal.

Cuvinte-cheie: protecția datelor, infracțiuni sexuale, registru, dreptul de a fi uitat.

▣ Abstract

On June 20th 2019, the Romanian legislator adopted Law no 118/2019 on the Automated National Register on persons who have committed sexual offenses, exploitation of persons or crimes against minors, as well as for the completion of Law

* Lect. univ. dr. Bogdan BODEA, Facultatea de Drept, Universitatea din Oradea.

no. 76/2008 regarding the organization and functioning of the National Judicial Genetic Data System.

The declared purpose for adopting this normative act was to prevent and combat sexual acts, exploitation of persons or crimes against minors as prescribed and punished by criminal law, as well as to avoid the risk of recidivism of convicted persons for committing this type of crimes.

The law in the form adopted by the Parliament has, in our opinion, some deficiencies that are incompatible with the fundamental rights of persons, especially with the right to be forgotten, a fact that requires a thorough analysis of its conformity with the requirements arising from this right and from the necessity to protect personal data.

Keywords: data protection, sexual offender, registry, the right to be forgotten.

I. Premise

La data de 20 iunie 2019 legiuitorul român a adoptat Legea nr. 118/2019 privind Registrul național automatizat cu privire la persoanele care au comis infracțiuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum și pentru completarea Legii nr. 76/2008 privind organizarea și funcționarea Sistemului Național de Date Genetice Judiciare¹.

Scopul declarat al adoptării acestui act normativ a fost acela al prevenirii și combaterii faptelor de natură sexuală, de exploatare a unor persoane sau asupra minorilor, prevăzute și pedepsite de legea penală, precum și cel de a evita riscul recidivei persoanelor condamnate pentru săvârșirea acestui tip de infracțiuni².

Realizarea unei evidențe naționale privitoare la persoanele care săvârșesc astfel de fapte nu constituie o noutate absolută. În Europa au fost adoptate o serie de acte normative ce prevăd registre similare, printre care vom aminti *Le fichier judiciaire automatisé des auteurs d'infractions sexuelles et violentes (FIJAVIS)* creat în Franța în anul 2004 sau *Sex offenders register (SOR)*, creat în Regatul Unit al Marii Britanii, în temeiul legislației adoptate în anul 2003.

În Statele Unite, *Sex Offender Registration and Notification Act* („SORNA”) a fost adoptat în anul 2006, ca parte a pachetului legislativ Adam Walsh Child Protection and Safety Act³, însă diverse reglementări statale, precum cea a statului Washington, prevăd încă din anul 1990⁴ norme referitoare la înregistrarea persoanelor ce săvârșesc fapte îndreptate împotriva vieții sexuale sau a minorilor.

Deși niciuna dintre aceste reglementări nu a fost ferită de critici, legislația adoptată de legiuitorul român prevede o serie de aspecte punctuale ce vor ridica probleme din perspectiva interpretării normei sau a conformării acesteia rigorilor impuse de necesitatea protecției datelor cu caracter personal. Articolul de față își propune să supună analizei provocările ce rezultă din incongruența reglementărilor.

¹ Publicată în M. Of. nr. 522 din data de 26 iunie 2019.

² A se vedea, în acest sens, art. 1 al actului normativ indicat.

³ C. R. Yung, *One of these laws is not like the others: why the federal sex offender registration and notification act raises new constitutional questions*, în *Harvard Law Journal*, vol. 46, 2009, p. 369, disponibil pe https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1193871.

⁴ S.J. Schulhofer, *Sex-Offense Registry Laws Abroad* disponibil pe <https://ccresourcecenter.org/2020/11/24/sex-offense-registries-in-europe-and-around-the-world/>.

II. Datele cu caracter personal. Contextul drepturilor fundamentale și al antrenării răspunderii penale

Preocuparea deopotrivă doctrinară și jurisprudențială cu privire la protecția datelor cu caracter personal cunoaște, de dată recentă, o expansiune vizibilă ce nu poate fi trecută cu vederea. Materia drepturilor fundamentale nu a rămas indiferentă acestei expansiuni și deși dreptul de a avea datele personale protejate nu constituie un drept fundamental distinct, acesta este indisolubil legat de persoana umană. În sfera drepturilor fundamentale, protecția datelor cu caracter personal este analizată ca o componentă a dreptului la viață privată.

Normele ce reglementează protecția datelor cu caracter personal sunt menite să protejeze confidențialitatea, identitatea, reputația și autonomia persoanelor și, astfel cum s-a arătat, par a fi (constant) insuficiente pentru a asigura o protecție adecvată în raport de noi riscuri⁵.

De aceea, adaptarea constantă a legislației reprezintă o necesitate axiomatică. În dreptul european această adaptare s-a realizat prin punerea în aplicare, la 25 mai 2018, a noului *Regulament general privind protecția datelor* (GDPR sau „Regulamentul”) ce a înlocuit Directiva 46 din 1995 privind protecția datelor. Adoptat ca răspuns la extinderea masivă a procesării de date cu caracter personal de la introducerea Directivei și respectiv ca răspuns la dezvoltarea unor tehnologii din ce în ce mai intruzive, Regulamentul se bazează pe Directivă și pe jurisprudența Curții de Justiție a UE (CJUE) în materie, extinzând în mod semnificativ Directiva și consolidând în acest fel principalul regim de protecție a datelor în Uniunea Europeană⁶.

Aspecte proprii protecției datelor cu caracter personal au devenit instituții consacrate ale drepturilor omului. Astfel, dreptul de a fi dat uitării⁷, consacrat jurisprudențial de către CJUE în *Cauza Google Spain*⁸, este analizat ca o componentă de netăgăduit a dreptului la viață privată, inclusiv în jurisprudența Curții Europene a Drepturilor Omului (CEDO)⁹.

⁵ S. Wachter & B. Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI*, Columbia Business Law Review, Issue 2, 2019, p. 5, disponibil pe https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829.

⁶ D. Korff, M. Georges, *The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation*, disponibil pe https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3428957, p. 6.

⁷ *The right to be forgotten*, tradus adeseori ca dreptul la ștergerea datelor sau de a fi uitat.

⁸ Hotărârea CJUE din 13 mai 2014, publicată pe <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN>. În deja celebra decizie, s-a reținut ca stare de fapt că în martie 2010, domnul Costeja González, cetățean spaniol, a formulat o reclamație în fața autorității spaniole competente, împotriva societății care publica un cotidian de largă difuzare precum și împotriva Google Spain și a Google Inc. având în vedere că atunci când se introducea numele său în motorul de căutare al grupului Google erau afișate linkuri către două pagini ale cotidianului La Vanguardia pe care figura un anunț, în care se menționa numele său în legătură cu o procedură de vânzare la licitație a unor imobile desfășurată în vederea plății unor datorii la asigurările sociale, cu toate că executarea silită în cauză s-a finalizat în întregime în urmă cu mai mulți ani. El a solicitat să se dispună ca La Vanguardia fie să elimine sau să modifice paginile menționate astfel încât să nu mai apară datele sale cu caracter personal, iar Google Spain sau Google Inc. să elimine sau să oculteze datele sale cu caracter personal, astfel încât acestea să nu mai apară printre rezultatele căutării.

⁹ A se vedea, cu titlu de exemplu, M.L. și W.W. c. Germaniei, Hotărârea din 18 iunie 2018, publicată pe <https://hudoc.echr.coe.int/fre#%7B%22languageisocode%22:%5B%22ENG%22%5D%22app>

Deși în jurisprudența CEDO temeiul beneficiază de o autonomie conceptuală proprie, în esență componente ale dreptului la viață privată dezvoltate în cadrul acestei jurisprudențe înglobează majoritatea principiilor și exigențelor ce decurg din standardele impuse de GDPR. Aceste standarde, devenite componente ale unui drept fundamental, au aptitudinea de a surclasa legislația națională în temeiul dispozițiilor art. 20 din Constituție, situație în care filtrarea normelor de drept intern prin prisma lor este inevitabilă.

Cu toate acestea, activitatea de antrenare a răspunderii penale pare a fi exceptată de la standardele GDPR¹⁰, în condițiile în care Regulamentul general al UE privind protecția datelor, transpus în dreptul național prin Legea nr. 190/2018¹¹, conține în art. 10 dispoziții speciale cu privire la prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe. Potrivit reglementării, aceasta se efectuează numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate, iar orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat¹².

Astfel, cel puțin din perspectiva persoanelor a căror răspundere este antrenată, datele cu caracter personal sunt cunoscute și pot fi utilizate de către autorități, ele servind atât la identificarea corectă a persoanei a cărei răspundere penală urmează a fi angajată cât și la realizarea unor baze de date precum cazierul judiciar ce în sine nu sunt contrare principiilor de utilizare conformă a datelor¹³.

Cu referire la *Registrul național al persoanelor care au comis infracțiuni sexuale, de exploatare a unor persoane sau asupra minorilor*, observăm că aparent nu există un concurs de norme aflate în disonanță în ceea ce privește protecția datelor cu caracter personal. Legea nr. 118/2019 prevede expres posibilitatea preluării în Registru în integralitate, pentru fiecare persoană în cauză, datele cu caracter personal și datele judiciare prevăzute la art. 8 alin. (11) și (13), art. 9 și 11 din Legea nr. 290/2004, republicată, cu modificările și completările ulterioare¹⁴. Cu toate acestea, unele aspecte vor trebui nuanțate, interferențele nelimitându-se exclusiv la situația preluării datelor.

no%22:[%2260798/10%22,%2265599/10%22],%22documentcollectionid%22:[%22CHAMBER%22],%22itemid%22:[%22001-183947%22]}.

¹⁰ Cel puțin din perspectiva persoanelor a căror răspundere este antrenată. În ceea ce privește inculpatul datele sale personale sunt cunoscute și pot fi utilizate oricând de către autorități, ele servind de cele mai multe ori la identificarea corectă a persoanei a cărei răspundere penală urmează a fi angajată. Realizarea unor baze de date precum cazierul judiciar și registrul nu este în sine contrară principiilor de utilizare conformă a datelor.

¹¹ Publicată în M. Of. nr. 651 din 26 iulie 2018.

¹² A se vedea art. 10 din Regulamentul 2016/679, 27 aprilie 2016, publicat în JO 119 L din 04 mai 2016.

¹³ În privința altor participanți, suprapunerile sunt și mai evidente, iar pentru a exemplifica aceste suprapuneri este îndeajuns să amintim instituțiile procesual penale precum cea a martorului protejat sau protecția conferită victimelor infracțiunii prin protecția datelor de identitate.

¹⁴ Art. 9 alin. (2) din Legea nr. 118/2019.

Regulamentul prevede expres dreptul la ștergerea datelor (de a fi uitat) reținând că persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate atunci când: datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate; persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare; persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea; datele cu caracter personal au fost prelucrate ilegal; datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul; sau datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la art. 8 alin. (1)¹⁵.

Din această perspectivă, una dintre duratele de stocare a datelor prevăzute de Legea nr. 118/2019 o considerăm disproporționată. Astfel, art. 10 din Legea nr. 118/2019 prevede că persoanele fizice înscrise în Registru se scot din evidență la împlinirea vârstei de 85 de ani, dacă pedeapsa aplicată este mai mare de 5 ani.

Cum pentru majoritatea infracțiunilor ce antrenează înscrierea în registru pedeapsa de 5 ani se situează între limitele speciale de pedeapsă, o persoană care săvârșește una dintre infracțiunile în discuție la o vârstă fragedă, va suporta, de principiu pe tot parcursul vieții sale, consecințele înscrierii în acest registru.

În aceste condiții se pune în mod just problema perioadei pentru care se consideră că datele cu caracter personal sunt necesar a fi stocate, respectiv determinarea momentului de la care acestea nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate, moment ce ar putea conduce la ștergerea acestor date în temeiul art. 17 alin. (1) lit. (a) al Regulamentului.

Astfel cum arătam anterior, scopul culegerii și stocării acestor date este acela al prevenirii și combaterii faptelor de natură sexuală, de exploatare a unor persoane sau asupra minorilor, prevăzute și pedepsite de legea penală, precum și cel de a evita riscul recidivei persoanelor condamnate pentru săvârșirea acestui tip de infracțiuni. Putem accepta că acest scop subzistă, de principiu pentru o lungă perioadă de timp, însă exprimăm serioase rezerve că el subzistă pe întreaga viață a persoanei condamnate.

Este de observat că legislația stipulează expres că intervenirea grațierii, prescripției executării pedepsei, amnistiei sau reabilitării cu privire la persoanele fizice înscrise în Registru nu conduc la scoaterea acestora din evidența Registrului¹⁶. Nu vom argumenta, în contra dispozițiilor legale, că reabilitarea ar trebui să conducă la ștergerea automată a acestor date. Opțiunea disocierii momentului de la care păstrarea datelor devine inoportună de momentul reabilitării condamnatului ține de politica penală a statului, cu care, de altfel, prin raportare la natura infracțiunilor, suntem mai mult decât de acord.

Însă o evaluare a factorilor de risc de recidivă este la îndemâna organelor judiciare, fapt pentru care argumentăm că subsecvent reabilitării ar trebui instituită o procedură judiciară în cadrul căreia acești factori de risc să fie analizați. Dacă aceștia subzistă, scopul pentru care au fost colectate sau prelucrate datele este actual, iar ștergerea acestora este inoportună. Dacă scopul nu mai subzistă, menținerea datelor în registru

¹⁵ A se vedea art. 17 din Regulamentul 2016/679.

¹⁶ A se vedea art. 10 alin. (5) din Legea nr. 118/2019.

constituie o încălcare a GDPR iar legislația ar trebui să reglementeze o procedură judiciară de eliminare a acestor date. De altfel, CJUE a statuat că o prelucrare inițial legală a unor date exacte poate deveni cu timpul incompatibilă cu Directiva sau cu Regulamentul atunci când datele respective nu mai sunt necesare în raport cu scopurile pentru care au fost colectate sau prelucrate. Aceasta este situația în special atunci când ele sunt inadecvate, atunci când nu sunt sau nu mai sunt relevante ori sunt excesive în raport cu scopurile respective și cu timpul care s-a scurs¹⁷.

O altă situație ce va ridica serioase probleme în raport de conformitatea cu exigențele ce decurg din Regulament o reprezintă obligația organelor de poliție de a desfășura periodic, dar nu mai târziu de o dată la 3 luni, verificări la domiciliu, reședința sau imobilul în care persoanele înscrise în Registrul locuiesc efectiv, în scopul obținerii de date și informații privind comportamentul acestor persoane și modul de obținere a mijloacelor de existență, precum și actualizării, după caz, a datelor din Registrul sau din celelalte baze de date ale Poliției Române¹⁸.

Cu toate că legea prevede că aceste verificări se vor desfășura în condiții de confidențialitate¹⁹, o atare prevedere este mai mult decât utopică. A considera că persoanele de la care astfel de date se obțin²⁰ nu își vor pune problema rațiunii unei asemenea verificări este de neconceput. Cum legislația în vigoare nu prevede expres o altă situație în care asemenea informații să fie obținute *cu o asemenea regularitate*, confidențialitatea ar putea fi păstrată doar dacă prezumăm că aceste persoane nu cunosc legislația ce impune astfel de verificări.

În mod evident, o atare procedură atrage atenția societății asupra persoanei condamnatului și asupra împrejurării condamnării sale pentru o infracțiune de natură sexuală, de exploatare a unor persoane sau asupra minorilor, chiar dacă infracțiunea în sine nu este identificată²¹.

Scopul normei nu este acela de a stigmatiza persoana condamnatului în societate, aspect ce se deduce cu prisosință din împrejurarea că aceste date referitoare la condamnare sunt accesibile unui număr relativ restrâns de persoane, iar nu publicului larg. În acest context, așteptarea rezonabilă privind viața privată există, iar aducerea la cunoștința terților, chiar indirect, a calității de condamnat va constitui o încălcare a vieții private și a obligației legale de confidențialitate prevăzută de art. 12 alin. (4) al Legii nr. 118/2019.

De altfel, așteptarea rezonabilă privind protecția vieții private decurge din chiar stipularea normativă a obligației de confidențialitate, ce în mod practic apreciem că va fi imposibil de asigurat. Această obligație nu trebuie înțeleasă restrictiv, în sensul în care aceasta se referă exclusiv la obligația agentului de a nu divulga rațiunea interogării, ci extensiv, prin raportare la necesitatea ca societatea să nu cunoască în niciun mod situația condamnatului sau rațiunea verificărilor.

În Jurisprudența CJUE s-a reținut că o prelucrare a unor date referitoare la condamnări poate fi legală, în temeiul dispozițiilor art. 8 al Directivei și 10 al

¹⁷ A se vedea cauza *GC and Others*, Hotărârea CJUE din 24 septembrie 2019, disponibilă pe [¹⁸ Această obligație este stipulată expres în cuprinsul art. 12 alin. \(3\) al Legii nr. 118/2019.](https://curia.europa.eu/juris/document/document.jsf?jsessionid=B2F294B463CCD17EBC739CA58D3BD459?text=&docid=218106&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=4253061, § 74.</p>
</div>
<div data-bbox=)

¹⁹ Art. 12 alin. (4) al Legii nr. 118/2019.

²⁰ Prin ipoteză altele decât condamnatul pentru a asigura eficiența culegerii de date.

²¹ De cele mai multe ori chiar neidentificarea infracțiunii va putea genera prejudicii mai mari decât determinarea ei *in concreto*, deoarece necunoscutul generează incertitudine.

Regulamentului și sub rezerva respectării celorlalte condiții de legalitate stabilite de Directivă și de Regulament, în special dacă dreptul național prevede garanții corespunzătoare și specifice, acesta putând fi cazul când informațiile în discuție au fost divulgate publicului de autoritățile publice *cu respectarea dreptului național aplicabil*²². Câtă vreme dreptul național impune obligația confidențialității, scurgerea chiar indirectă a datelor referitoare la condamnare este inadmisibilă.

Soluțiile remediale ar fi două: pe de-o parte, s-ar putea argumenta că înlăturarea obligației de confidențialitate ar face ca așteptarea rezonabilă să dispară, iar o potențială astfel de divulgare indirectă să fie conformă, realizată inclusiv cu respectarea dreptului național. O a doua soluție ar fi o regândire a modalității de verificare a acestor persoane și reformularea textului legal indicat. În ceea ce ne privește, optăm pentru această din urmă soluție, deoarece prima ar păstra în continuare inconvenientul nerespectării așteptării rezonabile referitoare la respectul datorat vieții private, prin prisma argumentului sferei limitate de persoane care pot avea acces la datele înscrise în Registru.

În aceste condiții, apreciem că textul art. 12 trebuie reformulat astfel încât acesta să conțină obligația de a face verificări *cu privire* la domiciliu, reședința sau imobilul în care persoanele înscrise în Registru locuiesc efectiv și *cu privire* la comportamentul acestor persoane și modul de obținere a mijloacelor de existență. O atare modificare va permite utilizarea unui spectru mai larg de metode investigative decât simpla prezentare *la domiciliul* persoanei condamnate.

IV. Concluzii

Activitatea de antrenare a răspunderii penale pare a fi exceptată de la standardele impuse de Regulamentul GDPR. Cu toate acestea, unele aspecte sunt necesar a fi nuanțate, interferențele nelimitându-se exclusiv la situații reglementate normativ.

În privința duratei de stocare a datelor am arătat că o evaluare a factorilor de risc de recidivă (scopul principal al stocării) este la îndemâna organelor judiciare, fapt pentru care după o anumită perioadă, spre exemplu subsecvent reabilitării, ar trebui instituită o procedură judiciară în cadrul căreia acești factori de risc să fie analizați. Dacă aceștia subzistă, scopul pentru care au fost colectate sau prelucrate datele este actual, iar ștergerea acestora este inoportună. Dacă scopul nu mai subzistă, menținerea datelor în Registru constituie o încălcare a GDPR iar legislația ar trebui să reglementeze o procedură judiciară de eliminare a acestor date.

Referitor la obligația organelor de a efectua verificări ale persoanei condamnatului cu respectarea confidențialității, am apreciat că textul art. 12 trebuie reformulat astfel încât acesta să conțină obligația de a face verificări *cu privire* la domiciliu, reședința sau imobilul în care persoanele înscrise în Registru locuiesc efectiv și *cu privire* la comportamentul acestor persoane și modul de obținere a mijloacelor de existență. O atare modificare va permite utilizarea unui spectru mai larg de metode investigative decât simpla prezentare *la domiciliul* persoanei condamnate, în vederea realizării acestor verificări, prezentare ce altminteri ar putea cu ușurință devoala rațiunea verificărilor periodice.

²² A se vedea cauza *GC and Others*, Hotărârea CJUE din 24 septembrie 2019, precitată, § 73.

Case law on access to personal data processed in parliamentary activity

NICOLAE PLOEȘTEANU*

□ Rezumat

Curtea de Justiție a Uniunii Europene s-a pronunțat în cauza C-272/19, în sensul că prelucrarea datelor cu caracter personal realizată de către Comisia de petiții din cadrul Parlamentului Landului Hessen intră în domeniul de aplicare a Regulamentului General privind Protecția Datelor. În acest studiu se evidențiază, pornind de la jurisprudența CJUE, câteva reguli și criterii de interpretare a unei excepții de la aplicarea RGPD pentru a se delimita situațiile care intră și cele care nu intră sub incidența Regulamentului, din perspectiva art. 2 alin. (2) pct. (a), în sensul că o asemenea activitate nu intră sub incidența dreptului Uniunii. De asemenea, studiul evidențiază anumite subtilități din cererea formulată de judecătorul național către CJUE în vederea unei decizii preliminare, subtilități care par să conducă la ideea că judecătorul național a încercat, prin rolul său, să obțină de la Curte un „dialog” mai vast decât cel necesar pentru soluționarea cauzei.

Cuvinte-cheie: Parlamentul Landului Hessen; Regulamentul General privind Protecția Datelor; cerere de acces la date cu caracter personal; comisia de petiții; domeniul de aplicare RGPD.

□ Abstract

The Court of Justice of the European Union ruled in Case C-272/19 that the processing of personal data by the Petitions Committee of the Hessen Land Parliament falls within the scope of the General Data Protection Regulation. In this study, the CJEU case law is used to highlight some rules and criteria for interpreting an exception to the application of the GDPR in order to distinguish between situations which are covered and those which are not, in the light of Article 2(2)(a) of the Regulation to the effect that such activity is not covered by Union law. The study also highlights certain points in the national judge's application to the CJEU for a preliminary ruling, which seem to lead to the idea that the national judge was trying through his role to obtain from the Court a broader „dialogue” than necessary for the resolution of the case.

Keywords: Hessen Land Parliament; General Data Protection Regulation; request for access to personal data; petitions committee; scope of GDPR.

Cauza C-272/19, Land Hessen, 9 iulie 2020. Activitățile parlamentare indirecte și prelucrarea datelor cu caracter personal

1. Istoricul și relevanța cauzei

Cauza¹ C-272/19 a fost soluționată de către CJUE, prin hotărârea pronunțată la data de 9 iulie 2020 de către Camera a treia a Curții. Acesteia i s-a adresat, în anul 2019,

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

¹ ECLI:EU:C:2020:535.

Verwaltungsgericht Wiesbaden (Tribunalul Administrativ din Wiesbaden, Germania) cu o cerere de decizie preliminară formulată în temeiul art. 267 din Tratatul privind Funcționarea Uniunii Europene (TFUE). Cauza nu prezintă dificultăți mari, însă ridică mai multe chestiuni importante, având la bază o **respingere** de către președintele Hessischer Landtag (Parlamentul landului Hessa) a **cererii de acces** a persoanei interesate la datele cu caracter personal care o privesc, înregistrate de Comisia pentru petiții din cadrul acestui parlament. Respingerea cererii de acces a reprezentat obiectul litigiului între VQ, pe de o parte, și Land Hessen (landul Hessa, Germania), pe de altă parte. Motivul pentru care președintele Parlamentului landului Hessa a decis să respingă cererea a fost că procedura de petiționare constituie o misiune parlamentară și că parlamentul respectiv nu intră în domeniul de aplicare al Regulamentului 2016/679. Trebuie arătat că în cauză au prezentat observații scrise, în afara părților implicate în litigiul principal, guvernul ceh, estonian, polonez și Comisia europeană.

a. Aplicarea rationae materiae a RGPD. În primul rând, din perspectiva Regulamentului General privind Protecția Datelor apreciem că o singură problemă juridică serioasă s-a pus, anume dacă activitatea unei Comisii de petiții din cadrul unui Parlament se încadrează sau nu în excepția de la aplicarea RGPD, prevăzută de art. 2 alin. (2) pct. (a), în sensul că o asemenea activitate nu intră sub incidența dreptului Uniunii. Altfel spus, problematica juridică principală privește aplicarea *rationae materiae* a RGPD. Atunci când o problemă legată de interpretarea art. 2 alin. (2) se ridică, există raționamente importante privind interpretarea excepției, exprimate cu prilejul soluționării altor cauze, precum Martorii lui Iehova.

b. Reguli de evaluare a excepției de inaplicabilitate a RGPD. În cele ce urmează evidențiem câteva **reguli metodologice** de evaluare a unei excepții în sensul art. 2 alin. (2) lit. a) RGPD, reguli care se desprind din analiza realizată de Avocatul General în cauza *Martorii lui Iehova*, chiar dacă prin raportare la Directiva 46/95 în vigoare la momentul producerii faptelor.

O primă regulă este una generală de interpretare, anume că art. 2 alin. (2) lit. a) RGPD cuprinde o excepție, o derogare de la regula generală a aplicabilității RGPD, astfel că norma care o prevede trebuie *interpretată în mod restrictiv*. Acest mod de interpretare este consecința faptului că obiectivul² RGPD este de a garanta un nivel ridicat de protecție a drepturilor și a libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață privată, în privința prelucrării datelor cu caracter personal. Aceasta înseamnă *inter alia* că în afara excepțiilor de la art. 2 alin. (2) RGPD nu prevede nicio limitare suplimentară a domeniului său de aplicare. În același sens, dar menit să configureze tipologia situațiilor care ar cădea în sfera excepției, această regulă de interpretare trebuie să țină cont de *natura excepțiilor* incluse inițial la art. 3 alin. (2) prima liniuță (cele pur domestice și casnice fiind menționate la cea de a doua liniuță!), deoarece acestea³ „sunt menite să definească domeniul de aplicare al excepției prevăzute în dispoziția amintită, astfel încât această excepție nu se aplică decât

² A se vedea, exemplificativ, Hotărârea din 11 decembrie 2014, Ryneš (C-212/13, EU:C:2014:2428, par. 27).

³ În cauză sunt redatate cu mențiunea de a fi exemplificative, prin raportare la Directiva 95/46, activitățile din domeniile prevăzute în titlurile V și VI din Tratatul privind Uniunea Europeană și prelucrările care au ca obiect siguranța publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când aceste prelucrări sunt legate de probleme de securitate a statului) și activitățile statului în domeniul dreptului penal.

activităților expres menționate în această dispoziție sau care pot fi încadrate în aceeași categorie (*etusdem generis*)⁴.

O altă regulă rezultă din coroborarea art. 2 alin. (2) lit. a) RGPD cu enunțul considerentului (16) al aceluiași regulament, coroborare din care reiese că în categoria de excepții se includ, *doar exemplificativ*, prelucrările de date realizate în contextul activităților de *siguranță națională*. La rândul său, domeniul siguranței naționale comportă nuanțele evidențiate de jurisprudența CJUE, pe care le vom expune într-o secțiune distinctă.

A treia regulă este că, spre deosebire de unele drepturi fundamentale a căror protecție europeană este asigurată atunci când ele prezintă o legătură cu *libertatea de circulație între statele membre*, legislația de protecție a datelor (RGPD) „definește în mod foarte larg domeniul său de aplicare, printre altele făcând ca aplicarea normelor de protecție să nu depindă de aspectul dacă prelucrarea presupune o legătură efectivă cu libera circulație între statele membre⁵.

O a patra regulă, pune accentul pe *calitatea entităților* care ar realiza prelucrări de date în contextul unor activități ce cad sub incidența excepției. Activitățile vizate de excepție „sunt, în toate cazurile, activități proprii statelor sau autorităților statale, străine de domeniile de activitate ale particularilor”⁶.

A cincea regulă, mai degrabă de natură practică, constă în faptul că statele membre au *competență exclusivă* de a reglementa un anumit domeniu, situație care nu înlătură în mod obligatoriu nici aplicarea RGPD și nici *nu conduce automat* la încadrarea unei activități din acel domeniu în *categoria excepțiilor* avute în vedere de art. 2 alin. (2) lit. a) RGPD.

În final, o **a șasea regulă** care s-ar putea desprinde din jurisprudența Curții în general, este că atunci când activitățile de prelucrare a datelor, care de regulă intră în sfera excepțiilor, presupun totuși o legătură cu alte activități de prelucrare a datelor care cad sub incidența RGPD, tendința de a asigura un nivel cât mai ridicat de protecție conduce la includerea tuturor în sfera de aplicabilitate a RGPD, excluzând aplicarea excepției.

2. Concluzia Curții asupra excepției

Curtea a evidențiat în cauza Landul Hessen, că excepțiile prevăzute de art. 2 alin. (2) RGPD sunt de strictă interpretare în raport cu domeniul larg de reglementare a aplicabilității acestuia⁷. De asemenea, pe aceeași linie de gândire, Curtea a arătat că activitățile parlamentare nu sunt, cu acest titlu, enumerate în Regulamentul 2016/679, în special în considerentul (20) și la art. 23 din acesta, ca reprezentând excepții.

Ceea ce a subliniat cu titlu nou Curtea este că activitățile unei Comisii pentru petiții din cadrul unui Parlament federat au evident o natură politică și administrativă, contribuind indirect la activitatea parlamentară și chiar dacă au o natură publică și sunt proprii acestui land nu înseamnă cu sunt activități care se încadrează în excepția analizată și prevăzută de RGPD. Ca urmare, „prelucrarea datelor cu caracter personal

⁴ Hotărârea din 6 noiembrie 2003, *Lindqvist* (C-101/01, EU:C:2003:596, pct. 44).

⁵ Hotărârea din 20 mai 2003, *Österreichischer Rundfunk și alții* (C-465/00, C-138/01 și C-139/01, EU:C:2003:294, pct. 43).

⁶ Hotărârea din 6 noiembrie 2003, *Lindqvist* (C-101/01, EU:C:2003:596, pct. 43).

⁷ Punctul 68 din Hotărâre.