editorial

În căutarea unui responsabil cu protecţia datelor

SILVIU-DORIN ŞCHIOPU*

Având în vedere adagiul *nemo censetur ignorare legem* (nimănui nu-i este îngăduit să nu cunoască legea), probabil fiecare student al unei facultăţi de drept şi-a propus ca după absolvire să citească la cafeaua de dimineaţa Monitorul Oficial al României (măcar Partea I). În practică însă, în cel mai bun caz am setat nişte alarme privind evenimentele legislative suferite de actele normative de imediat interes, serviciu oferit de unele software-uri pentru documentare şi cercetare juridică.

Am ajuns a da curs promisiunii din studenţie odată cu venirea virusului SARS-CoV-2 pe meleagurile noastre, când starea de urgenţă a făcut ca publicarea legislaţiei să se facă mai ales la ceas de seară. Astfel, cu rare scăpări, de aproape doi ani parcurg titlurile actelor normative. Deunăzi, văzând publicarea unui Regulament privind organizarea şi funcţionarea *platformei online* de schimbare a furnizorului de energie electrică şi gaze naturale şi pentru contractarea furnizării de energie electrică şi gaze naturale[1], am adulmecat o prelucrare de date cu caracter personal.

Lecturând penultimul articol al acestui regulamentul se poate citi că „(u)tilizatorii POSF [platforma online destinată schimbării de către clientul final a furnizorului de energie electrică şi/sau de gaze naturale – n.n.] au obligaţia respectării în cadrul şi în legătură cu POSF a *Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date* (s.n.) în raport cu datele şi informaţiile CF [clientului final – n.n.] […]"[2]. Am oftat…

Menţionarea Regulamentului general privind protecţia datelor a devenit o figură de stil cu precădere în actele administrative cu caracter normativ. De regulă, o atare

* Doctorand, Universitatea Nicolae Titulescu din Bucureşti; https://orcid.org/0000-0002-9927-1016.

[1] Aprobat prin art. 1 din Ordinul Preşedintelui Autorităţii Naţionale de Reglementare în Domeniul Energiei nr. 3 din 26 ianuarie 2022, publicat în M. Of. nr. 108 din 3 februarie 2022.

[2] În continuare se precizează că obligaţia respectării Regulamentului (UE) 2016/679 există „atât la momentul introducerii acestora (datelor cu caracter personal ale clienţilor finali – n.n.) în POSF, cât şi în cazul în care se impun actualizări", de unde rezultă că trimiterea la Regulamentul general privind protecţia datelor pare să aibă în vedere numai *principiul exactităţii datelor* prevăzut de art. 5 alin. (1) lit. d) GDPR, ignorând restul.

trimitere îmbrăcă forma: „cu respectarea prevederilor Regulamentului (UE) 2016/679", ca și cum o asemenea formulă ar avea darul de a asigura ca prin magie, precum o simplă rotire a baghetei sau o răsucire de inel, protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal ori punerea în operă a principiilor protecției datelor.

Mânat de un gând șăgalnic am decis să adresez operatorului de date cu caracter personal o întrebare în temeiul liberului acces la informațiile de interes public. Precum rezultă din art. 8 alin. (1) din Regulamentul privind organizarea și funcționarea platformei online, administratorul și operatorul POSF va fi Autoritatea Națională de Reglementare în Domeniul Energiei (ANRE) – însuși emitentul regulamentului cu pricina – iar ANRE este o autoritate administrativă autonomă[3]. Astfel, am solicitat a mi se preciza „care va fi temeiul juridic (prevăzut de art. 6 GDPR) al prelucrării datelor cu caracter personal al clienților finali, persoane fizice, în cadrul platformei POSF".

Nu mică mi-a fost mirarea când, la nicio oră după trimiterea cererii, am primit un răspuns de la responsabilul cu protecția datelor din cadrul ANRE (acesta având și calitatea de „Expert Birou IT") care, după ce confirmă primirea solicitării[4], precizează că „(u)nul dintre experții IT va reveni în scurt timp cu mai multe informații"[5]. În asemenea momente cei mai slabi de înger (și de știință) încep să aibă dubii cu privire la prevederile Regulamentului (UE) 2016/679.

Potrivit art. 39 alin. (1) lit. b) GDPR, responsabilul cu protecția datelor *monitorizează respectarea* Regulamentului general privind protecția datelor, în acest sens furnizând operatorului orientări pentru demonstrarea conformității[6]. Cum operatorul este responsabil de respectarea principiilor legate de prelucrarea datelor cu caracter personal, inclusiv de demonstrarea legalității prelucrării, este nefiresc ca tocmai cel care ar trebui să acorde asistență operatorului pentru monitorizarea conformității să nu știe răspunsul la o întrebare privind temeiul juridic al prelucrării. Iar aceasta cu atât mai mult cu cât art. 37 alin. (5) GDPR prevede că responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, *în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor*[7], iar obligația de informare a persoanelor vizate, când platforma va deveni operațională, va include comunicarea temeiului juridic al prelucrării.

Deși nu putem nega contribuția unui „Expert Birou IT" la buna implementare a măsurilor tehnice și organizatorice de securitate, a reduce responsabilul cu protecția datelor la competențe ce nu se circumscriu pe deplin literei și spiritului Regulamentului (UE) 2016/679 este nefast pentru orice autoritate publică sau organism privată și nu fără impact asupra efectivității protecției drepturilor persoanelor vizate.

În sistemul heliocentric al Regulamentului general privind protecția datelor nu sistemele IT constituie miezul, ci persoanele fizice și dreptul lor fundamental la protecție

---

[3] A se vedea art. 1 alin. (1) din O.U.G. nr. 33 din 4 mai 2007 privind organizarea și funcționarea Autorității Naționale de Reglementare în Domeniul Energiei, publicată în M. Of. nr. 337 din 18 mai 2007, cu modificările și completările ulterioare.

[4] Https://servicedesk.intern.anre/Ticket/13923.

[5] În original lipseau diacriticele.

[6] În acest sens, a se vedea considerentul (77) GDPR.

[7] De asemenea, a se vedea considerentul (97) GDPR care prevede că, în cazul în care prelucrarea este efectuată de o autoritate publică, responsabilul cu protecția datelor ar trebuie să fie „o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor [și care] ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament".

în ceea ce priveşte prelucrarea datelor cu caracter personal. În acest sens considerentul (15) GDPR subliniază că „protecţia persoanelor fizice ar trebui să fie neutră din punct de vedere tehnologic şi să nu depindă de tehnologiile utilizate", astfel că expertiza în tehnologia informaţiei nu este suficientă (şi poate nici necesară) pentru a face un veritabil responsabil cu protecţia datelor. Aşa cum o coroană nu te face rege, nici titulatura unei funcţii nu-l face pe deţinător DPO. Totuşi hârtia suportă multe[8], la fel şi o carte de vizită.

[8] Observaţia priveşte şi decizia Autorităţii Naţionale de Reglementare în Domeniul Energiei, în calitate de operator de date cu caracter personal, de a desemna un responsabil cu protecţia datelor potrivit art. 37 alin. (1) lit. a) GDPR.

In Search of a Data Protection Officer

SILVIU-DORIN ŞCHIOPU*

In view of the brocard *nemo censetur ignorare legem* (nobody is thought to be ignorant of the law), probably every law student promised himself/herself that after graduation they will read the Official Journal of Romania (at least Part I – legislation) while having the morning coffee. In practice, however, at best we have set some alarms for legislative events suffered by normative acts of immediate interest, service provided by some software for legal documentation and research.

I managed to fulfil the promise made as a student when the SARS-CoV-2 virus visited our lands and the state of emergency made the publication of the legislation to be done especially in the dead of night. So, for almost two years, I have been reading the titles of normative acts. A couple of days ago, seeing the publication of a Regulation on the organization and operation of the *online switching platform* for electricity and natural gas suppliers and for contracting the supply of electricity and natural gas[1], I sniffed out a personal data processing.

Looking at the penultimate article of this regulation one can read that: „the users of POSF [the online platform for end customer to change the electricity and/or natural gas supplier] are required to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, in and in connection with the POSF in relation to CF [end customers'] data and information […]"[2]. I sighed…

Mentioning the General Data Protection Regulation has become a figure of speech, especially in normative administrative acts. Usually such a reference takes the form: „in accordance with the provisions of Regulation (EU) 2016/679", as if this formula had the ability of providing by magic, like a simple rotation of the wand or a ring twist, the protection of natural persons in relation to personal data processing or ensure the implementation of data protection principles.

Driven by a mischievous thought, I decided to ask the personal data controller a question under the free access to information of public interest. As it results from Article 8 (1) of the Regulation on the organization and operation of the online platform, the administrator and controller of the platform will be the National Energy Regulatory Authority (ANRE) – the issuer of the said regulation – and ANRE is an autonomous

* PhD Candidate, Nicolae Titulescu University of Bucharest (Romania); https://orcid.org/0000-0002-9927-1016.

[1] Approved by Article 1 of the President of the National Energy Regulatory Authority Order no. 3 of 26 January 2022, published in the Official Journal of Romania, Part I no. 108 from 3 February 2022.

[2] It is further stated that the obligation to comply with Regulation (EU) 2016/679 exists "both at the time of their introduction [personal data of end customers] in the POSF and in the event that updates are required", hence it follows that the reference to the General Data Protection Regulation seems to take into account only the *principle of data accuracy* provided by Article 5 (1) (d) GDPR, ignoring the rest.

administrative authority[3]. Thus, I asked to be told „which will be the legal basis (provided by Article 6 GDPR) for the processing of end consumers – natural persons – personal data, within the POSF platform".

For my surprise, less than an hour after sending the request, I received a response from the Data Protection Officer within ANRE (he also has the title of „IT Office Expert") who, after confirming receipt of the request[4], stated that: „one of the IT experts will be back shortly with more information". At such times, the easily influenced (and less knowledgeable) start to have doubts about the provisions of Regulation (EU) 2016/679.

According to Article 39 (1) (b) GDPR, the data protection officer (DPO) monitors the compliance with the General Data Protection Regulation, to this end providing the controller with guidance on the demonstration of compliance[5]. As the controller is responsible for complying with the principles relating to processing of personal data, including demonstrating the lawfulness of the processing, it is unnatural that the person who is tasked with assisting the operator in monitoring compliance does not know the answer to a question about the legal basis for processing. This all the more so as Article 37 (5) GDPR states that the DPO is designated on the basis of professional qualities and, *in particular, expert knowledge of data protection law and practices*[6], and the obligation to inform the data subjects, when the platform becomes operational, will include the communication of the legal basis for processing.

Although one cannot deny the contribution of an „IT Office Expert" to the proper implementation of technical and organizational security measures, reducing the DPO to competences that are not fully in line with the wording and spirit of Regulation (EU) 2016/679 is detrimental to any public authority or private body and not without impact on the effective protection of data subjects' rights.

In the heliocentric system of the General Data Protection Regulation, IT systems are not at its core, but the individuals are and their fundamental right to protection in relation to the processing of their personal data. In this respect, Recital (15) GDPR points out that „the protection of natural persons should be technologically neutral and should not depend on the techniques used", so that information technology expertise is not enough (and maybe not even necessary) to qualify as a DPO. Just as a crown does not a king make, a job title does not make a DPO. However, the paper bears anything[7] and so does a business card.

[3] See Article 1 (1) of the Government Emergency Ordinance no. 33 of 4 May 2007 on the organization and functioning of the National Energy Regulatory Authority, published in the Official Journal of Romania, Part I no. 337 from 18 May 2007, with subsequent amendments.

[4] https://servicedesk.intern.anre/Ticket/13923.

[5] In this respect, see Recital (77) GDPR.

[6] See also Recital (97) GDPR which explicitly states that, where the processing is carried out by a public authority, the data protection officer should be „a person with expert knowledge of data protection law and practices [and] should assist the controller or processor to monitor internal compliance with this Regulation".

[7] The remark also concerns the decision of the National Energy Regulatory Authority, as a controller, to designate a data protection officer according to Article 37 (1) (a) GDPR.

Registrul naţional al persoanelor care au comis infracţiuni sexuale, de exploatare a unor persoane sau asupra minorilor din perspectiva protecţiei 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 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 naţional automatizat cu privire la persoanele care au comis infracţiuni sexuale, de exploatare a unor persoane sau asupra minorilor, precum şi pentru completarea Legii nr. 76/2008 privind organizarea şi funcţionarea Sistemului Naţional de Date Genetice Judiciare[1].

Scopul declarat al adoptării acestui act normativ a fost acela al prevenirii şi combaterii faptelor de natură sexuală, de exploatare a unor persoane sau asupra minorilor, prevăzute şi pedepsite de legea penală, precum şi cel de a evita riscul recidivei persoanelor condamnate pentru săvârşirea acestui tip de infracţiuni[2].

Realizarea unei evidenţe naţionale privitoare la persoanele care săvârşesc 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 (FIJAIS)* creat în Franţa în anul 2004 sau *Sex offenders register* (SOR), creat în Regatul Unit al Marii Britanii, în temeiul legislaţiei 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 Act[3], însă diverse reglementări statale, precum cea a statului Washington, prevăd încă din anul 1990[4] norme referitoare la înregistrarea persoanelor ce săvârşesc fapte îndreptate împotriva vieţii sexuale sau a minorilor.

Deşi niciuna dintre aceste reglementări nu a fost ferită de critici, legislaţia 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 protecţiei datelor cu caracter personal. Articolul de faţă îşi propune să supună analizei provocările ce rezultă din incongruenţa reglementărilor.

---

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

[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 şi al antrenării răspunderii penale

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

Normele ce reglementează protecţia datelor cu caracter personal sunt menite să protejeze confidenţialitatea, identitatea, reputaţia şi autonomia persoanelor şi, astfel cum s-a arătat, par a fi (constant) insuficiente pentru a asigura o protecţie adecvată în raport de noi riscuri[5].

De aceea, adaptarea constantă a legislaţiei 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 protecţia datelor* (GDPR sau „Regulamentul") ce a înlocuit Directiva 46 din 1995 privind protecţia datelor. Adoptat ca răspuns la extinderea masivă a procesării de date cu caracter personal de la introducerea Directivei şi respectiv ca răspuns la dezvoltarea unor tehnologii din ce în ce mai intruzive, Regulamentul se bazează pe Directivă şi pe jurisprudenţa Curţii de Justiţie a UE (CJUE) în materie, extinzând în mod semnificativ Directiva şi consolidând în acest fel principalul regim de protecţie a datelor în Uniunea Europeană[6].

Aspecte proprii protecţiei datelor cu caracter personal au devenit instituţii consacrate ale drepturilor omului. Astfel, dreptul de a fi dat uitării[7], consacrat jurisprudenţial de către CJUE în Cauza *Google Spain*[8], este analizat ca o componentă de netăgăduit a dreptului la viaţă privată, inclusiv în jurisprudenţa Curţii 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 ştergerea 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 reţinut ca stare de fapt că în martie 2010, domnul Costeja González, cetăţean spaniol, a formulat o reclamaţie în faţa autorităţii spaniole competente, împotriva societăţii care publica un cotidian de largă difuzare precum şi împotriva Google Spain şi a Google Inc. având în vedere că atunci când se introducea numele său în motorul de căutare al grupului Google erau afişate linkuri către două pagini ale cotidianului La Vanguardia pe care figura un anunţ, în care se menţiona numele său în legătură cu o procedură de vânzare la licitaţie a unor imobile desfăşurată în vederea plăţii unor datorii la asigurările sociale, cu toate că executarea silită în cauză s-a finalizat în întregime în urmă cu mai mulţi ani. El a solicitat să se dispună ca La Vanguardia fie să elimine sau să modifice paginile menţionate 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. şi W.W. c. Germaniei, Hotărârea din 18 iunie 2018, publicată pe https://hudoc.echr.coe.int/fre#{%22languageisocode%22:[%22ENG%22],%22app

Deşi în jurisprudenţa CEDO temenii beneficiază de o autonomie conceptuală proprie, în esenţă componente ale dreptului la viaţă privată dezvoltate în cadrul acestei jurisprudenţe înglobează majoritatea principiilor şi exigenţelor ce decurg din standardele impuse de GDPR. Aceste standarde, devenite componente ale unui drept fundamental, au aptitudinea de a surclasa legislaţia naţională în temeiul dispoziţiilor art. 20 din Constituţie, situaţie 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 GDPR[10], în condiţiile în care Regulamentul general al UE privind protecţia datelor, transpus în dreptul naţional prin Legea nr. 190/2018[11], conţine în art. 10 dispoziţii speciale cu privire la prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni sau la măsuri de securitate conexe. Potrivit reglementării, aceasta se efectuează numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate, iar orice registru cuprinzător al condamnărilor penale se ţine numai sub controlul unei autorităţi de stat[12].

Astfel, cel puţin din perspectiva persoanelor a căror răspundere este antrenată, datele cu caracter personal sunt cunoscute şi pot fi utilizate de către autorităţi, ele servind atât la identificarea corectă a persoanei a cărei răspundere penală urmează a fi angajată cât şi la realizarea unor baze de date precum cazierul judiciar ce în sine nu sunt contrare principiilor de utilizare conformă a datelor[13].

Cu referire la *Registrului naţional al persoanelor care au comis infracţiuni sexuale, de exploatare a unor persoane sau asupra minorilor,* observăm că aparent nu există un concurs de norme aflate în disonanţă în ceea ce priveşte protecţia 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 şi datele judiciare prevăzute la art. 8 alin. (11) şi (13), art. 9 şi 11 din Legea nr. 290/2004, republicată, cu modificările şi completările ulterioare[14]. Cu toate acestea, unele aspecte vor trebui nuanţate, interferenţele nelimitându-se exclusiv la situaţia preluării datelor.

---

no%22:[%2260798/10%22,%2265599/10%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-183947%22]}.

[10] Cel puţin din perspectiva persoanelor a căror răspundere este antrenată. În ceea ce priveşte inculpatul datele sale personale sunt cunoscute şi pot fi utilizate oricând de către autorităţi, 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 şi 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 privinţa altor participanţi, suprapunerile sunt şi mai evidente, iar pentru a exemplifica aceste suprapuneri este îndeajuns să amintim instituţiile procesual penale precum cea a martorului protejat sau protecţia conferită victimelor infracţiunii prin protecţia datelor de identitate.

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

III. Interferenţe

Regulamentul prevede expres dreptul la ştergerea datelor (de a fi uitat) reţinând că persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge 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 îşi retrage consimţământul pe baza căruia are loc prelucrarea şi nu există niciun alt temei juridic pentru prelucrare; persoana vizată se opune prelucrării şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea; datele cu caracter personal au fost prelucrate ilegal; datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se află operatorul; sau datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la art. 8 alin. (1)[15].

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

Cum pentru majoritatea infracţiunilor ce antrenează înscrierea în registru pedeapsa de 5 ani se situează între limitele speciale de pedeapsă, o persoană care săvârşeşte una dintre infracţiunile în discuţie la o vârstă fragedă, va suporta, de principiu pe tot parcursul vieţii sale, consecinţele înscrierii în acest registru.

În aceste condiţii 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 ştergerea acestor date în temeiul art. 17 alin. (1) lit. (a) al Regulamentului.

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

Este de observat că legislaţia stipulează expres că intervenirea graţierii, prescripţiei executării pedepsei, amnistiei sau reabilitării cu privire la persoanele fizice înscrise în Registru nu conduc la scoaterea acestora din evidenţa Registrului[16]. Nu vom argumenta, în contra dispoziţiilor legale, că reabilitarea ar trebui să conducă la ştergerea automată a acestor date. Opţiunea disocierii momentului de la care păstrarea datelor devine inoportună de momentul reabilitării condamnatului ţine de politica penală a statului, cu care, de altfel, prin raportare la natura infracţiunilor, 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 aceşti factori de risc să fie analizaţi. Dacă aceştia subzistă, scopul pentru care au fost colectate sau prelucrate datele este actual, iar ştergerea acestora este inoportună. Dacă scopul nu mai subzistă, menţinerea 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 legislaţia ar trebui să reglementeze o procedură judiciară de eliminare a acestor date. De altfel, CJUE a statuat că o prelucrare iniţial 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 situaţia în special atunci când ele sunt inadecvate, atunci când nu sunt sau nu mai sunt relevante ori sunt excesive în raport cu scopurile respective şi cu timpul care s-a scurs[17].

O altă situaţie ce va ridica serioase probleme în raport de conformitatea cu exigenţele ce decurg din Regulament o reprezintă obligaţia organelor de poliţie de a desfăşura periodic, dar nu mai târziu de o dată la 3 luni, verificări la domiciliu, reşedinţa sau imobilul în care persoanele înscrise în Registru locuiesc efectiv, în scopul obţinerii de date şi informaţii privind comportamentul acestor persoane şi modul de obţinere a mijloacelor de existenţă, precum şi actualizării, după caz, a datelor din Registru sau din celelalte baze de date ale Poliţiei Române[18].

Cu toate că legea prevede că aceste verificări se vor desfăşura în condiţii de confidenţialitate[19], o atare prevedere este mai mult decât utopică. A considera că persoanele de la care astfel de date se obţin[20] nu îşi vor pune problema raţiunii unei asemenea verificări este de neconceput. Cum legislaţia în vigoare nu prevede expres o altă situaţie în care asemenea informaţii să fie obţinute *cu o asemenea regularitate*, confidenţialitatea ar putea fi păstrată doar dacă prezumăm că aceste persoane nu cunosc legislaţia ce impune astfel de verificări.

În mod evident, o atare procedură atrage atenţia societăţii asupra persoanei condamnatului şi asupra împrejurării condamnării sale pentru o infracţiune de natură sexuală, de exploatare a unor persoane sau asupra minorilor, chiar dacă infracţiunea în sine nu este identificată[21].

Scopul normei nu este acela de a stigmatiza persoana condamnatului în societate, aspect ce se deduce cu prisosinţă din împrejurarea că aceste date referitoare la condamnare sunt accesibile unui număr relativ restrâns de persoane, iar nu publicului larg. În acest context, aşteptarea rezonabilă privind viaţa privată există, iar aducerea la cunoştinţa terţilor, chiar indirect, a calităţii de condamnat va constitui o încălcare a vieţii private şi a obligaţiei legale de confidenţialitate prevăzută de art. 12 alin. (4) al Legii nr. 118/2019.

De altfel, aşteptarea rezonabilă privind protecţia vieţii private decurge din chiar stipularea normativă a obligaţiei de confidenţialitate, ce în mod practic apreciem că va fi imposibil de asigurat. Această obligaţie nu trebuie înţeleasă restrictiv, în sensul în care aceasta se referă exclusiv la obligaţia agentului de a nu divulga raţiunea interogării, ci extensiv, prin raportare la necesitatea ca societatea să nu cunoască în niciun mod situaţia condamnatului sau raţiunea verificărilor.

În Jurisprudenţa CJUE s-a reţinut că o prelucrare a unor date referitoare la condamnări poate fi legală, în temeiul dispoziţiilor art. 8 al Directivei şi 10 al

[17] A se vedea cauza *GC and Others*, Hotărârea CJUE din 24 septembrie 2019, disponibilă pe 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.

[18] Această obligaţie este stipulată expres în cuprinsul art. 12 alin. (3) al Legii nr. 118/2019.

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

[20] Prin ipoteză altele decât condamnatul pentru a asigura eficienţa culegerii de date.

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