ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „ALEXANDRU IOAN CUZA" DIN IAȘI
TOMUL LXIV, ȘTIINȚE JURIDICE, 2018, SUPLIMENT

TRANSFERUL TRANSFRONTALIER DE DATE CU CARACTER PERSONAL

TRANSBORDER DATA-FLOW

HORIA ALEXANDRU MODRAN[1]

Rezumat: Acest studiu definește și explică conceptul de transfer transfrontalier de date, abordând, de asemenea, problema transferului de date cu caracter personal către statele terțe în contextul Regulamentului general privind protecția datelor. Transferul transfrontalier de date este una dintre cele mai importante probleme ale legislației privind protecția datelor. În epoca unor rețele complexe, este posibil din punct de vedere tehnic ca o companie să își păstreze datele într-un centru de date străin și, apoi, să le obțină și să le utilizeze fără întârziere. Această posibilitate poate fi exploatată de companii pentru a eluda legislația națională și europeană privind protecția datelor, prin stocarea datelor personale sensibile în centrul de date din străinătate Nevoia de a analiza interesul companiilor pentru transferul datelor în străinătate față de interesul persoanelor vizate în protejarea propriilor date a condus la adoptarea unui cadru de reglementare relativ complex. Cu toate acestea, transferul de date în străinătate continuă să ridice multe probleme, adesea generate de dificultățile legiuitorului de a anticipa diversele scenarii care pot implica transferuri de date în străinătate, precum și de interpretarea diferită a normelor existente de către autorități și practicieni.
Cuvinte cheie: transfer de date transfrontalier, date cu caracter personal, state terțe, regulamentul general privind protecția datelor

Abstract: This study defines and explains the concept of transborder data-flow, addressing as well the problem of the transfer of personal data to third-countries in the context of the General Data Protection Regulation. Cross-border data transfer is one of the central and most important problems of data protection law. In the age of comprehensive networks, it is technically possible for a company to store its data in a foreign data center and, then, to retrieve and use it without any time delay. This possibility can be exploited by companies to circumvent national and European data protection laws by storing all important personal data in foreign data center. The need to ponder companies' interest in transferring data abroad with the data subjects'

[1] Informatician, CSB Bucuresti, email: modranhoria@gmail.com.

interest in protecting their own data has led to the adoption of a relatively complex regulatory framework. However, the transfer of data abroad continues to raise many problems, often generated by the legislator's difficulties to anticipate the various scenarios that may involve data transfers abroad and the different interpretation of existing rules by either authorities and practitioners.
Keywords: transborder data-flow, personal data, third countries, general data protection regulation.

1. Internetul și protecția datelor

Datorită evoluției tehnologice din ultimele două decenii, internetul a devenit devenit tot mai utilizat, iar astăzi peste 55% din populația lumii[2] este conectată la internet și acest număr este în continuă creștere. Pentru mulți oameni, Internetul este încă un loc enigmatic. Limitele sale nu sunt tangibile, iar fundalul tehnic este adesea ascuns utilizatorul. Cu câțiva ani în urmă, cancelarul german Angela Merkel a descris internetul drept "o lume nouă"[3]. Cel puțin din punct de vedere juridic, această afirmație nu este total greșită. Lumea juridică trebuie să se dezvolte în același ritm cu dezvoltarea tehnologică și, chiar dacă juriștii sunt reticenți în a admite acest lucru, uneori nici măcar ei nu reușesc să înțeleagă pe deplin complexitatea internetului. Cu toate acestea, internetul nu este tocmai un loc ferit de aplicarea legilor. Situația juridică este, totuși, încă destul de neclară. În special pentru persoanele fără studii juridice, pare aproape imposibil să se țină seama de evoluțiile juridice din larga sferă desemnată de internet.

Deoarece informația este probabil cel mai valoros element pe care îl deținem în prezent, existența unei legislații adecvată a devenit vitală. Astfel, dreptul tehnologiei informației (IT) este una dintre cele mai tinere discipline juridice. Rădăcinile sale sunt, totuși, încă în întuneric, din cauza lipsei unei limitări clare a conținutului acestei discipline.

Datorită dinamicii legislației privind internetul, unele tendințe în domeniul protecției datelor sunt în curs de dezvoltare. În ceea ce privește legislația referitoare la dreptul internetului, incidentele recente arată clar că este necesară o acțiune de reglementare cât mai strictă. Dar există și reversul medaliei în acest domeniu, respectiv abuzul libertății de exprimare prin discursuri de ură pe internet, fapt ce dovedește necesitatea controlării

[2] Internet World Stats website, [Online] la https://www.internetworldstats.com/stats.htm.

[3] Declarație dată la data de 19.06.2013, în cadrul întrevederii cu președintele american Barack Obama.

opinilor exprimate în mediul online. Din acest motiv, Germania a adoptat Legea pentru îmbunătățirea aplicării legii în rețelele sociale (în lb. germană *Netzwerkdurchsetzungsgesetz*, prescurtat NetzDg)[4], cunoscută ca Legea Facebook, fapt salutat și de Comisia Europeană.

Ubicuitatea internetului ridică probleme mai profunde, cum ar fi punerea în aplicare și executarea cererilor de apărare în justiție în contextul aplicării drepturilor de proprietate intelectuală. De multe ori, intermediarii pot fi făcuți responsabili de problemele de aplicare ale acestuia. De asemenea, în contextul stabilirii de conținut ilegal în *hyperlink*-uri există unele schimbări în ceea ce privește răspunderea, după cum reiese din hotărârea Curții de justiție a Uniunii Europene (denumită în continuare CJUE) din 8 septembrie 2016[5].

În domeniul legislației privind protecția datelor, începând cu luna mai a anului 2018 se aplică Regulamentul General privind Protecția Datelor cu caracter personal (denumit în continuare RGPD)[6], oferind multe inovații în acest domeniu. Problematica centrală este, probabil, legătura dintre legislația privind protecția datelor și alte domenii ale dreptului. Astfel, problemele legate de protecția consumatorilor, probleme de marketing direct și legislația națională privind publicitatea prin telefon și e-mail au ocolit, prin intermediul modelului de *opt-out*, articolul 21 al RGPD. Această problematică este luată în calcul în cadrul unui alt regulament, Regulamentul privind viața privată și comunicațiile electronice[7]. RGPD înlocuiește reglementărilor naționale privind protecția datelor, aplicându-se direct, fără a fi nevoie de transpunere în legislația națională. În ceea ce privește domeniul *big data* și al comunicării de tip *machine to machine*, legislația privind protecția datelor pare cel puțin ineficientă, aici fiind necesare abordări de reglementare ceva mai avansate.

---

[4] Legea 772-8 adoptată de Parlamentul Federal al Germaniei la data de 01.09.2017, intrată în vigoare începând cu data de 01.10.2017.

[5] CJUE, Decizia din data de 08.09.2016 în cazul C-160/15, [Online] la *www.curia.eu*, accesat 07.11.2018.

[6] Regulamentul (UE) 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 95/46/CE (Regulamentul general privind protecția datelor) J.O. L119/04.05.2016.

[7] Propunere de Regulament al Parlamentului European și al Consiliului privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice și de abrogare a Directivei 2002/58/CE (Regulamentul privind confidențialitatea și comunicațiile electronice).

Una dintre principalele probleme este dată de dilema privind cine ar trebui să aibă dreptul de proprietate asupra datelor, precum și cum ar trebui să se deducă dreptul de a dispune de aceste date. O altă problemă este manipularea *blockchain-urilor*[8]. În plus față de anumite avantaje ale acestei tehnologii, cum ar fi de exemplu domeniul *e*-guvernării, aceasta implică și riscuri considerabile pentru protecția datelor, ca în cazul spălării banilor. Rămâne de analizat dacă, în ciuda riscurilor și problemelor considerabile, există și oportunități de dezvoltare juridică.

Regulamentul privind confidențialitatea în mediul electronic este o propunere de regulament privind confidențialitatea comunicațiilor electronice, fiind, de asemenea, și *lex specialis* la Regulamentul general privind protecția datelor. Acesta reglementează tipurile de date din cadrul comunicații electronice care se califică drept date cu caracter personal, precum și cerințele de consimțământ în ceea ce privește utilizarea cookie-urilor. Planificat inițial să intre în vigoare la 25 mai 2018, implementarea acestuia a fost amânată pentru anul 2019.

2. Conceptul de transfer transfrontalier de date

Transferul transfrontalier de date este una dintre problemele cele mai importante ale legislației privind protecția datelor. În epoca unor rețele complexe, este posibil din punct de vedere tehnic ca o companie să își păstreze datele într-un centru de date situat pe teritoriul altui stat și, apoi, să le obțină și să le utilizeze fără întârziere. Această posibilitate poate fi exploatată de companii pentru a eluda legislația națională și europeană privind protecția datelor, prin stocarea tuturor datelor personale sensibile în centrul de date din străinătate. Nevoia de a analiza interesul companiilor pentru transferul datelor în străinătate cu interesul persoanelor vizate în protejarea propriilor date a condus la adoptarea unui cadru de reglementare relativ complex. În prima sa versiune, Directiva 95/46/CE (denumită în continuare Directiva)[9] nu a cunoscut încă această posibilitate și, prin urmare, nu a reglementat-o. În ultimii ani, schimbul transfrontalier de date a devenit o amenințare majoră pentru dezvoltarea unei piețe digitale europene unice.

[8] Un *blockchain* este o listă de înregistrări în continuă creștere, numite blocuri, care sunt legate și securizate cu ajutorul criptografiei.

[9] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, J.O. L281/23.11.1995.

În prezent, aproape toate statele membre ale UE au o legislație privind protecția datelor. Cu toate acestea, structura și aplicarea practică a normelor europene au fost inițial destul de diferite. Acest lucru a creat pericolul apariției unor "oaze de date" speciale, prin care societățile ar putea prelucra în mod sigur datele lor în anumite state, pentru a evita legislația strictă privind protecția datelor din statele lor de proveniență.

Între timp, fluxul transfrontalier de date (engleză *transborder data-flow*) este reglementat atât la nivel european, cât și la nivel național. În conformitate cu articolului 25, alineatul (1), din Directivă, datele cu caracter personal pot fi transmise în țările terțe[10] doar dacă există un "nivel adecvat de protecție". Cu toate acestea, nu este foarte clară definiția acestui nivel de protecție și cum poate fi acesta verificat. Articolul 25, alineatul (2), din Directivă se limitează la a afirma că nivelul adecvat de protecție este "evaluat în funcție de circumstanțe". În general, tipul de date, durata procesării datelor și "normele juridice generale sau sectoriale în vigoare în țara terță în cauză, precum și normele de stat și măsurile de securitate aplicabile acolo" sunt decisive. Comisia Europeană poate decide, printr-o procedură formală, dacă o țară terță garantează nivelul de protecție necesar pentru transmiterea datelor, conform articolului 25 alineatul (4) și articolului 31 alineatul (2) al Directivei.

Regulamentul european privind protecția datelor, care a abrogat Directiva și se aplică începând din 25.05.2018, prevede, de asemenea, reglementări corespunzătoare. Art. 44 din RGPD reglementează principiile generale ale transferului de date. Articolul 45 prevede că datele pot fi transmise numai țărilor terțe cu un nivel adecvat de protecție. Obiectivul său este de a asigura securitatea juridică și uniformitatea în întreaga Uniune Europeană[11]. Conform legislației UE, un nivel de protecție a datelor este considerat adecvat în cazul în care țara terță garantează efectiv un nivel de protecție echivalent cu nivelul de protecție prevăzut în Uniune în temeiul dreptului său național sau al obligațiilor internaționale, astfel încât să fie asigurată continuitatea protecției prevăzute la articolul 8 alineatul (1) din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale[12]. În conformitate cu articolul 45 alineatul (9) din RGPD, constatările privind

[10] Prin stat terț se înțelege orice stat care nu este membru al Uniunii Europene.

[11] Nota 103 din Regulament.

[12] Convenția Europeană privind drepturile omului, ratificată la 04.11.1950, efectivă din data de 03.09.1953

caracterul adecvat definite în temeiul articolului 25 alineatul (6) din Directiva UE sunt menținute pentru moment.

Conform unei decizii definitive a Curții de Justiție a Uniunii Europene[13], furnizarea de date pe o pagină web nu intră sub incidența conceptului de transmitere a datelor conform Directivei UE privind protecția datelor și, prin urmare, nu poate fi calificată drept schimb de date transfrontalier. Catehistul suedez L. Lindqvist a prezentat pe un site privat, "într-un mod plin de umor", 18 persoane care lucrau cu el în biserică, fără a obține consimțământul persoanelor în cauză. Printre informațiile obișnuite prezentate, au existat și câteva date sensibile. Ulterior, a fost inițiată o cauză penală împotriva lor și, în consecință, cazul a ajuns la CJUE. Deși s-au furnizat date personale în conformitate cu articolul 8 alineatul (1) din Directiva 95/46 /CE, Curtea a constatat că nu există o transmitere a datelor către o țară terță atunci când acestea sunt introduse pe internet, conform articolului 25 din Directivă.

În cazuri excepționale, datele pot fi transferate și în țări terțe care nu dispun de un nivel adecvat de protecție. De exemplu, Directiva conține reguli generale de autorizare care justifică transferul de date către o țară terță nesigură (în special consimțământul persoanei vizate, executarea contractului, păstrarea intereselor, transmiterea dintr-un registru public, în măsura în care acestea nu stau în calea unor interese legitime). În afara acestor excepții, transferul este permis doar dacă furnizorul de date oferă suficiente garanții pentru protecția vieții private și a drepturilor fundamentale ale persoanei vizate. Articolului 26 alineatul (2) din Directivă oferă un exemplu de garanții de protecție corespunzătoare soluției contractuale. În continuare, transferul de date către țara terță nesigură este convenit contractual între transmițătorul de date și persoanele vizate sau autoritatea națională de supraveghere În acest din urmă caz, autoritatea de supraveghere competentă autorizează transmiterea.

Directiva permite, de asemenea, transferul de date pe baza unor coduri de conduită, de exemplu în cadrul unui grup global de operare, deși nu sunt trasate modalitățile în care autoritățile de protecție a datelor autorizează astfel de coduri. Există o soluție specială pentru transferul de date în conformitate cu principile "*Safe Harbor*" (obligația de informare,

[13] CJUE, Decizia din data de 06.11.2013 în cazul C-160/15, [Online] la www.curia.eu, accesat 07.11.2018.

alegere, transfer, securitate, integritatea datelor, dreptul la informare și executare). În acest scop, Comisia Europeană a decis în anul 2000, de comun acord cu Statele Unite, acordul "*Safe Harbor*"[14]. Companiile străine au trebuit să adere la acest acord, să se supună regulamentelor și astfel să garanteze nivelul adecvat necesar de protecție a datelor. Nu au fost prevăzute măsuri de control adecvate privind respectarea și implementarea nivelului de protecție a datelor. În decizia sa de referință din 6 octombrie 2015[15], CJUE a invalidat acordul "*Safe Harbor*" din cauza lipsei de competențe a Comisiei Europene de a restrânge competențele autorităților naționale de protecție a datelor și de a încălca dreptul fundamental la viață privată. Începute cu mult timp în urmă, negocierile complexe dintre SUA și Comisia Europeană privind adoptarea unor soluții speciale au continuat. Statele Unite nu dispun de un nivel de protecție a datelor similar cu cel al statelor UE (la fel ca și în cazul Australiei sau Japoniei). Prin urmare, transferul de date din Europa în SUA este, în fapt, interzis. În această situație de urgență, s-a lucrat la dezvoltarea unor modele de contracte care să stabilească relațiile contractuale între organismul care transmite datele și destinatarul din SUA. La mijlocul anului 2001, au fost adoptate două clauze contractuale standard, unul pentru transferul de date cu caracter personal către destinatarii din statele terțe[16] și pentru procesarea acestor date în aceste țări[17].

La 15 mai 2010, au intrat în vigoare noile modele de contracte[18] pentru schimbul transfrontalier de date cu țările care nu fac parte din Uniunea Europeană. Acestea au dus la extinderea activităților de prelucrare a datelor și a unor noi modele de afaceri pentru procesarea internațională a datelor cu caracter personal. Decizia stabilește dispoziții specifice care permit externalizarea activităților de prelucrare către subcontractanți în anumite condiții și protejând în același timp confidențialitatea datelor cu

[14] Decizia Comisiei Europene din 26 iulie 2000 în temeiul Directivei Directiva 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al principiilor "*Safe Harbor*", publicată în Jurnalul Oficial al Comunităților Europene, la 25 august 2000, J.O. L215/25.08.2000.

[15] CJUE, decizia din data de 06.10.2015 în cazul C-362/14, [Online] la *www.curia.eu*, accesat 07.11.2018.

[16] Contract standard din 15.06.2001, [Online] la http://eur-lex.europa.eu/legal-content/ro/ALL/?uri=CELEX:32001D0497, accesat 07.11.2018.

[17] Contract standard din data de 27.12.2001.

[18] Modelele de contract sunt disponibile [Online] la https://ec.europa.eu/info/law/law-topic/data-protection_ro, accesat 07.11.2018.

caracter personal. Ulterior, un importator de date care dorește să subcontracteze lucrările efectuate în numele entității exportatoare de date trebuie să obțină un consimțământ scris prealabil din partea exportatorului de date. Subcontractantul este obligat printr-un acord scris să respecte aceleași obligații pe care importatorul datelor trebuie să le îndeplinească în conformitate cu clauzele contractuale standard. În cazul în care subcontractantul nu respectă obligațiile sale privind protecția datelor, importatorul datelor rămâne în întregime responsabil față de exportatorul de date pentru îndeplinirea obligațiilor acestuia. În plus, subcontractarea include numai activitățile de prelucrare convenite în contractul inițial între exportatorul de date din UE și importatorul de date. Contractele existente încheiate pe baza clauzelor aprobate prin Decizia 2002/16/CE rămân valabile atâta timp cât transferul și activitățile de prelucrare a datelor se mențin în continuare.

Companiile cu sediul în SUA au fost obligate ca, în cazul unui proces iminent, să furnizeze cantități mari de documente stocate electronic, precum e-mailuri, fișiere PDF, foi de calcul, fotografii stocate electronic, etc. Dacă filialele în cauză sunt situate în străinătate, aceștia au obligația, de asemenea, să furnizeze informațiile relevante. Conform principiului "*Litigation Hold*", materialele ce pot fi implicate într-un potențial litigiu nu pot fi șterse atunci când o companie se așteaptă să fie implicată într-un proces. În cazul în care societatea nu respectă aceste obligații extinse de stocare a datelor, aceasta este considerată drept o infracțiune de diminuare a dovezilor, care implică consecințe legale considerabile. În plus, judecătorul american are posibilitatea de a adopta un ordin de interferență neadecvată. Datorită deciziei CJUE privind invalidare acordului Safe Harbor, negocierile dintre Uniunea Europeană și SUA pentru reglementarea transferului transfrontalier de date au fost intensificate. La 2 februarie 2016, s-a ajuns la un acord politic cu privire la Scutul de confidențialitate UE-SUA, ca un nou cadru pentru transmiterea de date, care urmărește remedierea deficiențelor acordului "*Safe Harbor*". La 29 februarie 2016, a fost prezentată o versiune de proiect a scutului de confidențialitate UE-SUA[19]. Schema include cerințe mai stricte pentru întreprinderile din Statele Unite, menite să protejeze datele

[19] Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA, notificată cu numărul C(2016) 4176, J.O. L207/01.08.2016.

cu caracter personal ale cetățenilor UE. Acordul prevede, de asemenea, o restricție privind accesul autorităților americane la datele cu caracter personal transmise în conformitate cu Scutul de confidențialitate UE-SUA, pentru a preveni o supraveghere intensă a acestor date. În plus, cetățenilor UE ar trebui să li se acorde opțiuni juridice extinse de protecție prin posibilitatea de a se adresa unor avocați desemnați și de a-și susține afirmațiile în fața instanțelor americane. La data de 12 iulie 2016, Comisia Europeană a emis o decizie prin care obligă companiile americane să poate prezenta un nivel adecvat de protecție, cu condiția să se angajeze să respecte principiile Scutul de confidențialitate UE-SUA. Începând cu 1 august 2016, companiile din Statele Unite pot să solicite Departamentului de Comerț al SUA certificarea în vederea transferul de date cu caracter personal din UE în Statele Unite. Cu toate acestea, este de așteptat ca admisibilitatea deciziei de adecvare cu privire la Scutul de confidențialitate UE-SUA sa fie, de asemenea, contestată la CJUE. În plus, conform procedurii "*Pre-Trial Discovery*" din Legea privind procedura civilă din SUA, părțile pot solicita informații pertinente de la partea adversă, pentru a fi folosite în cadrul urmăririi penale. În conformitate cu norma 34 din Regulamentul federal al procedurilor civile[20], informația stocată electronic este de asemenea acoperită de acest drept.

Instanțele americane nu cunosc suficient faptul că legea europeană privind protecția datelor ar putea să se opună unei astfel de abordări. Potrivit "*Restatement of Foreign Law Relations*", SUA pot renunța la depunerea documentelor din străinătate. Cu toate acestea, această regulă nu este obligatorie din punct de vedere juridic și nu este întotdeauna aplicată. În plus, statele membre UE nu au apelat, în cadrul Convenția de la Haga, la care Statele Unite ale Americii este parte, la nicio cerere de asistență juridică reciprocă de la Statele Unite bazată pe procedura "*Pre-Trial Discovery*".

Cu toate acestea, transmiterea datelor personale ale părților către instanță este mai permisivă, deoarece documentele depuse în procesele din SUA trebuie să fie puse la dispoziția publicului, la cerere, cu excepția cazului în care sunt afectate secrete de afaceri sau alte interese de nivel superior. În ansamblu, acest lucru ar putea duce la erodarea legislației naționale privind protecția datelor, în cazul în care orice constrângere exercitată de jurisdicții străine asupra companiilor europene va conduce în

[20] Traducerea din engleză a Federal Rules of Civil Procedures (FRCP).

mod automat la transmiterea unor date protejate ale persoane fizice în temeiul legislației naționale.

Pentru a crea un posibil echilibru de interese, fiecare organism responsabil și părțile interesate trebuie să încerce să realizeze o armonie între cele două sisteme juridice conflictuale. Există însă o mare nesiguranță în ceea ce privește încălcarea legislației americane sau a legislației europene privind protecția datelor. Legislația americană, în special Actul privind comunicările stocate din 1986[21] nu autorizează instanțele să ordone eliberarea datelor stocate exclusiv pe serverele din statele terțe. Legea invocată de guvernul Statelor Unite a fost aplicabilă numai datelor stocate în Statele Unite, protejând datele personale ale persoanelor fizice de accesul arbitrar al guvernului. În mod similar, societăților americane nu li se putea cere, chiar și în cazul unui mandat de percheziție adecvat, să furnizeze date stocate în alte state.

3. Schimbul de date transfrontalier în contextul GDPR

Protecția datelor se află la intersecția dintre dreptul de acces ale terților și dreptul exclusiv al persoanei vizate, care se referă, în acest sens, la "dreptul său de a fi singur"[22], la intimitatea sa sau, mai exact, la dreptul său la autodeterminare informațională.

Parlamentului European și Consiliului UE au convenit, în decembrie 2015, asupra unei versiuni comune a unui nou regulament UE privind protecția datelor (RGPD). Un motiv esențial pentru adoptarea unui regulament privind protecția datelor a fost obiectivul de a standardiza legislația din acest domeniu în statele membre ale UE. Spre deosebire de directivă, care trebuia transpusă de statele membre în legislația națională, regulamentul se aplică direct în toate statele membre. Legislațiile naționale existente privind protecția datelor sunt în mare parte înlocuite, în măsura în care RGPD este aplicabil. Dat fiind faptul că RGPD este, în principiu, aplicabil întregului proces de prelucrare a datelor cu caracter personal (cu excepția câtorva zone clar menționate, în special cele referitoare la aplicarea legilor privind securitatea și siguranța națională), părțile mari ale reglementărilor naționale existente sunt înlocuite de acesta. Cu toate acestea, RGPD permite statelor membre un anumit spațiu de manevră pentru a-și

[21] Stored Communications Act, adoptat la 21.10.1986, codificat la Titlul 18, Capitolul 121 §§ 2701-2712 din Codul de Legi al Statelor Unite ale Americii.

[22] Traducerea din engleză a „*the right to be let alone*“.

menține sau a-și retrage propriile reguli. Aceste lucruri sunt permise prin intermediu unor "clauze de deschidere" din regulament. Există o clauză de deschidere foarte cuprinzătoare pentru prelucrarea datelor cu caracter personal pe baza unei obligații legale sau în exercitarea interesului public (articolul 6 alineatul (1) literele (c) și (e), (2) și (3) litera (b) din RGPD). Ulterior, statele membre pot adapta aplicarea regulilor RGPD prin dispoziții mai stricte în aceste domenii de prelucrare a datelor. În consecință, în domeniul prelucrării datelor de către autoritățile publice, normele naționale pot fi aplicate sau nu în mod regulat, dacă conțin dispoziții mai specifice în limitele RGPD. Cu toate acestea, deoarece RGPD conține numai reguli foarte generale privind prelucrarea datelor, este posibil ca părți importante din legile naționale de protecție a datelor să rămână aplicabile.

Regulamentul privind protecția datelor reglementează, de asemenea, transferul datelor care fac obiectul prezentării unor garanții adecvate (articolul 46 alineatul (1) din RGPD).

Și aici, articolul 47 din RGPD în conține o prevedere corespunzătoare cu privire la legile interne obligatorii privind protecția datelor (Reguli corporative obligatorii[23]). Prezentul regulament contrastează cu art. 26 din Directivă, privind regulile corporative obligatorii din punctul de vedere al legii protecției datelor, reprezentând o inovație semnificativă. În schimb, art. 47 RGPD face acum în mod explicit o descriere detaliată a acestor reguli, specificând și cerințele pentru recunoașterea lor juridică.

În plus, pentru prelucrarea datelor în scopuri jurnalistice, științifice, artistice sau literare, scutirile de la normele regulamentului la nivel național sunt posibile atunci când acest lucru necesar pentru a aduce în concordanță dreptul la protecția datelor cu caracter personal cu libertatea de exprimare și de informare (articolul 85 alineatul (2) din RGPD). Dreptul la protecția datelor cu caracter personal trebuie să fie analizat din perspectiva libertății de exprimare și libertății de informare (articolul 85 alineatele (1), (2) din RGPD). De asemenea, există o clauză privind prelucrarea datelor cu caracter personal în contextul ocupării forței de muncă (articolul 88 RGPD). Aici se poate vedea în ce măsură legislatorul național va folosi această flexibilitate, putând recurge la adoptarea unei legi mai stricte privind protecția datelor cu caracter personal.

[23] Regulile corporative obligatorii (engl. *Bindind Corporate Rules*) sunt reguli interne pentru transferul de date în cadrul companiilor multinaționale.

În conformitate cu articolul 99 paragraful 2, RGPD este, din 25 mai 2018, direct aplicabil în toate statele membre ale UE. Noile reglementări au început să producă efecte semnificative, în special asupra companiilor străine ce operează în Europa și care își bazează modelele de afaceri pe analiza datelor cu caracter personal. Cu toate acestea, transmiterea de date către SUA este problematică, deoarece este clasificată de Comisia Europeană drept o țară terță care nu oferă un nivel de protecție a datelor comparabil cu standardele europene, motiv pentru care schimbul de date cu caracter personal a fost bazat inițial pe acord *Safe Harbor*. Acest acord între SUA și UE se baza pe articolul 25 alineatul (6) din Directiva europeană privind protecția datelor. Până în 2015, a fost fundamentul transferului de date cu caracter personal către SUA. Cu toate acestea, acordul "Safe Harbor" a fost abrogat prin hotărârea CJUE din 6 octombrie 2016, în timp ce CJUE consideră că este contrar Cartei Fundamentale a drepturilor Uniunii Europene. Problema dacă transferurile de date se pot baza în continuare pe clauzele contractuale standard ale UE a fost lăsată fără răspuns de CJUE[24]. Totuși, în februarie 2016, Comisia UE a introdus noul scut de confidențialitate UE-SUA și l-a adoptat la 12 iulie al aceluiași an, după ce statele UE au votat în favoarea acesteia, devenind astfel baza pentru schimbul de date cu caracter personal cu SUA. Conținutul acestui scut de confidențialitate include obligația companiilor americane să certifice și să respecte anumite cerințe privind confidențialitatea datelor cu caracter personal. În plus, pentru prima dată au fost create opțiuni de protecție juridică pentru persoanele afectate de companii din SUA, astfel încât să se asigure un nivel adecvat de protecție a datelor, incluzând posibilitatea cetățenilor UE de a acționa în judecată companiile americane.

În cazul în care un controlor sau un procesator de date din afara UE oferă bunuri sau servicii persoanelor din UE, sau supraveghează comportamentul persoanelor din UE, RGPD este aplicabil și în acest caz (articolul 3 alineatul (2) din RGPD). Acesta trebuie apoi să desemneze un reprezentant din cadrul Uniunii Europene, care să acționează ca punct de contact pentru persoanele vizate și autoritățile de supraveghere în ceea ce privește respectarea dispozițiilor RGPD în statul membru în care se află persoanele vizate (articolul 27 din RGPD). Printre altele, obligația de a numi

[24] Clauzele contractuale standard, [Online] la https://ec.europa.eu/info/law/law-topic/data-protection_ro, accesat 07.11.2018.

un reprezentant în cadrul Uniunii nu există în cazul în care prelucrarea datelor are loc doar ocazional sau de către o autoritate publică (articolul 27 alineatul (2) din RGPD). Cu toate acestea, RGPD nu specifică clar ce condiții trebuie să îndeplinească persoanele desemnate ca reprezentanți. În conformitate cu articolul 4 paragraful 17 RGPD, în esență orice persoană fizică sau juridică poate îndeplini această funcție.

Transmiterea către țări terțe sau organizații internaționale poate continua numai dacă Comisia Europeană a stabilit un nivel adecvat de protecție a datelor (articolul 45 din RGPD) sau dacă s-au demonstrat alte garanții adecvate pentru respectarea unui astfel de nivel de protecție a datelor (de exemplu, linii directoare obligatorii ale societății, conform art. 46 RGPD). În plus, este posibilă transmiterea transfrontalieră a datelor prin consimțământul persoanei în cauză. Cu toate acestea, este necesară, în prealabil, o instruire cu privire la riscul posibil (articolul 49 alineatul (1) litera (a) din RGPD). În acest sens, RGPD nu aduce nicio modificare situației juridice actuale.

De asemenea, există reguli extinse și standarde de calitate care trebuie respectate. Prelucrarea trebuie să fie organizată și realizată cu mijloace tehnice adecvate normelor europene de protecție a datelor. În plus, procesatorul inițial al datelor nu poate implica niciun alt procesator de date fără consimțământul persoanei vizate (articolul 28 alineatul (2) din RGPD). Chiar dacă persoana responsabilă și-a dat consimțământul, prelucrătorul inițial rămâne pe deplin răspunzător (articolul 28 alineatul (4) din RGPD). Între procesorul inițial și fiecare procesor suplimentare se aplică aceleași standarde ca și în relația dintre operator și procesorul original (Art. 28, alin. (4) din RGPD).

4. Perspective viitoare

Având în vedere că, în epoca contemporană, se preconizează un rapid progres tehnologic, cadrul legislativ național și internațional trebuie să fie într-o continuă adaptare, pentru a ține pasul cu evoluția tehnologică. Din acest punct de vedere, reforma adusă legislației privind protecția datelor prin adoptarea RGPD a avut un rol important. Strategia privind piața unică digitală prevede și revizuirea Directivei 2002/58/CE („Directiva asupra confidențialității și comunicațiilor electronice") prin adoptarea unui nou regulament privind respectarea vieții private și protecția datelor cu caracter personal în comunicațiile electronice (Regulamentul privind viața privată și

comunicațiile electronice). Acest lucru este necesar în vederea asigurării unui nivel adecvat de protecție al datelor personale ale utilizatorilor serviciilor de comunicații electronice.

Directiva asupra confidențialității și comunicațiilor electronice asigură protecția libertăților și drepturilor fundamentale, în special privind confidențialitatea comunicațiilor, viața privată, și protecția datelor cu caracter personal în cadrul comunicațiilor electronice. De asemenea, aceasta garantează libera circulație a datelor transmise în cadrul comunicațiilor electronice în întreaga Uniune Europeană. De la ultima revizuire, din anul 2009, a Directivei asupra confidențialității și comunicațiilor electronice, s-a petrecut importante schimbări economice și tehnologice. Atât persoanele fizice, cât și cele juridice, folosesc tot mai des serviciile bazate pe internet care permit comunicațiile interpersonale, în locul comunicațiilor tradiționale. Astfel, serviciile de email, de mesagerie, de telefonie prin internet nu intră, de regulă, sub incidența cadrului actual al Uniunii privind comunicațiile electronice, inclusiv a Directivei asupra confidențialității și comunicațiilor electronice. Întrucât directiva nu a ținut pasul cu evoluțiile tehnologice, acest fapt a dus la o lipsă de protecție a comunicațiilor efectuate prin intermediul internetului.

Fiind o lex specialis în raport cu RGPD, această propunere de regulament completează și detaliază prevederile regulamentului referitoare la datele cu caracter personal transmise în cadrul comunicațiilor electronice. Spre deosebire de o directivă, un regulament le permite persoanelor fizice să beneficieze de același nivel de protecție în întreaga Uniune, precum și persoanelor juridice care desfășoară activități transfrontaliere să suporte cheltuieli reduse.

Comunicațiile electronice pot conține informații extrem de sensibile privind utilizatorii implicați în comunicarea respectivă. De asemenea, metadatele provenite din comunicațiile electronice pot dezvălui informații confidențiale cu caracter personal, lucru admis în mod expres de către CJUE[25]. Majoritatea statelor membre au admis, de asemenea, că necesitatea de protecție a comunicațiile reprezintă un drept constituțional distinct. Deși este posibil ca statele membre să adopte anumite politici prin

[25] CJUE, decizia din data de 08.04.2014 în cazurile conexe C-293/12 și C-594/12 (Digital Rights Ireland și Seitlinger și alții), respectiv decizia din data de 21.12.2016 în cazurile conexate C-203/15 și C-698/15 (Tele2 Sverige AB și Secretary of State for the Home Departmen), disponibile [Online] la *www.curia.eu*, accesat 07.11.2018.

care pot garanta că acest drept nu este încălcat, acest fapt nu poate fi atins în absența unor norme ale Uniunii Europene, putând să creeze restricții privind transferul transfrontalier de date cu caracter personal. În plus, pentru a putea fi păstrată coerența cu RGPD, este necesară revizuirea Directivei asupra confidențialității și comunicațiilor electronice și adoptarea de măsuri pentru armonizarea acestor două instrumente. Evoluțiile tehnologice și strategiei europeană privind piața unică digitală au fost argumente solide în favoarea unei acțiuni la nivelul Uniunii. Având în vedere că tehnologiile digitale și internetul nu au frontiere, această problemă nu se limitează doar la nivelul limitelor teritoriale ale unui stat membru. Conform articolului 19, atribuțiile Comitetului European pentru Protecția Datelor sunt extinse, iar mecanismul pentru asigurarea coerenței prevăzut în RGPD se va aplica în cazul disputelor transfrontaliere legate de prezentul regulament, fapt subliniat și de articolul 20.

5. Concluzii

Fiind o problemă centrală a protecției datelor cu caracter personal, transferul transfrontalier de date și modalitatea de folosire a acestor stârnește multe controverse. Acest lucru se datorează în special dificultăților legiuitorului de a anticipa diversele scenarii ale transferurilor de date în străinătate, precum și interpretării diferită a normelor existente.

Având în vedere rapiditatea evoluțiilor tehnologice, cadrul legislativ național și european trebuie să fie într-o adaptare continuă, pentru a ține pasul cu acestea. Noul RGPD reglementează transferul de date atât în cadrul Uniunii Europene, cât și pe cel dintre statele membre și țările terțe, care nu au un nivel adecvat de protecție. Preconizat a intra în vigoare în anul 2019, Regulamentul privind viața privată și comunicațiile electronice detaliază și completează prevederile RGPD referitoare la datele transmise în cadrul comunicațiilor electronice care se încadrează în categoria datelor cu caracter personal.