ANALELE ŞTIINȚIFICE ALE UNIVERSITĂȚII „ALEXANDRU IOAN CUZA” DIN IAŞI
ŞTIINȚE JURIDICE, TOMUL LXIV, 2018, NR. I

PROTECȚIA DATELOR CU CARACTER PERSONAL. ASPECTE DE DREPT EUROPEAN

PROTECTION OF PERSONAL DATA. ASPECTS OF EUROPEAN LAW

ANDRA IFTIMIEI[1]

Rezumat: Odată cu Regulamentul 679 din 2016 și cu Directiva 680 din 2016, protecția datelor cu caracter personal intră într-o nouă eră. Plecând de la variatele decizii ale Curții europene de justiție, dar și de la coordonatele existente ale protecției datelor cu caracter personal (condițiile necesare transferului de date, precum transparența și necesitatea), prin prezentul studiu propunem o analiză dublu direcționată. Pe de o parte, vom aduce în discuție aspecte de drept comparat și aspecte jurisprudențiale, iar de cealaltă parte vom analiza prevederile actelor legislative europene ce vor fi aplicate din 2018, și de această dată prin prisma dreptului comparat (vezi Franța, care deja a elaborat o lege nouă în acest domeniu – legea pentru o republică digitalizată). Elementele de noutate care ne atrag atenția sunt cele referitoare la drepturi nou instituite, cum este cazul dreptului de a fi uitat.
Cuvinte-cheie: date personale; dreptul de a fi uitat; principii; reglementare europeană.

Abstract: With Regulation 679 of 2016 and Directive 680 of 2016, personal data protection enters a new era. Starting from the various decisions of the European Court of Justice, but also from the existing data protection personal data (conditions necessary for the transfer of data, such as transparency and necessity), we propose a double-targeted analysis in this study. On the one hand, we will discuss comparative law issues and jurisprudential issues, and on the other hand we will analyze the provisions of the European legislative acts to be applied from 2018, this time also in terms of comparative law (see France, which has already elaborated a new law in this field - the law for a digitized republic). The novelty elements that draw attention to us are those relating to newly established rights, such as the right to be forgotten.
Keywords: personal data; the right to be forgotten; principles; European regulation.

[1] Asistent universitar dr., Universitatea „Alexandru Ioan Cuza” din Iași, Facultatea de Drept, email: andra.iftimiei@uaic.ro.

1. Aspecte introductive

Individul este o „ființă informatizată”[2]. Catalogate fiind ca substrat al persoanei, drepturile cu caracter personal permit identificarea individuală și socială a fiecăruia dintre noi. Cu toate acestea, identificarea individuală nu se realizează exclusiv prin datele cu caracter personal. Spre exemplu, dreptul la nume[3], primordial și esențial în identificarea individului, nu este considerat un drept cu caracter personal[4]. Carta drepturilor fundamentale[5], în articolul 8, prevede că aceste date cu caracter personal trebuie utilizate în limite bine determinate și, în mod obligatoriu, având consimțământul persoanei vizate, aceasta din urmă dispunând de un drept de acces, dar și de modificare a datelor ce îl vizează.

Tehnologizarea și informatizarea vieții individului sunt structuri evolutive cu duble implicații: pozitive, în sensul în care accesul la informație este mult facilitat, iar comunicarea transfrontalieră a devenit dependentă de mijloace informatice. Implicațiile negative sunt de la cele mai simple (orice conectare la internet sau orice navigare pe internet lasă urme – abandonarea voluntară sau nu a propriilor date personale), la cele complexe, cu implicații penale (hackering, cybercrime, cyberterorism etc.).

Protecția datelor cu caracter personal nu reprezintă o preocupare europeană și internațională chiar de ultim deceniu, ci a suscitat interes chiar din anii '70. Primele state europene care au consacrat legislativ protecția datelor cu caracter personal au fost Franța, Germania și Suedia[6]. Germania a debutat printr-o reglementare care proteja fișierele, Suedia a legiferat în 1973 *datalag*-ul, iar Franța a legiferat, mai întâi, condiții mai stricte pentru sectorul public, în privința datelor cu caracter personal[7].

La nivel internațional există o serie de documente care vizează protecția datelor cu caracter personal.

---

[2] J. Frayssinet, *La protection des données personnelles* în *Droit de l'informatique et de l'Internet* coord. De A. Lucas, J. devèze și J. Frayssinet, PUF, 2001, prima parte, nr. 10.

[3] Dreptul la nume, grație interpretării extensive a articolului 8 din Convenția europeană a drepturilor omului, este considerat parte a dreptului la viață privată și familial (J. F. Renucci, *Droit européen des droits de l'homme*, ed. a doua, L.G.D.J., Paris, 2012, p. 272).

[4] J. C. Saint-Pau (dir.), *Droits de la personnalité*, ed. Lexis Nexis, Paris, 2013, p. 548.

[5] Carta a fost concepută și semnată în anul 2000, iar ulterior a fost integrată Tratatului de la Lisabona din anul 2009.

[6] J. C. Saint-Pau (dir.),*op. cit.*, p. 552.

[7] *Ibidem.*

Organizația de cooperare și dezvoltare economică (OCDE) a enunțat, la începutul anilor 1980, liniile directoare privind stocarea și transferul datelor personale[8], care au devenit norme minimale comune de protecție, dar și sursă de inspirație pentru diferite legislații naționale[9].

Dinamica dreptului european. Acte legislative noi

Cadrul legislativ european se află într-o continuă dinamică, iar domeniul protecției datelor cu caracter personal se află în centrul preocupărilor ce țin de politicile europene. Astfel, prin dinamica dreptului european în domeniul protecției datelor cu caracter personal înțelegem necesitatea actualizării legislative, ținând cont însă de principiile care stau la baza acestui domeniu.

Principii care guvernează respectarea datelor cu caracter personal

Cele șapte principii cheie care vizează protecția datelor cu caracter personal sunt următoarele[10]:

Principiul finalității

Datele cu caracter personal trebuie să fie întrebuințate pentru un scop bine determinat și legal. Potrivit articolului 6 alin. (1) din Regulamentul nr. 679/2016, prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții: persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice; prelucrarea este necesară pentru

---

[8] *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, disponibile la adresa http://www.oecd.org/fr/internet/ieconomie/lignesdirectricesregissantlaprotectiondelavieprivee etlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm, document consultat la data de 7 noiembrie 2017.

[9] Conștientizarea, la nivel legislativ, a necesității protecției datelor cu caracter personal a survenit într-un ritm diferit în statele europene. Dacă, spre exemplu, Franța a făcut primii pași în anii 1970, România a făcut primul pas în anul 2002 prin Ordinul Avocatului Poporului, nr. 75 din 4 iunie 2002 (disponibil la http://www.dataprotection.ro/servlet/ViewDocument?id=860), iar legislativ, târziu, în anul 2009, prin Legea 238 din 10 iunie 2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice (disponibilă la http://www.dataprotection.ro/servlet/ViewDocument?id=575).

[10] http://www.cil.cnrs.fr/CIL/spip.php?article1390, consultat la data de 22 noiembrie 2017.

executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract; prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului; prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice; prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul; prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Principiul proporționalității

Proporționalitatea este unul dintre principiile fundamentale ale dreptului european, astfel că nici domeniul protecției datelor personale nu iese din sfera aplicabilității acestuia. În acest sens, proporționalitatea presupune că trebuie înregistrate și stocate doar acele date care servesc unui scop legitim și bine definit. Protecția dreptului fundamental la respectarea vieții private la nivelul Uniunii impune ca derogările de la protecția datelor cu caracter personal și limitările acesteia să fie efectuate în limitele strictului necesar[11].

[11] Cauza CJUE C-73/16 din 27 septembrie 2017, consultată la data de 24 noiembrie 2017, la pagina web http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62016CJ0073&rid=4. În fapt, întrucât considera că este victima unei atingeri aduse drepturilor sale referitoare la personalitate prin înscrierea numelui său în lista în litigiu, domnul Puškár a solicitat Najvyšší súd Slovenskej republiky (Curtea Supremă a Republicii Slovace), printr-o acțiune introdusă la 9 ianuarie 2014, urmată de o acțiune introdusă la 19 noiembrie 2014, să oblige Direcția finanțelor, toate birourile de impozite subordonate acesteia și Biroul de combatere a criminalității financiare să nu înscrie numele său în lista în litigiu sau în orice altă listă similară, precum și să elimine orice mențiune care îl privește de pe aceste liste și din sistemul informatic al administrației financiare.

Potrivit domnului Puškár, Direcția finanțelor și Biroul de combatere a criminalității financiare au întocmit și utilizează lista în litigiu, care, potrivit indicațiilor domnului Puškár, cuprinde numele a 1227 de persoane fizice pe care autoritățile publice le desemnează prin expresia „biele kone” („cai albi”). Această expresie ar fi utilizată pentru a desemna o persoană care servește drept interpus pentru a ocupa funcții de conducere. Fiecare persoană fizică ar fi în principiu legată, cu numărul său personal de identificare și cu un număr de identificare fiscală, de una sau de mai multe persoane juridice, în număr total de 3369 potrivit indicațiilor

Principiul pertinenței datelor

Datele cu caracter personal trebuie să fie adecvate, pertinente şi să nu fie excesive raportat la scopul pentru care sunt utilizate.

Principiul duratei limitate pentru păstrarea datelor

Expresie a dreptului de a fi uitat, drept nou introdus prin noua reglementare europeană, principiul duratei limitate pentru păstrarea datelor presupune imposibilitatea stocării datelor pentru o durată nelimitată. Durata de păstrare trebuie stabilită în funcție de finalitate fiecărui fişier de stocare.

Principiul securității şi confidențialității

Securitatea şi confidențialitatea datelor cu caracter personal incumbă persoanei care le utilizează sau le administrează. Persoana responsabilă trebuie să ia toate măsurile în scopul împiedicării divulgării datelor cu caracter personal. Astfel: datele stocate nu pot fi consultate decât de către serviciile abilitate să le acceseze; responsabilul cu gestionarea datelor trebuie să ia toate măsurile pentru a împiedica posibilitatea ca datele să fie deteriorate sau ca terții neautorizați să le acceseze. Măsurile de securitate trebuie să vizeze, spre exemplu, copii de siguranță ori schimbarea frecventă a parolei de acces, după cum aceste măsuri de securitate trebuie să fie adaptate la natura datelor, precum şi la riscurile prezentate.

Principiul securității şi confidențialității vizează şi un aspect secundar, respectiv cel al supravegherii transferului datelor cu caracter personal. Astfel, autoritățile naționale de supraveghere, sesizate de o persoană cu o cerere de protecție a drepturilor şi libertăților sale în ceea ce privește prelucrarea datelor cu caracter personal care o privesc, trebuie să poată examina, în condiții de independență deplină, dacă transferul acestor date respectă cerințele stabilite de directiva menționată. În caz contrar, persoanele ale căror date cu caracter personal au fost sau ar putea fi transferate către țara terță respectivă ar fi private de dreptul, garantat la articolul 8 alineatele (1) şi (3) din cartă, de a sesiza autoritățile naționale de supraveghere cu o cerere în vederea protecției drepturilor lor fundamentale[12].

---

domnului M. Puškár, în cadrul căreia sau al cărora aceasta şi-ar îndeplini funcțiile pe o perioadă determinată.

[12] Cauza C-362/14 CJUE din 6 octombrie 2015, consultată la data de 29 noiembrie 2017, pe pagina web http://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1512047095116&uri=CELEX:62014CJ0362. În fapt, Domnul Schrems, resortisant austriac având reședința în Austria, este utilizator al rețelei sociale Facebook (denumită în continuare „Facebook") din anul 2008. Orice persoană care are

Principiul transparenței

Adesea invocat în jurisprudența Curții europene de justiție, principiul transparenței presupune garantarea prin lege a posibilității persoanei de a primi informațiile necesare privitoare la tratamentul aplicat

reședința pe teritoriul Uniunii și care dorește să utilizeze Facebook trebuie să încheie, la momentul înscrierii sale, un contract cu Facebook Ireland, filială a Facebook Inc., stabilită ea însăși în Statele Unite. Datele cu caracter personal ale utilizatorilor Facebook care au reședința pe teritoriul Uniunii sunt, în tot sau în parte, transferate către servere aparținând Facebook Inc., situate pe teritoriul Statelor Unite, unde fac obiectul unei prelucrări. La 25 iunie 2013, domnul Schrems a sesizat Comisarul cu o plângere prin care îi solicita în esență acestuia să își exercite competențele statutare interzicând Facebook Ireland să transfere datele sale cu caracter personal către Statele Unite. În cadrul plângerii, invoca faptul că dreptul și practicile în vigoare în țara menționată nu garantau o protecție suficientă a datelor cu caracter personal stocate pe teritoriul său împotriva activităților de supraveghere practicate de autoritățile publice în această țară. Domnul Schrems se referea în această privință la dezvăluirile făcute de domnul Edward Snowden cu privire la activitățile serviciilor de informații din Statele Unite, în special cele ale National Security Agency (denumită în continuare „NSA"). Considerând că nu era obligat să deschidă o investigație cu privire la faptele denunțate de domnul Schrems în plângerea sa, Comisarul a respins plângerea menționată ca fiind nefondată. Acesta a estimat astfel că nu existau dovezi că NSA ar fi avut acces la datele cu caracter personal ale persoanei interesate. Comisarul a adăugat că motivele formulate de domnul Schrems în plângerea sa nu puteau fi invocate în mod util, dat fiind că orice problemă referitoare la caracterul adecvat al protecției datelor cu caracter personal în Statele Unite trebuia să fie soluționată în conformitate cu Decizia 2000/520 și că, în această decizie, Comisia constatase că Statele Unite ale Americii asigurau un nivel adecvat de protecție. Domnul Schrems a introdus o acțiune la High Court (Înalta Curte de Justiție) împotriva deciziei în discuție în litigiul principal. După ce a examinat probele prezentate de părțile din litigiul principal, această instanță a constatat că supravegherea electronică și interceptarea datelor cu caracter personal transferate din Uniune către Statele Unite răspundeau unor scopuri necesare și indispensabile pentru interesul public. Instanța menționată a adăugat însă că dezvăluirile făcute de domnul Snowden demonstraseră că NSA și alte organe federale săvârșiseră „excese considerabile". Or, potrivit aceleiași instanțe, cetățenii Uniunii nu ar dispune de niciun drept efectiv de a fi ascultați. Supravegherea acțiunilor serviciilor de informații ar fi efectuată în cadrul unei proceduri secrete și necontradictorii. Odată ce datele cu caracter personal sunt transferate către Statele Unite, NSA și alte organe federale, cum ar fi Federal Bureau of Investigation (FBI), ar putea avea acces la aceste date în cadrul supravegherii și interceptărilor nediferențiate pe care aceștia le practică pe scară largă. High Court (Înalta Curte de Justiție) a constatat că dreptul irlandez interzice transferul datelor cu caracter personal în afara teritoriului național, cu excepția cazurilor în care țările terțe în discuție asigură un nivel adecvat de protecție a vieții private, precum și a drepturilor și libertăților fundamentale. Importanța dreptului la respectarea vieții private și a dreptului la inviolabilitatea domiciliului, garantate de Constituția irlandeză, ar impune ca orice ingerință în aceste drepturi să fie proporțională și conformă cu cerințele prevăzute de lege.

propriilor date cu caracter personal, după cum i se asigură acestuia posibilitatea controlului personal. Persoana responsabilă cu gestionarea datelor cu caracter personal trebuie să avertizeze persoana vizată cu privire la colectarea acestor date, iar în caz de transmitere a datelor către terți, să avertizeze persoana vizată. Curtea a statuat că transparența este un interes legitim[13], prin interes legitim putând înțelege chiar că interesul unui terț în obținerea informațiilor cu caracter personal ale unei persoane care a produs daune unui bun aflat în proprietatea sa pentru a acționa în justiție respectiva persoană în vederea obținerii de despăgubiri poate fi calificat ca fiind un interes legitim[14].

Principiul respectării dreptului persoanelor

Acest principiu presupune la rândul lui trei componente: informarea celor interesați, dreptul de acces şi de modificare, dreptul la opoziție.

Prima componentă, informarea celor interesați, presupune ca în momentul în care persoana accesează servicii informatizate sau dacă datele sunt colectate prin intermediul unor chestionare, utilizatorii vizați trebuie să fie informați cu privire la: finalitatea colectării datelor, caracterul obligatoriu sau facultativ al cererii, destinatarii datelor şi modalitatea exercitării drepturilor care le incumbă (dreptul de acces şi de rectificare, dreptul de a face opoziție).

[13] Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke şi Eifert.

[14] Cauza C-13/16 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde împotriva Rīgas pašvaldības SIA „Rīgas satiksme”. Situația de fapt era următoarea: Un șofer de taxi și-a oprit vehiculul pe marginea carosabilului în Riga. La momentul la care un troleibuz aparținând Rīgas satiksme (denumită în continuare „intimata”) a trecut prin dreptul taxiului, un pasager care se afla în taxi a deschis brusc ușa. A urmat o coliziune care a condus la avarierea troleibuzului. Rīgas satiksme a solicitat poliției (denumită în continuare „recurenta”) să dezvăluie identitatea pasagerului. Ea intenționa să formuleze o acțiune civilă împotriva acestuia pentru repararea prejudiciului produs prin avarierea troleibuzului. Poliția a comunicat Rīgas satiksme numai numele pasagerului. Aceasta a refuzat să comunice numărul actului de identitate și domiciliul. În acest context factual, instanța de trimitere solicită să se stabilească dacă articolul 7 litera (f) din Directiva 95/46/CE (denumită în continuare „directiva”) 2 impune obligația dezvăluirii tuturor datelor cu caracter personal necesare pentru inițierea unei proceduri civile împotriva persoanei suspectate de săvârșirea unei contravenții. De asemenea, se întreabă dacă răspunsul la această întrebare ar fi diferit în cazul în care persoana respectivă ar fi minoră.

Dreptul de acces şi de rectificare presupune că persoana vizată poate solicita orice informație care o vizează, după cum are dreptul de a rectifica sau de a solicita ștergerea informațiilor eronate.

Dreptul de a face opoziție presupune că orice persoană are dreptul de a face opoziție, pentru motive legitime, la posibilitatea ca datele să fie stocate într-un fişier informatic, cu excepția situației în care stocarea nu prezintă caracter obligatoriu.

2.2. Acte legislative noi

La nivelul anului 2016, au fost elaborate două acte legislative noi, din necesitatea resimțită pe planul digitalizării fiecărui stat membru în parte. Mai mult decât atât, s-a simțit nevoia actualizării directivei din anul 1995, urmare a creșterii politicilor de securitate.

Directiva 95/46 din 24 octombrie 1995 avea ca principal scop armonizarea legislațiilor diferitelor state membre. Însă, nivelul armonizării procedurilor şi sancțiunilor între statele membre nu era încă atins. Astfel, vor intra în vigoare două documente noi, respectiv Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)[15] şi Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului[16].

Prin analiza celor două documente, ne propunem să evidențiem câteva aspecte care prezintă relevanță pentru dinamica dreptului european, accentul fiind pus pe aspectele legislative noi și impactul acestora în dreptul național.

---

15 http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679, consultat la data de 23 noiembrie 2017.

16 http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L0680, consultat la data de 23 noiembrie 2017.

O primă observație este legată de textul Regulamentului. Conform principiului (1) din Regulament „protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal reprezintă un drept fundamental". Drepturile fundamentale sunt cele care sunt declarate ca atare fie prin declarații de drepturi, fie prin legile fundamentale ale statului. O scurtă privire asupra Constituției României arată că nu este consacrat un astfel de drept în catalogul drepturilor fundamentale, astfel că asistăm fie la necesitatea manifestării fenomenului de constituționalizare[17] cu privire la acest drept, fie admitem existența, și în spațiul național, a ideii de „bloc de constituționalitate"[18], astfel cum este aceasta definită în spațiul francez. În ambele cazuri, subliniem faptul că se întregește cea de-a treia generație de drepturi[19].

Principalele elemente de noutate constau în consacrarea unor drepturi pentru cel căruia i se conferă protecția datelor cu caracter personal. Sunt astfel de drepturi enunțate de Regulament[20]: dreptul de acces la datele colectate și dreptul de informare[21]; dreptul de rectificare[22]; dreptul la opoziție[23]; dreptul de a fi uitat[24]; dreptul la restricționarea prelucrării[25]; dreptul la portabilitatea datelor[26], drept care permite persoanei posibilitatea de a-și recupera datele în scopul transmiterii acestora către o altă persoană însărcinată cu gestionarea lor (acest drept permite persoanei îndreptățite să schimbe oricând pe cel care se ocupă cu gestionarea datelor personale).

[17] Pentru detalii privind fenomenul de constituționalizare a dreptului, a se vedea A. Iftimiei, *Constituționalizarea în dreptul penal român și francez,* ed. Universul Juridic, București, 2016.

[18] Pentru detalii privind noțiunea de „bloc de constituționalitate" în Franța, a se vedea P. Pactet, F. Mélin-Soucramanien, *Droit constitutionnel*, ediția 29, ed. Dalloz, Paris, 2010, pp. 534-537.

[19] Un astfel de drept se înscrie în cea de-a treia generație de drepturi, alături de drepturile ce privesc progresul științific sau biomedicina.

[20] Capitolul III din Regulament – „Drepturile persoanei vizate".

[21] Articolul 15 din Regulament.

[22] Articolul 16 din Regulament.

[23] Articolul 21 din Regulament.

[24] Articolul 17 din Regulament.

[25] Articolul 18 din Regulament.

[26] Articolul 20 din Regulament.

Dreptul la ștergerea datelor („dreptul de a fi uitat”) este consacrat astfel odată cu decizia C-131/12 Google Spania[27] în cuprinsul căreia este precizat că dreptul de a fi uitat este parte componentă a dreptului la viață privată[28]. Mai mult decât atât, din cuprinsul deciziei reiese că „dreptul de a fi

[27] http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62012CJ0131&from=FR, consultat la data de 25 noiembrie 2017.

[28] Situația de fapt era următoarea: La 5 martie 2010, domnul Costeja González, cetățean spaniol cu domiciliul în Spania, a formulat o reclamație la AEPD împotriva La Vanguardia Ediciones SL (denumită în continuare „La Vanguardia”), care publică un cotidian cu difuzare largă, în special în Catalonia (Spania), precum și împotriva Google Spain și a Google Inc. Această reclamație se întemeia pe faptul că, atunci când un utilizator de internet introducea numele domnului Costeja González în motorul de căutare al grupului Google (denumit în continuare „Google Search”), se afișau linkuri către două pagini ale cotidianului La Vanguardia și, respectiv, din 9 martie 1998, pe care figura un anunț, în care se menționa numele domnului Costeja González, cu privire la o vânzare la licitație a unor imobile asociată unei proceduri de executare silită desfășurate în vederea plății unor datorii la asigurările sociale. Prin această reclamație, domnul Costeja González a solicitat, pe de o parte, 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, fie să utilizeze anumite instrumente puse la dispoziție de motoarele de căutare pentru a proteja aceste date. Pe de altă parte, a solicitat să se dispună ca 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 și să nu mai figureze în linkuri ale La Vanguardia. Domnul Costeja González a afirmat în acest context că executarea silită al cărei obiect a fost s-a finalizat în întregime în urmă cu mai mulți ani și că menționarea acesteia este în prezent lipsită de orice relevanță. 16 Prin decizia din 30 iulie 2010, AEPD a respins reclamația menționată în măsura în care privea La Vanguardia, apreciind că publicarea de către aceasta a informațiilor în cauză era justificată din punct de vedere legal, dat fiind că a avut loc la ordinul Ministerului Muncii și Afacerilor Sociale și a avut ca scop să confere vânzării la licitație publică o publicitate maximă pentru a reuni un număr cât mai mare de licitanți. În schimb, respectiva reclamație a fost admisă în măsura în care era îndreptată împotriva Google Spain și a Google Inc. AEPD a considerat în această privință că operatorii de motoare de căutare sunt supuși legislației în materie de protecție a datelor, dat fiind că realizează o prelucrare a datelor pentru care sunt răspunzători și că acționează în calitate de intermediari ai societății informaționale. AEPD a apreciat că este abilitată să dispună ca operatorii de motoare de căutare să retragă datele și să interzică accesul la anumite date în cazul în care ea consideră că găsirea și difuzarea lor pot aduce atingere dreptului fundamental la protecția datelor și demnității persoanelor în sens larg, ceea ce ar include și simpla voință a persoanei interesate ca datele respective să nu fie cunoscute de terți. AEPD a considerat că această obligație poate incumba direct operatorilor de motoare de căutare, fără a fi necesară ștergerea datelor sau a informațiilor de pe site-ul web pe care figurează, în special în cazul în care menținerea acestor informații pe site-ul respectiv este justificată printr-o dispoziție legală. Google Spain și Google Inc. au introdus două acțiuni

uitat", prevalează asupra intereselor legitime ale operatorului unui motor de căutare și asupra interesului general privind libertatea de informare.

Regulamentul prevede un drept și o obligație corelativă: „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 în cazul în care se aplică unul dintre următoarele motive: 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 prelucrareași 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 sau persoana vizată se opune prelucrării; 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; datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale.

Limitele acestui „drept de a fi uitat" au în vedere posibilitatea de a nu da curs solicitării de ștergere a datelor cu caracter personal, în măsura în care prelucrarea este necesară: (a) pentru exercitarea dreptului la liberă exprimare și la informare; (b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul; (c) din motive de interes public în domeniul sănătății publice; (d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau

separate împotriva deciziei menționate la Audiencia Nacional, care au fost conexate de aceasta. Instanța respectivă arată în decizia de trimitere că aceste acțiuni ridică problema obligațiilor care incumbă operatorilor de motoare de căutare în ceea ce privește protecția datelor cu caracter personal ale persoanelor interesate care nu doresc ca anumite informații, publicate pe site-urile web ale unor terți și conținând datele lor cu caracter personal care permit asocierea acestor informații cu aceste persoane, să fie găsite, indexate și puse la dispoziția utilizatorilor de internet în mod nedefinit. Soluționarea acestei probleme ar depinde de modul în care trebuie interpretată Directiva 95/46 în contextul acestor tehnologii, care au apărut după publicarea sa.

istorică ori în scopuri statistice, sau (e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

O altă noutate adusă în discuție prin Regulament este cea privitoare la introducerea unui principiu de răspundere a operatorului de date datelor, responsabil care trebuie astfel să efectueze un autocontrol intern. Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu dispozițiile regulamentului[29].

Două elemente noi reies din articolul 25 al Regulamentului[30]. Conform acestuia „ (1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate. (2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane". Practic, sunt implementate două metode noi, denumite generic *privacy by design* pentru alineatul (1), adică punerea în aplicare, de la momentul conceperii, de tehnologii organizaționale care să permit respectarea Regulamentului și *privacy by default*, care presupune colectarea doar a datelor cu caracter personal necesare prelucrării.

[29] Articolul 24 din Regulament – *Responsabilitatea operatorului.*

[30] *Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit*.

Concluzii

Datele cu caracter personal sunt parte integrantă din identitatea fiecărui individ în parte. Preocuparea pentru o politică mai concentrată de protejare a datelor personale este pe deplin justificată, astfel că dinamica dreptului european se afișează ca o realitate evolutivă firească. Jursiprudența menționată în cuprinsul articolului reprezintă exemple de încălcare a regimului de protecție a datelor cu caracter personal.

Crearea de noi drepturi, recunoscute individului ca titular de date cu caracter personal, alături de instituirea unui regim de răspundere operatorului de date sunt mijloace de prevenție, care au menirea să evite aspectele represive, de drept penal, ca *ultima ratio.*

În același context, al datelor personale conexate cu dreptul penal, Directiva impune ca autoritățile de aplicare a legii să facă o distincție clară între datele diferitelor categorii de persoane, inclusiv: cele în privința cărora există motive serioase să se creadă că au săvârșit sau că urmează să săvârșească o infracțiune; cele care au fost condamnate pentru săvârșirea unei infracțiuni; victimele unor infracțiuni sau persoanele în privința cărora există motive să se creadă că ar putea fi victimele unor infracțiuni; cele care sunt părți care au legătură cu infracțiunea, inclusiv potențialii martori.

Din perspectiva dreptului european, rămâne în discuție modalitatea de implementare a directivei 680/2016 în fiecare stat membru în parte. Franța a făcut deja primul pas în acest sens. Prin implementarea directivei, țările UE trebuie să stabilească termene pentru ștergerea datelor cu caracter personal sau pentru o revizuire periodică a necesității de stocare a acestor date.

Regulamentul 679/2016 vizează o armonizare legislativă direcționată cu precădere spre crearea unui spațiu de securitate și de garantare a protejării datelor cu caracter personal, cu aplicarea principiului egalității, pentru fiecare dintre resortisanții spațiului european.