Dreptul la protecţia datelor cu caracter personal: esenţă şi conţinut

Veronica MOCANU,
doctor în drept, lector universitar
Facultatea de Drept, USM

Sumar

Pornind de la ideea prevenirii apariţiei si dezvoltării confuziilor în ceea ce priveşte utilizarea şi interpretarea normelor de protecţie a datelor cu caracter personal, în cadrul acestui articol ne propunem să stabilim limitele dreptului de protecţie a datelor cu caracter personal, să clarificăm conţinutul şi esenţa dreptului de protecţie a datelor cu caracter personal, ca o categorie juridică şi o prerogativă a cetăţeanului. Nu poate fi realizat un drept, dacă nu-i cunoşti esenţa. Deci, în cadrul acestui articol vom încerca să punem în discuţie importanţa şi valoarea dreptului de protecţie a datelor cu caracter personal şi să explicăm atribuţiile părţilor implicate în prelucrarea datelor cu caracter personal.

Cuvinte-cheie: *date cu character personal, informaţii, utilizare, computer, cadru legal.*

Summary

The data protection right: essence and content

Starting from the idea to prevent the apparition and development of confusion in use and in interpretation of data protection norms, by this article, we proposed to establish the limits of data protection right and clarify the content and essence of the data protection right like a legal category and prerogative of citizen. You can not realize a right if you do not know the essence of it. So, by this article we try to discuss the importance and the value of data protection right and explain the duties of parts involved in processing of personal data.

Key-words: *personal dates, informations, use, computer, legal framework* .

Problema protecţiei datelor este una destul de mediatizată în ultimul timp, însă nu totdeauna subiectul vizat este abordat cu deplină cunoştinţă de cauză. Mai mult ca atât, fără a înţelege esenţa deplină a instituţiei, mulţi dintre funcţionarii implicaţi în activităţi de gestionare a informaţiei încearcă să jongleze cu interpretări juridice, creându-şi un paravan după care să se ascundă atunci când li se cere furnizarea informaţiei.

Pornind de la ideea depistării confuziilor în abordare şi în scopul preîntâmpinării statornicirii unei practici de aplicare greşite, prezentăm articolul dat cu titlu de identificare a limitelor dreptului la protecţia datelor cu caracter personal şi clarificare a conţinutului şi esenţei acestuia drept categorie juridică şi prerogativă a cetăţeanului.

Dreptul la protecţia datelor cu caracter personal este un drept recent instituit în legislaţia Republicii Moldova, fapt ce implică deficienţe în realizare şi exercitare. În plan european însă respectivul drept a căpătat deja recunoaşterea de drept fundamental prin includerea prevederilor de reglementare a acestuia în art. 8 al Cartei Drepturilor Fundamentale a Uniunii Europene.

Evoluţia dreptului la protecţia datelor cu caracter personal este strâns legată de dezvoltarea tehnologiilor informaţionale. Dreptul la protecţia datelor cu caracter personal se impune ca un instrument de ofensivă în lupta cu riscurile aduse de societatea informaţională individului şi ca o posibilitate de control asupra activităţilor de prelucrare a datelor cu caracter personal.

Colectarea, stocarea şi prelucrarea informaţiei despre oameni nu este un fenomen nou. Activitatea de colectare şi înregistrare a datelor despre indivizi este una explorată pe larg pe tot parcursul dezvoltării omenirii. Imperiul Roman, spre exemplu, deţinea o amplă bază de date cu referire la numărul populaţiei, ocupaţia acesteia, proprietate, liste de impozite ş.a. La fel şi Whiliam I al Angliei a dispus în 1086 colectarea informaţiei despre cetăţenii săi, astfel, la ordinul acestuia, au început înregistrările în Domesday Book [1].

[1] Wayne M. Handbook of Personal Data Protection. New York: Stockton Press and Basingstoke, Hants: Macmillan Publishers Ltd, 1992. 1048 p.

După Madsen, „colectarea datelor personale despre cetăţenii unei ţări străine este primul şi cel mai important pas în cucerirea acestora". O materializare clară a ideilor lui Madsen sunt înregistrările datelor cu caracter personal din fişierele SD (Sicherheistsdientst) – fişierele Serviciului de Securitate al Germaniei Naziste. Pe lângă cucerirea teritoriilor, în sarcina armatei naziste era pusă obligaţia de colectare a informaţiei despre populaţia cucerită. După invadarea Danemarcei, Norvegiei, Irlandei, Belgiei, Luxemburgului, Franţei, în Germania se constituie un departament specializat a cărui activitate era îndreptată direct spre colectarea informaţiilor, înscrisurilor, registrelor ţinute în acele state. Ulterior, informaţiile erau transmise Serviciului de Securitate spre analiză şi prelucrare, astfel fel încât, la final, aceştia elaborau registre clasificate, conţinând informaţii referitoare la evrei şi descendenţii acestora, masoni, comunişti, ţigani etc. În baza acestor informaţii, milioane de oameni au fost represaţi.

Odată cu creşterea numărului populaţiei, dezvoltarea tehnologiilor informaţionale, diversificarea vieţii politice, economice şi sociale, apare o nouă industrie – industria colectării, stocării şi prelucrării datelor, practicată pe larg la nivel public şi privat. Datele personale au devenit adevărate valori ale perioadei contemporane în aşa măsură încât societatea în care trăim a căpătat o nouă denumire – „societate informaţională"[2].

Pe parcursul anilor, creşte nu doar cantitatea informaţiei colectate, dar şi calitatea, procedeele utilizate în stocarea şi prelucrarea acesteia. Apariţia tehnologiilor informaţionale a avut o influenţă crucială asupra dezvoltării colectării datelor cu caracter personal. Computerele devin capabile să stocheze o largă diversitate de date, să le prelucreze şi să le tipizeze relativ uşor, ieftin şi rapid[3].

Dezvoltarea comunicaţiilor electronice, reţelelor sociale, accesarea şi utilizarea oricărui tip de informaţie constituie avantaje ale perioadei contemporane, pe de altă parte, însă, acestea implică un şir de riscuri, printre ele pot fi evidenţiate următoarele: stocarea şi ulterior utilizarea unor informaţii imprecise, incomplete sau denaturate, accesarea sau ştergerea neautorizată a datelor personale, utilizarea pentru alte scopuri decât cele pentru care informaţia a fost colectată, distrugerea şi/sau modificarea datelor personale.

Ar. Miller, vorbind despre ameninţările computerului, menţionează: „Computerul are un apetit interminabil pentru informaţie, are o imagine incoruptă, are capacitatea de a nu uita nimic din ceea ce ai pus în el, poate deveni inima unui sistem de supraveghere care transformă casele noastre într-o lume transparentă în care banii noştri, plăcerile noastre, starea noastră de sănătate vor fi liber determinate de orice utilizator" [4].

În prezent, elaborarea şi nemijlocit aplicarea a normelor juridice legate de prelucrarea datelor cu caracter personal este privită ca cea mai potrivită soluţie de stopare a incursiunilor tehnologiilor în viaţa personală a individului, acest fapt datorându-se instrumentariului conex al dreptului. Dreptul la protecţia datelor cu caracter personal nu este o simplă garanţie, ci o prerogativă legală a individului, însoţită de un mecanism complex de realizare, îndreptată spre asigurarea posibilităţilor cetăţenilor de a stabili şi deţine controlul asupra informaţiei personale prelucrate de autorităţi publice sau private.

Reieşind din prevederile cadrului legal, stabilim că dreptul la protecţia datelor cu caracter personal poate fi invocat în oricare dintre situaţiile în care subiectul datelor este implicat în relaţii ce apar în procesul de prelucrare a datelor cu caracter personal, date ce fac parte dintr-un sistem de evidenţă sau care sunt destinate să fie incluse într-un asemenea sistem, efectuate în totalitate sau în parte prin mijloace automatizate, precum şi prin alte mijloace decât cele automatizate.

În sensul *Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal*, prelucrarea de date este înţeleasă ca orice operaţiune sau serie de operaţiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea. Obligaţia legată de asigurarea protecţiei datelor cu caracter

[2] Bennett Colin J. Regulating privacy: data protection and public policy in Europe and United States. Ithaca: Cornell University Press, 1992. 288 p.

[3] Pablo Ouzel, Protecting privacy in surveillance societies. A Critique of the Data Protection Authority Model 1989. 10 p., publicat pe http://www.pabloouziel.com/Academic%20Essay/Protecting%20Privacy%20or%20Justifying%20Surveillance.pdf (vizitat 05.05.2012).

[4] The impact of technological developments. În: International social science journal. Unesco, Place de Fontenoy, 75007 Paris, 1972, vol. XXIV, nr. 3. 431p., publicat pe http://unesdoc.unesco.org/ images/ 0000/000025/002559eo.pdf (vizitat 01.06.2012).

personal şi posibilitatea de a fi protejate drepturile, apare în oricare dintre situaţiile în care sunt exercitate cel puţin una dintre acţiunile de prelucrare indicate mai sus. Totodată, reglementările privind protecţia datelor cu caracter personal nu se aplică în situaţia în care prelucrarea datelor se realizează exclusiv pentru nevoi personale sau familiale, dacă prin aceasta nu se încalcă drepturile subiecţilor datelor cu caracter personal. De asemenea, legislaţia privind protecţia datelor cu caracter personal nu este utilizată în situaţiile în care sunt prelucrate date personale atribuite la secret de stat, în această situaţie aplicându-se reglementările privind secretul de stat. În acelaşi context, trebuie să ţinem cont de faptul că dreptul la protecţia datelor cu caracter personal nu poate fi invocat în contextul operaţiunilor de prelucrare şi transmitere transfrontalieră a datelor cu caracter personal ce se referă la făptuitorii sau victimele crimelor de genocid, crimelor de război şi crimelor împotriva umanităţii.

Aşa cum am indicat mai sus, dreptul la protecţia datelor cu caracter personal este un drept complex, determinat de un instrumentariu amplu de prerogative. Pornind de la ideea deţinerii controlului asupra propriei personalităţi şi particularităţilor acestuia, prin dreptul la protecţia datelor cu caracter personal individului i s-a atribuit prerogativa de a fi informat despre prelucrările de date ce se realizează asupra datelor sale personale, prerogativa de acces şi intervenţie asupra datelor prelucrate, precum şi dreptul de opoziţie şi acces în justiţie. Prerogativele menţionate nu sunt altceva decât nişte componente logic structurate a unui mecanism amplu de realizare a dreptului pus spre exercitare pe seama individului şi latitudinea acestuia. Fără prerogativele enumerate, dreptul la protecţia datelor ar fi un drept mort. Logica individualizării exercitării dreptului la protecţia datelor cu caracter personal porneşte de la caracterul personal al dreptului şi abordarea individuală a valorilor. Astfel, fiecare individ în parte este lăsat să decidă de sine stătător care acţiuni întreprinse faţă de el pot fi considerate ca prejudiciabile sau care nu. În continuarea celor indicate, stabilim că recunoaşterea dreptului la protecţia datelor cu caracter personal, ca un drept fundamental, depinde în mare măsură nu doar de consacrarea acestuia în conţinutul reglementărilor fundamentale, dar şi de atitudinea generală faţă de necesitatea instituirii unui astfel de drept. Cu toate acestea, nu trebuie subestimat nici rolul statului în realizarea dreptului, statul fiind obligat să implimenteze şi să asigure existenţa unor mecanisme de realizare şi control. Astfel, prerogativele enunţate mai sus se transformă într-un mecanism complex de acţiuni interdependente îndreptate clar spre obţinerea şi deţinerea controlului asupra datelor personale.

Dreptul de a fi informat despre acţiunile de prelucrare de date ca parte componentă a mecanismului de exercitare a dreptului la protecţia datelor cu caracter personal este instituit pornind de la ideea „transmiterii controlului asupra datelor personale". Individul fiind "proprietar" al datelor ce-l individualizează este în drept să ştie cine, pentru ce şi în ce condiţii urmează să folosească atributele sale, sau chiar imaginea sa. Mai mult decât, atât, pornind de la ideea „proprietăţii" asupra propriei persoane şi atributelor de individualizare, legislatorul a prevăzut expres că, în spatele dreptului de a fi informat al persoanei vizate, trebuie să existe obligaţia expresă a operatorului de a informa subiectul de date despre o eventuală prelucrare de date.

Astfel, în corespundere cu prevederile Legii privind protecţia datelor cu caracter personal, cerinţa cu privire la informarea despre acţiunile de prelucrare de date nu este doar o prerogativă a subiectului de date, dar este, în primul rând, o obligaţie a operatorilor. Cadrul legal delimitează două forme de comportament prescris operatorilor de date în dependenţă de sursa furnizării de informaţii personale. Astfel, în cazul în care datele cu caracter personal sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată să-i furnizeze subiectului de date informaţii privind identitatea sa sau a persoanei împuternicite de către operator, scopul prelucrării datelor colectate, destinatarii sau categoriile de destinatari ai datelor cu caracter personal, existenţa drepturilor de acces la date, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care acestea pot fi exercitate.

În cazul în care datele cu caracter personal nu sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu în momentul primei dezvăluiri, să furnizeze subiectului datelor cu caracter personal informaţia privind categoriile de date care urmează a fi colectate sau dezvăluite. Totodată, în cazul în care, datele cu caracter personal nu sunt colectate direct de la subiectul datelor, operatorul nu este obligat să informeze titularul datelor

despre acţiunile de prelucrare sau alte informaţii dacă acesta din urmă deţine deja informaţiile respective sau se prezumă că ştie în baza prevederilor legale general acceptabile. Ca exemplificare în acest sens poate servi situaţia în care Casa Naţională de Asigurări Sociale prelucrează datele personale ale salariaţilor preluate de la angajator. În speţa descrisă, Casa Naţională de Asigurări Sociale, în temeiul prevederilor art. 12 alin.(3) lit. a) şi lit. d) al Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, este exceptată de la obligaţia de a informa subiectul de date despre prelucrările ce le realizează deoarece se prezumă că acesta deţine deja această informaţie, fiind informat de către angajator şi cunoscând faptul că obligaţia înregistrării sau dezvăluirii datelor privind veniturile personale provenite din salarii este prevăzută în mod expres de legislaţie.

De asemenea sunt exceptaţi de la obligaţia de informare obligatorie şi operatorii care prelucrează datele în scopuri statistice, de cercetare istorică sau ştiinţifică, chiar dacă aceste date nu au fost preluate direct de la subiecţii vizaţi, cu menţinerea obligaţiei de asigurare a regimului de confidenţialitate şi realizare a acţiunilor de depersonalizare.

Totodată, prevederile art. 12 alin. (3) lit. c) al Legii nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal indică faptul că sunt exceptaţi de la obligaţia de informare obligatorie şi operatorii care stabilesc că furnizarea informaţiilor este imposibilă sau implică un efort disproporţionat faţă de interesul legitim care ar putea fi lezat. Analizând conţinutul acestei reglementări, considerăm că, prin indicarea acestei prevederi, s-a atribuit operatorilor o marjă largă de manevră, care poate aduce atingere dreptului la protecţia datelor cu caracter personal.

În evaluarea unor asemenea situaţii, efortul disproporţionat de mare urmează a fi demonstrat şi nu pur şi simplu invocat. Mai mult ca atât, pornind de la caracterul personal al dreptului, nu considerăm oportună implicarea operatorului în evaluarea potenţialului interes ce ar putea fi lezat.

Informarea subiectului cu privire la acţiunile de prelucrare este o garanţie oferită de legislator pentru a acorda subiectului de date posibilitatea preluării controlului asupra datelor sale personale şi urmarea unui anumit comportament, acest fapt fiind elucidat cu minuţiozitate de Curtea Europeană prin pronunţarea asupra cauzei Copland către Regatul Unit.

În fapt: Reclamanta fusese angajată de către o instituţie de învăţământ postşcolar, organism înfiinţat prin lege şi gestionat de către stat, în calitate de asistentă personală a directorului. Începând cu sfârşitul anului 1995, a lucrat în strânsă colaborare cu directorul adjunct. La cererea directorului adjunct, i s-a monitorizat utilizarea telefonului, a e-mail-ului şi a Internetului. Potrivit Guvernului, această monitorizare era menită pentru a verifica dacă reclamanta nu abuza de facilităţile profesionale în scopuri personale. Monitorizarea utilizării telefonului s-a materializat prin analizarea facturilor telefonice ale şcolii, care arătau numerele apelate, datele şi orele apelurilor, ca şi durata şi costul acestora; monitorizarea Internetului a luat forma unor controale ale site-urilor vizitate, ale datelor şi orelor acestor vizite, iar controlul e-mail-ului a examinat adresele, datele şi orele de trimitere a mesajelor. La acel moment, instituţia de învăţământ care angajase reclamanta nu avea nicio politică de monitorizare. În plus, legislaţia engleză nu garanta un drept general la protecţia vieţii private, deşi, ulterior, au fost introduse legi privind reglementarea interceptării comunicaţiilor şi condiţiile în care angajatorii ar putea înregistra sau monitoriza comunicaţiile angajaţilor lor, fără consimţământul acestora.

În drept: Instituţia de învăţământ în cauză este un organism public ale cărui acte angajează responsabilitatea statului, în sensul Convenţiei. Prin urmare, întrebarea se referă la obligaţia negativă a statului de a nu viola viaţa privată şi corespondenţa reclamantei.

Domeniul de aplicare a noţiunii de viaţă privată - apelurile telefonice de la sediile instituţiilor sunt, la prima vedere, acoperite de noţiunea de «viaţă privată» şi «corespondenţă». Rezultă în mod logic că e-mail-urile trimise de la locul de muncă ar trebui să beneficieze de o protecţie similară, aşa cum ar trebui tratate şi informaţiile provenite din monitorizarea utilizării în scopuri personale a Internetului. Reclamanta nu a fost informată că apelurile sale ar putea fi monitorizate şi putea gândi, în mod legitim, că apelurile sale telefonice de la locul de muncă erau confidenţiale. Ea a avut, probabil, acelaşi sentiment cu privire la utilizarea e-mail-ului şi a Internetului.

Ingerinţă: Simplul fapt că instituţia de învăţământ şi-a procurat, în mod legitim, o serie de date sub formă de facturi telefonice nu se opune constatării unei ingerinţe. De asemenea, este lipsit de relevanţă faptul că informaţiile nu au fost divulgate

unor terţi sau utilizate împotriva reclamantei în cadrul unei proceduri disciplinare sau de altă natură. Colectarea şi păstrarea, fără înştiinţarea reclamantei, a informaţiilor cu caracter personal despre utilizarea telefonului, a e-mail-ului şi a Internetului sunt, prin urmare, o ingerinţă în dreptul reclamantei la respectul vieţii private şi a corespondenţei sale.

«Prevăzută de lege»: Pentru a îndeplini cerinţa de previzibilitate, legea trebuie să fie suficient de clară pentru a exprima de manieră satisfăcătoare în ce condiţii şi circumstanţe se permite autorităţii publice să recurgă la măsurile în cauză. Argumentul Guvernului precum că instituţia ar fi fost autorizată în temeiul competenţelor sale legale de a lua „toate măsurile necesare sau oportune" pentru a pune la dispoziţie studii superioare şi postşcolare nu este convingător. În plus, Guvernul nu aminteşte că, la momentul respectiv, textele generale de drept sau statutare ale instituţiei de învăţământ în cauză ar fi conţinut o dispoziţie care reglementa circumstanţele în care angajatorii puteau monitoriza utilizarea de către angajaţi a telefonului, a e-mail-ului şi a Internetului.

De aceea, lăsând deschisă întrebarea dacă monitorizarea utilizării de către un angajat a telefonului, a e-mail-ului sau a Internetului la locul său de muncă poate fi considerată „necesară, într-o societate democratică", în anumite situaţii, în urmărirea unui scop legitim, Curtea concluzionează că, în absenţa, la momentul faptei, a oricărei legi care să reglementeze monitorizarea la nivel intern, ingerinţa nu era „prevăzută de lege".

Concluzie: violare (unanimitate)[5].

Analizând expunerile Curţii, stabilim astfel că reglementarea prelucrării de date, chiar şi printr-un regulament intern, ar putea servi drept dovadă a realizării de către operator a obligaţiei de informare, în cazul în care există confirmarea aducerii la cunoştinţă a conţinutului regulamentului.

Neexercitarea de către operator a obligaţiei de a informa subiectul de date despre activităţile de prelucrare nu-l privează totuşi pe subiectul vizat de exercitarea dreptului de a fi informat despre acţiunile de prelucrare ce se realizează asupra datelor sale, aceste acţiuni înscriindu-se în contextul dreptului de acces la datele personale. Astfel, chiar dacă operatorul a început acţiunile de prelucrare în baza unei obligaţii prescrise de lege, sau a început acţiunile cu acordul subiectului de date, sau prelucrarea a început în baza împuternicirilor date de un alt operator, subiectul de date, în orice situaţie are dreptul să fie informat despre tipul şi conţinutul activităţilor de prelucrare ce sunt realizate asupra datelor sale personale, putând astfel să instituie sau să resinstituie ulterior dreptul de control asupra datelor personale. Informarea este prerogativa ce poate da start mecanismului de apărare a dreptului la protecţia datelor cu caracter personal. Fiind informat, subiectul de date poate identifica erori de prelucrare a datelor cu caracter personal, putând astfel să ceară rectificarea lor, restabilirea sau chiar în caz de prejudiciere, să ceară compensarea lor.

În vederea asigurării continuităţii exercitării dreptului la protecţia datelor cu caracter personal, este instituit dreptul de acces la datele personale ce se prezintă drept un instrument de control asupra îndeplinirii de către operator a obligaţiei de a informa subiectul de date despre acţiunile de prelucrare ce le realizează sau urmează să le realizeze. În contextul dreptului de acces la datele personale, orice subiect al datelor cu caracter personal are dreptul să obţină de la operator, la cerere, fără întârziere şi în mod gratuit, confirmarea faptului că datele care îl privesc, sunt sau nu sunt prelucrate de acesta, de asemenea informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele.

Atragem atenţia că în baza celor expuse mai sus, urmează să se realizeze o diferenţiere între dreptul de acces la datele personale şi dreptul de acces la informaţie, reglementat de Legea privind accesul la informaţie. Conform Legii privind protecţia datelor cu caracter personal, individul are dreptul de a solicita accesul doar la datele sale personale. Totodată, urmează să se facă diferenţiere între informaţiile oficiale şi informaţiile oficiale ce conţin date cu caracter personal. În cazul în care solicităm accesul la informaţii oficiale, dar acestea conţin şi date cu caracter personal ce ne privesc, întemeierea poziţiei noastre urmează a fi realizată în baza prevederilor Legii privind protecţia datelor cu caracter personal. O exemplificare în vederea deosebirii a acestor două drepturi a fost adusă de CtEDO prin pronunţarea asupra cauzei Trăilescu vs. România[6].

[5] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-119545

[6] DECIZIE din 22 mai 2012 cu privire la cererile nr. 5.666/04 şi 14.464/05 prezentate de Ovidiu Trăilescu împotriva României; Publicată în Monitorul Oficial din 31 august 2012.

Curtea Europeană a Drepturilor Omului s-a pronunţat în cauza Trăilescu vs. România [1] în sensul că reclamantul nu poate acuza statul de încălcarea dreptului său la viaţă privată atâta timp cât şi-a întemeiat căile interne de atac pe Legea nr. 544/2001 privind liberul acces la datele de interes public, întrucât nu a epuizat remediile din dreptul intern.

Reclamantul a acuzat statul român că a încălcat art. 6 (dreptul la un proces echitabil) şi art. 8 (dreptul la viaţă privată) atunci când nu a fost numit în funcţia de magistrat-asistent după ce fusese declarat admis la examenul organizat de Ministerul Justiţiei pentru suplinirea posturilor vacante în magistratură, întrucât nu ar îndeplini condiţia bunei reputaţii. Acest fapt a fost stabilit după întocmirea unui dosar personal de către Minister. După ce a atacat decizia de respingere în contencios administrativ şi a cerut reexaminarea dosarului său, reclamantul a fost informat că hotărârea privind lipsa bunei reputaţii nu va fi modificată, fiindu-i explicate motivele ce reies din dosar în acest sens: existenţa unei amenzi contravenţionale, urmată de o plângere penală pentru lovire şi alte violenţe, precum şi concedierea din postul de jurist din motive disciplinare de către fostul său angajator.

Reclamantul a atacat deciziile de respingere, solicitând, în cadrul procedurilor, şi depunerea dosarului personal ca probă, instanţa neadmiţând această cerere. După ce Curtea Supremă de Justiţie a respins recursul cu privire la anularea deciziilor, reclamantul a solicitat din nou acces la dosarul său, de data aceasta - direct Ministerului Public. Accesul i-a fost refuzat, pe motiv că datele din dosar nu sunt de interes public:

„Ministerul a notat că dosarul în cauză fusese întocmit în conformitate cu Legea nr. 92/1992 în urma cererii sale de a fi admis în magistratură, documentele existente în acest dosar neavând un caracter public. Prin urmare, reclamantul nu îl putea consulta sau face copii. A adăugat, în cele din urmă, că reclamantul a fost informat anterior cu privire la motivele pentru care cererea sa de admitere în magistratură a fost respinsă" (punctul 23).

Reclamantul a depus o plângere la Minister în baza Legii 544/2001, respinsă şi aceasta. Apoi a atacat în instanţă scrisoarea de respingere: „A cerut, de asemenea, acces la dosarul „personal" şi la realizarea de copii ale documentelor cuprinse în dosar. A arătat că accesul la aceste documente îi era necesar pentru a-şi putea restabili buna reputaţie. S-a bazat pe art. 13, 14 şi 22 din Legea nr. 544/2001 privind liberul acces la informaţii de interes public şi pe normele sale de aplicare" (Punctul 25).

Ministerul Public s-a apărat, afirmând că datele solicitate nu intră în domeniul de aplicare a Legii 544/2001, nefiind informaţii de interes public. Iar reclamantul a contra-argumentat că, „potrivit art. 14 alin. (1) din Legea nr. 544/2001, datele personale pot deveni informaţii de interes public numai în măsura în care afectează capacitatea de exercitare a unei funcţii publice" (punctul 27), susţinând că el se află în acest caz.

Tribunalul Bucureşti a hotărât că, „potrivit art. 2 lit. c) şi art. 12 lit. d) din Legea nr. 544/2001, coroborate cu art. 3 lit. a) din Legea nr. 677/2001, informaţiile cuprinse în dosarul „personal" aveau un caracter personal şi nu de interes public, dispoziţiile Legii nr. 544/2001 nefiind, prin urmare, aplicabile" (punctul 30). În ciuda acestei explicaţii, reclamantul a depus recurs cu argumentul că, „în măsura în care informaţiile cuprinse în dosar au fost folosite de pârât pentru a-i împiedica accesul la funcţia publică, aceste informaţii au devenit de interes public şi că Legea nr. 544/2001 era aplicabilă în speţă" (punctul 31). Cu alte cuvinte, reclamantul a persistat în demersul său de a demonstra că datele private conţinute în dosar erau, în realitate, de interes public, drept pentru care i se cuvenea să aibă acces la ele.

Curtea de Apel Bucureşti a respins recursul, hotărând că „datele solicitate de reclamant intrau sub incidenţa art. 12 lit. d) din Legea nr. 544/2001, fiind informaţii cu privire la datele personale" (punctul 32). Cu alte cuvinte, Curtea de Apel i-a transmis reclamantului că acesta nu poate avea acces la propriul dosar conform acţiunii sale, întrucât dosarul nu conţine informaţii de interes public, ci date cu caracter personal[7].

În sensul dreptului privind protecţia datelor cu caracter personal, subiectul de date dispune nu doar de prerogativa de a solicita informaţii despre acţiunile de prelucrare ce sunt realizate, dar şi de prerogativa de a interveni asupra activităţilor de prelucrare, prin înaintarea demersurilor legate de rectificarea, actualizarea, blocarea sau ştergerea datelor cu caracter personal a căror prelucrare contravine reglementărilor privind protecţia date-

[7] http://www.juridice.ro/217694/cedo-trailescu-vs-romania-accesul-la-propriul-dosar-se-face-conform-legii-protectiei-datelor-private-si-nu-legii-liberului-acces-la-informatii.html

lor, în special din cauza caracterului incomplet sau inexact al datelor. În contextul practicii CtEDO, şi în special, cauza Cauza Google c. Spaniei[8], chiar şi datele veridice cu timpul se pot transforma în date eronate, dând posibilitate subiectului de date să înainteze demersuri privind radierea datelor învechite.

Cauza priveşte un cetăţean spaniol care doreşte ca un articol din ziarul spaniol *La Vanguardia Ediciones* să fie şters sau, dacă acest lucru nu este posibil, atunci solicită ca articolul să nu mai apară pe lista rezultatelor de căutare a Google. Acesta susţine că informaţia pe care o doreşte ştearsă se referă la o datorie veche, pe care a plătit-o demult. Solicitările sale au fost respinse şi de către publicaţie, şi de către Google Spania, care a argumentat că cererea trebuie înaintată sediului principal al Google din SUA. Drept urmare, cetăţeanul a depus o plângere la autoritatea spaniolă de supraveghere a datelor personale, care a respins solicitarea cu privire la ştergerea informaţiilor de către publicaţie, dar a emis, în schimb, un ordin adresat Google Spania „pentru a lua toţi paşii necesari în retragerea datelor vizate din indexările sale şi să facă imposibil accesul la aceste date în viitor".

Fiind solicitată să stabilească dacă directiva permite persoanei vizate să solicite eliminarea de pe o astfel de listă de rezultate a unor linkuri către pagini web, pentru motivul că doreşte ca informaţiile referitoare la persoana sa, care figurează pe aceste pagini, să fie „uitate" după un anumit timp, Curtea arată că, în ipoteza în care se constată, ca urmare a unei cereri formulate de persoana vizată, că includerea acestor link-uri pe lista de rezultate este, în stadiul actual, incompatibilă cu prevederile legale actuale, informaţiile şi link-urile cuprinse în lista amintită trebuie să fie şterse. În această privinţă, Curtea observă că şi o prelucrare iniţial licită a unor date exacte poate deveni cu timpul incompatibilă cu prevederile legale în cazul în care, având în vedere ansamblul împrejurărilor caracteristice speţei, aceste date sunt inadecvate, nu sunt sau nu mai sunt pertinente, sau sunt excesive în raport cu scopurile pentru care au fost prelucrate şi cu timpul care s-a scurs. Curtea adaugă că, în cadrul aprecierii unei astfel de cereri formulate de persoana vizată împotriva prelucrării realizate de operatorul unui motor de căutare, trebuie să se examineze, în special, dacă această persoană are dreptul ca informaţiile respective referitoare la persoana sa să nu mai fie, în stadiul actual, asociate cu numele său de o listă de rezultate care este afişată în urma unei căutări efectuate plecând de la numele său. Dacă aceasta este situaţia, link-urile către paginile web care conţin informaţiile respective trebuie eliminate de pe lista de rezultate, cu excepţia cazului în care există motive speciale, precum rolul jucat de această persoană în viaţa publică, care să justifice un interes preponderent al publicului de a avea acces, în cadrul unei asemenea căutări, la informaţiile în cauză[9].

De asemenea, subiectul vizat poate solicita şi notificarea terţilor cărora le-au fost dezvăluite datele cu caracter personal incomplete sau inexacte, exceptând cazurile când această notificare se dovedeşte a fi imposibilă sau presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

În temeiul prevederilor art.2 alin. (2) şi (d) al Legii privind protecţia datelor cu caracter personal, domeniul reglementărilor privind protecţia datelor cu caracter personal se extinde asupra acţiunilor de prelucrare a datelor cu caracter personal în cadrul acţiunilor de prevenire şi investigare a infracţiunilor, punerii în executare a sentinţelor de condamnare şi altor acţuni din cadrul procedurii penale sau contravenţionale în condiţiile legii.

Atragem atenţia că dreptul la informare, acces şi intervenţie asupra datelor nu se impune spre realizare în cazul în care sunt efectuate acţiuni de prelucrare a datelor cu caracter personal în cadrul acţiunilor de prevenire şi investigare a infracţiunilor, punerii în executare a sentinţelor de condamnare şi a altor acţuni din cadrul procedurii penale sau contravenţionale în condiţiile legii. De asemenea, nu se impun spre asigurare drepturile sus indicate şi în cazul prelucrărilor de date realizate în scopul apărării naţionale, securităţii statului, menţinerii ordinii publice, protecţiei drepturilor şi libertăţilor subiectului datelor cu caracter personal sau ale altor persoane, dacă prin aplicarea acestora este prejudiciată eficienţa acţiunii sau obiectivul

[8] Hotărârea în cauza C-131/12 Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González.

[9] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070ro.pdf

urmărit în exercitarea competenţelor legale ale autorităţii publice (temei: prevederile art. 15 al Legii privind protecţia datelor cu caracter personal). Atenţionăm că cele invocate mai sus nu scutesc operatorii, chiar dacă aceştia sunt autorităţi publice şi realizează acţiuni de prevenire şi investigare a infracţiunilor, să se eschiveze de la îndeplinirea celorlalte garanţii prescrise de Legea privind protecţia datelor cu caracter personal. Mai mult decât atât, la încetarea acţiunilor de urmărire penală, reprezentanţii organului de urmărire penală sunt obligaţi să ofere subiecţilor ale căror date au fost prelucrate garanţiile prescrise de prevederile art. 12-14 ale Legii privind protecţia datelor (temei: art. 15 alin. (3) din Legea privind protecţia datelor cu caracter personal).

Tot în contextul dispunerii de dreptul la protecţia datelor, individului i s-a atribuit, în temeiul prevederilor art. 16 a Legii privind protecţia datelor, şi prerogativa de a se opune activităţilor de prelucrare. Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care legea stabileşte altfel. Dacă opoziţia este justificată, prelucrarea efectuată de operator nu mai poate viza aceste date.

Subiectul datelor cu caracter personal are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care îl vizează să fie prelucrate pentru prospectare comercială.

Totodată, e necesar de menţionat că, în afară de drepturile sus indicate, subiectul vizat dispune şi de dreptul la acces în justiţie, având dreptul nu doar la constarea încălcărilor, dar şi la repararea prejudiciilor materiale şi morale.

Reieşind din cele menţionate, dreptul la protecţia datelor cu caracter personal are un caracter complex şi oferă prin conţinutul său subiecţilor vizaţi posibilitatea de a menţine controlul asupra identităţii personale, în particular, şi asupra vieţii private, în general. Exercitarea prerogativelor date de cadrul legislativ se prezintă ca o manifestare de voinţă individuală, fiecare urmând până la urmă să identifice cadrul personal de intimitate şi acţiunile pe care urmează să le întreprindă.

Bibliografie:

1. Wayne M. Handbook of Personal Data Protection. New York: Stockton Press and Basingstoke, Hants: Macmillan Publishers Ltd, 1992. 1048 p.

2. Bennett Colin J. Regulating privacy: data protection and public policy in Europe and United States. Ithaca: Cornell University Press, 1992. 288 p.

3. Pablo Ouzel, Protecting privacy in surveillance societies. A Critique of the Data Protection Authority Model 1989. 10 p., publicat pe http://www.pabloouziel.com/Academic%20Essay/Protecting%20Privacy%20or%20Justifying%20Surveillance.pdf (vizitat 05.05.2012).

4. The impact of technological developments. În: International social science journal. Unesco, Place de Fontenoy, 75007 Paris, 1972, vol. XXIV, nr. 3. 431p., publicat pe http://unesdoc.unesco.org/ images/ 0000/000025/002559eo.pdf (vizitat 01.06.2012).

5. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-119545 (vizitat 20.09.2014).

6. DECIZIE din 22 mai 2012 cu privire la cererile nr. 5.666/04 şi 14.464/05 prezentate de Ovidiu Trăilescu împotriva României; Publicată în Monitorul Oficial din 31 august 2012.

7. http://www.juridice.ro/217694/cedo-trailescu-vs-romania-accesul-la-propriul-dosar-se-face-conform-legii-protectiei-datelor-private-si-nu-legii-liberului-acces-la-informatii.html.

8. Hotărârea în cauza C-131/12 Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González.

9. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070ro.pdf.