UNIVERSITATEA DIN CRAIOVA
ŞCOALA DOCTORALĂ DE ŞTIINŢE SOCIO-UMANE
FACULTATEA DE DREPT ŞI ŞTIINŢE SOCIALE

Drepturile persoanei cu privire la protecţia datelor private

- Teză de doctorat -

CONDUCERE ŞTIINŢIFICĂ:
Prof. univ. dr. SEVASTIAN CERCEL

Doctorand,
GABRIELA ZANFIR

Craiova
2013

- REZUMAT -

Protecţia datelor private este subiectul unor dezbateri intense în prezent, la nivel global, datorită dezvoltării extraordinare a tehnologiei informaţiilor, a capacităţii produselor acesteia de stocare şi de prelucrare de date, inter-conectivităţii ce caracterizează produsele tehnologice, dar mai ales datorită modului în care acestea sunt utilizate. Ca domeniu de reglementare, protecţia datelor private a apărut în nordul şi vestul Europei, precum şi în Statele Unite ale Americii, în anii ’70, acesta dezvoltându-se într-un ritm alert şi prezentând de-a lungul evoluţiei sale caracteristici ale unui adevărat fenomen global de reglementare.

România a adoptat prima lege a protecţiei persoanei cu privire la prelucrarea datelor personale abia în 2001, ca urmare a obligaţiilor asumate în vederea aderării la Uniunea Europeană în legătură cu transpunerea în dreptul intern a acquis-ului unional. Cu toate acestea, prelucrarea datelor personale şi-a făcut loc în noul Cod civil, fiind reglementată în art. 77, în secţiunea dedicată drepturilor personalităţii.

Lucrarea contribuie la umplerea unor lacune în literatura de specialitate română cu privire la protecţia datelor personale, caracterizând dreptul la protecţia datelor private ca drept subiectiv civil şi făcând o critică exhaustivă drepturilor persoanei vizate de a controla prelucrarea de date, privite ca prerogative ale acestui drept subiectiv.

Astfel, principala întrebare la care îşi asumă să răspundă este următoarea: „Care este rolul drepturilor de control asupra prelucrării datelor în materia protecţiei persoanei cu privire la prelucrarea datelor private şi cum se manifestă acestea în sistemul complex de norme ce le reglementează?”.

Partea I a tezei îşi propune să stabilească principalele coordonate ale unei teorii generale a protecţiei datelor. O fundamentare teoretică unidimensională a acesteia lipseşte din doctrina română, în timp ce în doctrina străină principala preocupare teoretică privind fundamentele protecţiei datelor personale se axează pe diferenţierea acesteia de protecţia vieţii private. Pentru a realiza scopul propus, demersul este împărţit în două capitole, primul dintre ele caracterizând domeniul de reglementare al protecţiei datelor, iar cel de-al doilea teoretizând dreptul la protecţia datelor private ca drept subiectiv civil.

Capitolul 1 reprezintă o *misce en scéne* istorică, multidimensională din punct de vedere teritorial, şi contextuală a reglementărilor privind protecţia datelor personale. Ideile principale ce pot fi individualizate din acest cadru general sunt trei.

Mai întâi, poate fi reţinută apariţia tehnologiilor de stocare şi prelucrare de informaţii ca fiind cea care a impus necesitatea unui mecanism juridic de protecţie a libertăţii individuale raportată la stocarea şi prelucrarea informaţiilor personale.

Apoi, acest mecanism a fost adoptat relativ simultan – în anii ’70 şi începutul anilor ’80, în democraţiile occidentale, având forme şi principii similare. Acest fapt a dus la apariţia teoriilor cu privire la convergenţa normelor privind protecţia datelor personale.

În fine, reţinem şi că, deşi până acum în doctrină au fost identificate mai multe generaţii ale reglementărilor ce au ca obiect protecţia datelor personale, în realitate singura diferenţă substanţială între conţinutul reglementării protecţiei datelor între anumite momente date este trecerea de la consacrarea mai multor norme dispersate ce au un scop comun – protecţia datelor, la consacrarea şi elaborarea unui drept subiectiv autonom la protecţia datelor private.

În ceea ce priveşte particularităţile sistemului român de protecţie a datelor prezentate în acest capitol, se remarcă analiza transpunerii în sistemul român de drept a normelor privind protecţia datelor personale, pornind de la fundamentarea necesităţii lor şi ajungând la sublinierea diferenţelor dintre legea de transpunere şi Directiva 95/46, diferenţe care ar putea duce în unele cazuri la concluzia unor erori de transpunere. A se vedea în acest sens înţelegerea mai largă dată de legea română temeiurilor care justifică o prelucrare a datelor personale.

Reglementarea exhaustivă a intimităţii informaţionale în Noul Cod Civil, precum şi preocuparea arătată strict prelucrării datelor personale (art. 77 NCC), sunt indicii că România are un cod civil modern, construit astfel încât individul să poată face faţă provocărilor erei digitale, pe de o parte, şi ingerinţelor în sfera privată a existenţei sale, pe de altă parte. Aşa cum a fost deja subliniat în doctrină, „cu siguranţă, această reglementare va contribui, în mare măsură, la civilizarea unor raporturi interumane aflate în mare suferinţă în perioada bulversată pe care o traversăm, dar şi la stăvilirea elanului necontrolat al autorităţilor, care, sub diferite pretexte, nesocotesc adesea drepturi precum cele la viaţă privată sau demnitate”[1]. În viitorul apropiat, însă, regulile cu privire la protecţia datelor personale - domeniul material al căreia este foarte larg, vor fi înlăturate din sistemul român de drept de un regulament general al protecţiei datelor, dar şi de

[1] E. Chelaru, *Drepturile personalităţii în reglementarea Noului Cod Civil*, Revista Dreptul, nr. 10/2011, p. 61.

o directivă a protecţiei datelor în materie penală, care se află în prezent în plin proces de legiferare la nivelul Uniunii Europene (în măsura în care vor fi contrare prevederilor acestora).

Capitolul 2, pornind de la dreptul obiectiv al protecţiei datelor, fundamentează teoretic existenţa acesteia în ideea de autodeterminare informaţională, căreia, la rândul ei, îi identifică rădăcina în ideea de liber arbitru. Capitolul continuă cu trecerea de la identificarea unui interes ce poate fi protejat prin normele din domeniul protecţiei datelor, la fundamentarea dreptului la protecţia datelor personale ca drept subiectiv civil. Sunt astfel identificate elementele dreptului subiectiv în dreptul la protecţia datelor personale – subiectul activ, obiectul şi conţinutul dreptului, în timp ce protecţia sa juridică va face obiectul ultimei părţi a tezei.

O contribuţie semnificativă teoretică adusă de Capitolul 2 este analiza rolului consimţământului persoanei vizate în protecţia datelor personale, propunându-se renunţarea la absolutizarea ideii de consimţământ în această materie şi abordarea contextuală a acestuia, mutându-se astfel centrul de greutate al dreptului la protecţia datelor spre alte garanţii legale adecvate, precum drepturile „de control" ale persoanei vizate, care, în mod real, contribuie la autodeterminarea informaţională, dar şi limitarea scopului prelucrării şi mecanismele complexe de răspundere ale operatorului de date – toate fiind reglementate având în substrat ideea creării unui sistem complex de protecţie a persoanei vizate de prelucrare. Aceste trei tipuri de garanţii legale adecvate ale persoanei vizate sunt identificate ca reprezentând prerogativele din conţinutul dreptului la protecţia datelor personale.

Am arătat că, în definitiv, filosofia protecţiei datelor poate fi schiţată astfel: orice persoană ar trebui să aibă dreptul să nu fie obiectul unei prelucrări a datelor sale decât dacă această prelucrare este făcută într-unul din temeiurile legale (pe care le-am identificat ulterior ca făcând parte dintr-un meta-conţinut al dreptului la protecţia datelor personale) şi decât dacă prelucrarea este supusă unor garanţii adecvate (pe care le-am identificat ca prerogative din conţinutul dreptului la protecţia datelor personale). Şi cum consimţământul persoanei vizate este doar unul din mai multe temeiuri legale de prelucrare prevăzute în legea protecţiei datelor, am argumentat că importanţa sa în acest domeniu trebuie ierarhizată sub necesitatea clarificării şi detalierii „garanţiilor adecvate" – ele fiind aplicabile ori de câte ori există o prelucrare a datelor personal, indiferent de temeiul în care este făcută. Acest lucru este o consecinţă a coordonării prerogativelor dreptului la protecţia datelor personale cu protejarea obiectului său, obiect despre

care am stabilit că are o natură procedurală şi desemnează un complex de mecanisme ca „instrumente normative de transparenţă”.

Acest capitol argumentează, deci, că dreptul la protecţia datelor personale este un drept subiectiv civil nepatrimonial, substanţializat astfel încât să răspundă intereselor persoanei în contextul Societăţii Informaţionale. Structura sa este una complexă, iar esenţa sa este mai degrabă procedurală. Am arătat însă că elementele clasice ale dreptului subiectiv civil au corespondente în consacrarea dreptului la protecţia datelor personale.

Drepturile persoanei vizate care facilitează auto-determinarea informaţională a acesteia, pe care le-am numit „drepturi de control”, sunt sistematizate în **Partea a II-a** a lucrării conform structurii propuse în proiectul de regulament al protecţiei datelor personale în Uniunea Europeană, respectiv urmărind principalele trei categorii de drepturi: drepturile de informare şi de acces, drepturile de rectificare şi ştergere, precum şi drepturile de opoziţie (la prelucrarea datelor, în general, dar şi la luarea unor decizii în temeiul creării automate de profiluri).

Un principiu fundamental al legilor privind protecţia datelor private este posibilitatea persoanelor vizate să participe la prelucrarea datelor care le privesc, făcută de alte persoane fizice sau juridice, precum şi să influenţeze prelucrarea lor. Acest principiu este recunoscut în doctrină ca *principiul controlului şi participării persoanei vizate*. Alături de alte şapte principii - cel al prelucrării corecte şi legale, al minimizării, al precizării scopului, al calităţii informaţiilor personale, al limitării transmiterii datelor către terţi, al securităţii informaţiei şi al sensibilităţii datelor, acesta are un rol important în prelucrarea legală a datelor private, ţinând cont de scopul ultim al protecţiei libertăţilor persoanei. Drepturile persoanei vizate în contextul prelucrării – dreptul la informare, dreptul de acces, dreptul de rectificare, dreptul de opoziţie, dreptul de a nu fi supus unei decizii automate, viitoarele drepturi de a fi uitat şi la portabilitatea datelor (ambele reglementate în propunerea de regulament), sunt expresii normative ale principiului controlului şi participării persoanei vizate în ceea ce priveşte prelucrarea datelor sale.

Sunt autori, precum Poullet, care au considerat că recunoaşterea expresă a unor drepturi subiective ale persoanei vizate în contextul prelucrării de date, în Convenţia 108 a Consiliului Europei din 1981, marchează a doua generaţie a reglementării protecţiei datelor cu caracter personal şi permite persoanei vizate să controleze circulaţia imaginii sale informaţionale şi să aprecieze motivele utilizării ei. Contrar acestei opinii, trebuie precizat însă că majoritatea legiuitorilor din statele europene care au adoptat legi privind protecţia datelor în anii ’70 au avut

în vedere faptul că „fluxul datelor private curge în principal de la actorii slabi spre actorii puternici”[2], garantând de la bun început un set de drepturi titularului datelor personale: dreptul de informare şi de acces la date, dreptul de rectificare şi dreptul de ştergere. Acest set de drepturi a evoluat ulterior în legile naţionale, fiind reglementate detaliat în Directiva 95/46 privind protecţia persoanei cu privire la prelucrarea datelor personale.

În capitolele Părţii a II-a, conţinutul fiecărui drept subiectiv expres prevăzut de legile din materia protecţiei datelor este fundamentat conceptual, iar forma reglementării sale este urmărită şi din punct de vedere al evoluţiei istorice a reglementării. Drepturile persoanei vizate sunt analizate având în vedere în primul rând legea română, apoi directivele UE din materia protecţiei datelor, dar şi proiectele de regulament şi de directivă ale protecţiei datelor, care se află într-o fază înaintată în procesul de legiferare. Jurisprudenţa Curţii Europene a Drepturilor Omului în aplicarea art. 8 al Convenţiei privind respectul vieţii private va fi, de asemenea, avută în vedere, în special cu privire la dreptul de acces la date. Necesitatea unei astfel de abordări comprehensive a drepturilor persoanei vizate în contextul prelucrării datelor personale este evidentă în sistemul de drept complex al unui stat membru UE.

Capitolul 3 detaliază drepturile la informare şi de acces la datele personale ale persoanei vizate de prelucrare. Protecţia datelor personale ar fi lipsită de eficienţă dacă persoana ale cărei date sunt prelucrate, mai întâi, nu ar cunoaşte existenţa prelucrării, contextul acesteia şi, apoi, nu ar şti ce date despre sine sunt colectate, în ce moduri sunt folosite şi cine mai are acces la ele.

Cele două drepturi sunt componente ale unui principiu al transparenţei prelucrării datelor personale, dar o transparenţă bidimensională, respectiv o transparenţă gestionată de operatorul de date şi opozabilă exclusiv persoanei ale cărei date sunt prelucrate.

Autodeterminarea informaţională are ca punct de plecare acest tip de transparenţă. Dacă persoana vizată nu cunoaşte faptul că informaţii despre sine sunt colectate şi păstrate în diferite baze de date, există imposibilitatea practică de a putea exercita oricare dintre prerogativele care decurg din garantarea dreptului la protecţia datelor personale.

Pe de altă parte, a fost exprimată în doctrină şi opinia conform căreia „dreptul de acces constituie în mod consistent o povară semnificativă, atât din punct de vedere administrativ, cât şi din punct de vedere financiar, pentru operatorii de date”[3].

[2] S. Gutwirth, *Privacy and the Information Age*, Rownan & Littlefield Publishers, Inc., SUA, 2002, p. 85.
[3] P. Carey, *Data Protection. A practical guide to UK and EU law*, 3rd edition, Oxford University Press, 2009, p. 130.

Dreptul la informare şi dreptul de acces sunt incluse în primele legi care au reglementat protecţia datelor, începând cu *Bundesdatenschutzgesetz* - legea federală germană adoptată în 1977, continuând cu *Loi relatif a l'informatique, aux fichiers et aux libertes*, adoptată în Franţa în 1978, *Data Protection Act*, adoptată în 1984 de către Parlamentul britanic, şi până la *Wet Persoonsregistraties*, adoptată în 1989 în Olanda. Iniţial, distincţia dintre cele două drepturi nu apare ca fiind clară, legea franceză fiind singura care le individualizează. Atât legea germană, cât şi cea britanică, prevăd prerogative similare celor două drepturi fie sub tutela unui drept la informare, fie sub tutela unui drept de acces.

Cele două drepturi apar ca „posibilităţi" în Convenţia 108 a Consiliului Europei, adoptată în 1981, şi, din nou, ca drepturi de sine stătătoare acordate persoanei vizate de prelucrare în Directiva 95/46 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, alături de dreptul de opoziţie al persoanei vizate, dreptul de a interveni asupra datelor şi dreptul de a nu fi supus unei decizii individuale.

Articolele 10, 11 şi 12 ale Directivei 95/46 prevăd că de fiecare dată când informaţii personale sunt colectate, persoanele vizate trebuie să fie informate cu privire la detaliile prelucrării datelor lor şi au dreptul să primească o copie a tuturor datelor prelucrate. Cele trei articole din directivă au fost transpuse în Legea 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, în articolele 12 şi 13, care sunt analizate în detaliu în acest capitol, din punct de vedere al conţinutului şi al modalităţii de exercitare.

Ideea unui regim legal care să garanteze accesul la propriile informaţii personale a apărut prima dată în sistemul român de drept cu privire la dosarele fostei securităţi. La doi ani după adoptarea Legii 187/1999 privind accesul la propriul dosar, a fost adoptată legea de transpunere a Directivei 95/46, într-un sistem care, până atunci, nu recunoscuse o nevoie socială şi legală în sensul protejării datelor personale dincolo de chestiunea sensibilă a accesului la dosarele fostei securităţi. Trebuie precizat totuşi că reglementarea dreptului de acces la propriile date, conform Legii 677/2001, presupune o procedură mult simplificată comparativ cu procedura de acces la propriul dosar deţinut de fosta securitate, prin intermediul Consiliului Naţional de Studiere a Arhivelor Securităţii, iar acest lucru ridică problema unei norme de drept intern care nu respectă standardul de armonizare stabilit printr-o directivă în acelaşi domeniu material de reglementare.

Prevederile Legii nr. 677/2001 cu privire la dreptul la informare şi dreptul de acces la date reprezintă în mare măsură o transpunere corectă a prevederilor directivale, inclusiv din punctul de vedere al excepţiilor şi restricţiilor. Singura inadvertenţă se referă la omiterea prevederii ca accesul la date să fie făcut fără constrângere. Această condiţie, însă, deşi este prevăzută în art. 12 alin. (1) al Directivei 95/46, nu este preluată în proiectul de Regulament. Cu toate acestea, până la intrarea Regulamentului în vigoare, norma din directivă poate fi invocată de către justiţiabil dacă acesta consideră că a fost constrâns să solicite acces la datele sale. Trebuie subliniat şi că Legea nr. 677/2001 a întărit protecţia celor două drepturi prin adăugarea unor detalii ale prelucrării care trebuie oferite în mod obligatoriu de către operator persoanei vizate, faţă de normele din Directiva 95/46.

Capitolul 4 analizează drepturile de intervenţie asupra prelucrării de date. S-ar putea spune că, după informare şi acces, o a doua etapă în realizarea scopului autodeterminării informaţionale permite persoanei vizate să intervină direct asupra prelucrării. Persoana vizată are dreptul să obţină rectificarea, actualizarea şi chiar ştergerea datelor despre sine care sunt prelucrate. Fără această a doua componentă a prerogativelor dreptului la protecţia datelor personale, auto-determinarea informaţională ar rămâne utopică.

Legea română privind protecţia datelor reglementează în art. 14 „dreptul de intervenţie asupra datelor", în conţinutul căruia cuprinde rectificarea, ştergerea, blocarea şi actualizarea datelor personale. Directiva 95/46 nu foloseşte termenul de „drept de intervenţie asupra datelor", ci reglementează ştergerea, blocarea şi rectificarea datelor în conţinutul art. 12 – „dreptul de acces". Considerăm că soluţia legiuitorului român exprimă esenţa acestor drepturi, ele reprezentând, în definitiv, posibilitatea persoanei vizate de a interveni direct asupra prelucrării datelor.

Posibilitatea persoanei vizate de a interveni efectiv şi concret asupra prelucrării datelor sale este aspectul care a născut cele mai multe controverse cu privire la conţinutul drepturilor persoanei vizate în pachetul de reformă privind protecţia datelor în Uniunea Europeană.

În virtutea acestei posibilităţi, Comisia Europeană a introdus două drepturi de intervenţie ale persoanei vizate – dreptul de a fi uitat (în fapt, o dezvoltare a dreptului de a solicita ştergerea datelor) şi dreptul la portabilitatea datelor. După cum reiese din acest capitol, intenţia de a legifera cele două drepturi a generat două opinii opuse. Pe de o parte, Comisia Europeană este susţinută în reglementarea celor două drepturi în special de Autoritatea Europeană pentru

Protecţia Datelor, de asociaţiile care promovează apărarea drepturilor omului în era digitală şi de mediul academic european din domeniul dreptului şi tehnologiei. Pe de altă parte, marile companii globale care furnizează servicii în domeniul IT, o parte dintre guvernele statelor membre UE, precum şi opinii din mediul academic american în materia dreptului şi tehnologiei au criticat introducerea celor două drepturi. Ambele perspective sunt detaliate în acest capitol.

Susţinătorii, dar mai ales criticii, reglementării dreptului de a fi uitat şi dreptului la portabilitatea datelor scapă din vedere însă faptul că individualizări ale ambelor drepturi există deja în reglementările actuale privind protecţia datelor în Uniunea Europeană. Acesta este unul dintre motivele pentru care am grupat drepturile efective de intervenţie asupra prelucrărilor în acelaşi capitol, pentru a înlesni compararea reglementărilor actuale cu reglementările din pachetul de reformă.

Printre concluziile deduse din acest capitol, se poate sublinia că, deşi tehnic vorbind dreptul de a fi uitat este un drept la ştergerea datelor care va avea două obligaţii corelative, una de rezultat – ştergerea datelor, şi una de diligenţă – înştiinţarea celor care au preluat datele cu privire la solicitarea de ştergere a acestora, obligaţii opozabile operatorilor la nivel cvasi-global, acesta reprezintă, în fond, mai mult decât atât: protejează autonomia, libertatea şi identitatea persoanei într-o lume supra-digitalizată, nu doar în plan spaţial, ci şi în plan temporal (de unde şi ideea de „uitare").

În ceea ce priveşte dreptul la portabilitatea datelor, se poate afirma că, în acest moment, este exponentul unei noi generaţii de concepte juridice relative la reglementarea vieţii private, admiţând în acelaşi timp că funcţiile pe care le poate îndeplini sunt complexe, având efecte inclusiv în ceea ce priveşte concurenţa între furnizorii serviciilor societăţii informaţionale. Cu toate acestea, reglementarea sa într-un act legislativ care are ca obiect protecţia datelor personale indică faptul că rolul fundamental al portabilităţii datelor este acela de a oferi un control sporit persoanelor vizate de prelucrarea datelor asupra autodeterminării lor informaţionale.

În **Capitolul 5** sunt studiate drepturile de opoziţie ale persoanei vizate cu privire la prelucrare, dar şi cu privire la deciziile individuale automate, luate în baza creării de profiluri.

Dreptul general de opoziţie la prelucrarea datelor, precum şi drepturile persoanei vizate cu privire la deciziile luate în temeiul unor profiluri create automat reprezintă categoria de prerogative ale persoanei vizate care are cel mai puţin clar conţinut. Acest lucru se datorează într-o oarecare măsură faptului că cele două drepturi nu au făcut parte din corpul comun de

prevederi ale primelor legi privind protecţia datelor personale ale unor state europene, spre deosebire de celelalte două categorii de drepturi ale persoanei vizate – „dreptul de a şti” şi drepturile de intervenţie directă asupra prelucrării.

Comparând scopurile reglementării celor două drepturi, dreptul general la opoziţie este mai degrabă expresia unor preocupări teoretice, care ţin de fundamentul unui drept la autodeterminare informaţională, în timp ce dreptul persoanei vizate de a se opune unor decizii individuale automatizate este mai degrabă un răspuns la probleme cât se poate de concrete şi de actuale. Succinta caracterizare a creării de profiluri făcută în una din subsecţiunile acestui capitol indică pericolul pe care crearea de profiluri dincolo de orice control îl reprezintă pe de o parte pentru libertatea individului, în sens larg, şi pe de altă parte pentru societăţile democratice.

Inspirată din legea franceză a protecției datelor adoptată în 1978, Directiva 95/46 a introdus un drept general al persoanei vizate de a se opune prelucrărilor de date, în situații excepționale, chiar dacă acestea respectă condițiile legale de prelucrare. O condiţie principală a exercitării cu succes a dreptului de a se opune prelucrării de date este existenţa unor „motive solide şi legitime” într-o situaţie particulară.

Într-o primă secţiune a capitolului, sunt făcute consideraţii cu privire la evoluţia în reglementare a dreptului general de opoziţie, fiind subliniată absenţa sa din majoritatea primelor legi ale protecţiei datelor din Europa, precum şi din instrumentele internaţionale în materie.

Ulterior, conţinutul dreptului la opoziţie prevăzut de Legea nr. 677/2001 este analizat prin prisma prevederilor corespondente din Directiva 95/46, pentru ca apoi să fie analizată maniera în care conţinutul dreptului a fost dezvoltat în pachetul de reformă privind protecţia datelor în UE. Una din concluziile la care aduce analiza prezentată în Capitolul 5 arată că legiuitorul român a extins cu mult domeniul material de aplicare al dreptului de opoziţie, faţă de prevederile din directivă. Astfel, nu sunt avute în vedere doar prelucrările de date în temeiurile aducerii la îndeplinire a unei sarcini în interes public (art. 7 lit. e) al Directivei 95/46) şi cel al necesităţii în scopul intereselor legitime ale operatorului (art. 7 lit. f) al Directivei 95/46), ci toate prelucrările de date, indiferent de temeiul acestora, adică inclusiv prelucrările întemeiate pe o obligaţie legală a operatorului sau prelucrările întemeiate pe consimţământul persoanei vizate.

În ceea ce priveşte dreptul persoanei vizate de a nu fi supusă unei decizii individuale automate, acesta este contextualizat prin analiza creării de profiluri ca fenomen al economiei

actuale. Apoi, sunt analizate prerogativele pe care le are persoana vizată împotriva efectelor arbitrarii ale creării de profiluri.

Analiza drepturilor persoanei vizate de prelucrarea datelor personale relevă fără îndoială existenţa unui drept general la autodeterminare informaţională garantat prin prevederile specifice protecţiei datelor personale. Persoana vizată nu doar că are dreptul să cunoască existenţa şi detaliile prelucrărilor, ci poate interveni direct asupra acestora prin solicitarea ştergerii, rectificării, actualizării datelor. Mai mult, se poate opune prelucrării, chiar dacă aceasta este făcută într-un temei recunoscut de lege. În principiu, controlul exercitat de persoana vizată asupra imaginii ei informaţionale este substanţial.

Substanţa acestuia este însă diminuată, din mai multe motive, precum domeniul material restrâns de aplicare al unor drepturi, sau excepţiile şi restricţiile reglementate în actele normative privind protecţia datelor – toate analizate şi exemplificate în Partea a II-a a lucrării. Pericolul celei mai semnificative diminuări provine însă din pasivitatea persoanei vizate. Pentru ca prin intermediul acestor drepturi să se exercite un control asupra identităţii informaţionale a persoanei, aceasta trebuie efectiv să exercite drepturile sale.

În acest sens, **Partea a III-a** a lucrării descrie modalităţile prin care persoana vizată îşi poate apăra drepturile care decurg din conţinutul larg al dreptului la protecţia datelor personale, analizând acţiunile simple în realizarea acestor drepturi, dar şi mai complexa acţiune în răspundere civilă delictuală.

Accesul în justiţie al persoanei vizate pentru apărarea drepturilor sale în legătură cu prelucrarea datelor private are un loc special în sistemul român al protecţiei datelor, întrucât este reglementat în capitolul dedicat „drepturilor persoanei vizate în contextul prelucrării datelor cu caracter personal” al Legii nr. 677/2001, în art. 18 – „dreptul de a se adresa justiţiei”.

Persoana vizată de prelucrarea datelor personale îşi poate apăra prerogativele din conţinutul dreptului la protecţia datelor private prin mecanisme specifice tuturor tipurilor principale de răspundere juridică, dar în special prin răspunderea civilă şi răspunderea administrativ-contravenţională.

În ceea ce priveşte remediile civile, acestea sunt de două feluri. În primul rând, apărarea drepturilor persoanei vizate poate fi făcută prin intermediul acţiunilor în realizarea drepturilor, posibilitate ce decurge din art. 18 alin. (1) al Legii nr. 677/2001. În al doilea rând, dacă persoana vizată consideră că prin prelucrarea nelegală a drepturilor a suferit prejudicii, aceasta are la

dispoziţie o acţiune în răspundere delictuală, în temeiul art. 18 alin. (2) al Legii nr. 677/2001. Aceasta din urmă se referă la orice încălcare a prevederilor legale privind protecţia datelor, nu în mod exclusiv la încălcarea drepturilor persoanei vizate, aşa cum sunt prevăzute în Capitolul IV al legii.

Răspunderea civilă a operatorilor de date şi a persoanelor împuternicite de operatori poate fi angajată şi în temeiurile reglementate de noul Codul Civil în art. 1349 – dispoziţia generală privind răspunderea delictuală, coroborat cu art. 253 – dispoziţie care reglementează răspunderea pentru prejudiciul cauzat prin încălcarea drepturilor nepatrimoniale. Răspunderea contravenţională a operatorului care nu respectă cerinţele impuse de legislaţia privind protecţia datelor personale poate fi angajată în temeiul art. 31 - 35 ale Legii nr. 677/2001 a protecţiei persoanei cu privire la prelucrarea datelor cu caracter personal, care reglementează „contravenţii şi sancţiuni" în materia prelucrării datelor, dar şi în temeiul art. 13 al Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice. Un rol fundamental în aplicarea sancţiunilor în materia protecţiei datelor îl are Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

În ultimul rând, dacă privim în sens larg dreptul la protecţia datelor personale, coroborat cu prerogativele specifice dreptului la respectul vieţii private, atunci putem considera că în materia încălcării acestuia poate fi angajată inclusiv răspunderea penală, conform art. 195 Cod Penal care sancţionează infracţiunea de violare a secretului corespondenţei. De altfel, chiar Legea nr. 677/2001 face referire la infracţiuni în capitolul dedicat sancţiunilor, admiţând că unele caracteristici ale contravenţiilor reglementate în cuprinsul său pot să se transforme în conţinutul „unei infracţiuni", fără a reglementa însă o astfel de infracţiune. Acest aspect nu face însă parte din scopul prezentei lucrări şi nu va fi analizat.

Deşi există o inflaţie de mijloace de apărare a prerogativelor ce sunt conferite persoanei prin garantarea dreptului la protecţia datelor personale, acestea sunt rareori utilizate. Conform datelor preliminare din cadrul unui raport al Agenţiei Uniunii Europene pentru Drepturi Fundamentale („Data Protection: Redress Mechanisms and Their Use", 2010) dedicat mecanismelor de reparare a prejudiciilor cauzate în materia prelucrării datelor personale şi realizat cu informaţii din 16 state membre UE, printre care şi România, cauzele în justiţie cu privire la protecţia datelor sunt puţine şi dispersate între o varietate de instanţe şi repararea

prejudiciilor în materia protecţiei datelor este centrată în jurul autorităţilor naţionale de supraveghere.

Aceste realităţi au mai multe explicaţii de natură normativă şi instituţională, dar, în acelaşi timp, sunt justificate şi prin prisma atitudinii pe care cetăţenii europeni, în general, şi cei români, în special, o au faţă de prelucrarea datelor lor personale. Conform celui mai recent Eurobarometru în materie (Eurobarometrul nr. 359), publicat în 2011, 33 la sută dintre europeni şi 39 la sută dintre români sunt „total de acord" că dezvăluirea de informaţii personale nu este o problemă majoră a lor, în timp ce 70 la sută din europeni şi 61 la sută din români au încredere totală că autorităţile publice naţionale le protejează informaţiile personale.

Capitolul 6 analizează acţiunile civile în realizarea drepturilor la care au acces persoanele vizate, marcând distincţia între temeiurile legale care prevăd măsuri în realizarea drepturilor persoanei vizate, pe de o parte, şi repararea daunelor produse prin prelucrările nelegale de date, în general, pe de altă parte. De asemenea, sunt discutate câteva aplicaţii practice ale acţiunilor în realizare. Spre exemplu, este subliniată confuzia făcută de actorii sistemului judiciar român în ceea ce priveşte dreptul de acces la propriile date şi dreptul de acces la informaţiile publice (Secţiunea 3).

Legiuitorul român a înţeles să garanteze procedural ocrotirea prerogativelor persoanei vizate în ceea ce priveşte prelucrarea datelor personale conferind *expressis verbis* un „drept de a se adresa justiţiei". Faptul că accesul la justiţie în cazul unei prelucrări nelegale a datelor personale este garantat sub forma unui drept subiectiv de sine stătător de către Legea nr. 677/2001 face din sistemul român al protecţiei datelor un sistem pregătit să ocrotească cât se poate de eficient persoana vizată. Doar „pregătit", deoarece eficienţa ocrotirii efective este influenţată de mai mulţi factori, precum nivelul de informare al persoanei vizate cu privire la pericolele pe care prelucrarea de date personale nelegale le are, dar şi nivelul de cunoaştere al actorilor sistemului de justiţie – magistraţi şi avocaţi, cu privire la mecanismele de protecţie ale persoanei în contextul prelucrărilor datelor sale personale, sau responsabilitatea pe care operatorii de date trebuie să şi-o asume în ceea ce priveşte prelucrările pe care le întreprind. Or, din toate aceste puncte de vedere, eficienţa ocrotirii drepturilor persoanei vizate prin acţiuni civile este încă aşteptată să se manifeste.

În ceea ce priveşte dreptul persoanei vizate de a se adresa justiţiei conform legii române, acesta conferă titularului său toate premisele pentru facilitarea realizării protecţiei datelor,

stabilind regula competenţei instanţei de domiciliu a persoanei vizate pentru acţiunile în apărarea drepturilor prevăzute de Legea nr. 677/2001 şi scutind de timbru judiciar aceste acţiuni. De asemenea, din punct de vedere substanţial, potenţialele acţiuni în apărarea drepturilor persoanei vizate acoperă întreaga sferă a încălcărilor acestora.

În acest capitol sunt descrise condiţiile de exercitare ale acţiunilor în realizarea drepturilor persoanei vizate în contextul prelucrării datelor personale, analizând în detaliu prevederile Legii nr. 677/2001. Este prezentat însă şi argumentul conform căruia nu doar drepturile persoanei vizate înţelese *stricto sensu* – dreptul de acces la date, dreptul de intervenţie, dreptul de opoziţie, dreptul de a nu fi supus unei decizii individuale, pot fi apărate prin intermediul acţiunilor civile în realizare, ci acestea pot avea în vedere ocrotirea oricărui drept corelativ obligaţiilor operatorului de date strict reglementate de legea specială.

Ca şi particularităţi, a fost argumentată lipsa interesului determinat pentru înaintarea unei acţiuni în realizarea dreptului la informare şi a fost prezentată confuzia între dreptul de acces la propriile date şi dreptul de acces la informaţiile de interes public, prezentă în practica instanţelor române şi care a fost tranşată în cele din urmă de Curtea Europeană a Drepturilor Omului, în cauza *Trăilescu*.

De asemenea, este analizată calitatea procesuală pasivă în cadrul acestor acţiuni, fiind prezentate conceptele de operator de date şi de persoană împuternicită de operator. A fost propusă, în acest context, o regulă generală de care se poate ţine cont în stabilirea domeniului material al normelor legii privind protecţia datelor: „nu există o prelucrare de date personale fără operator, precum nici operator fără o prelucrare de date”. Această perspectivă uşurează probarea existenţei unei persoane responsabile pentru îndeplinirea obligaţiilor în legătură cu prelucrările de date personale, aşa cum am arătat în cazul identificării motoarelor de căutare online ca fiind operatori de date cărora le sunt opozabile obligaţiile legale din materia protecţiei datelor.

Cu privire la calitatea procesuală pasivă în acţiunile civile prin care sunt apărate drepturile persoanei vizate, am observat că, în cazul acţiunii în realizarea dreptului de a nu fi supus unei decizii individuale, în funcţie de elementele *de facto* ale fiecărei situaţii, este posibil ca un terţ faţă de prelucrarea datelor să aibă calitate procesuală pasivă, având în vedere că în temeiul acestui drept pot fi revocate ori modificate „decizii” luate în baza unor profiluri create în mod automat.

Capitolul 7 al lucrării cuprinde o radiografie a răspunderii civile delictuale pentru prejudiciile aduse prin încălcarea drepturilor nepatrimoniale, având în vedere, pe de o parte, că art. 18 alin. (2) al Legii nr. 677/2001 prevede posibilitatea persoanei vizate de a obţine repararea prejudiciului cauzat printr-o prelucrare nelegală a datelor şi, pe de altă parte, că noul Cod civil creează un sistem complex de reparare a prejudiciului adus prin încălcarea drepturilor nepatrimoniale.

Se argumentează în secţiunile acestui capitol că răspunderea pentru prejudiciul cauzat prin încălcarea drepturilor nepatrimoniale prezintă caracteristici care ne îndreptăţesc să considerăm că, odată cu intrarea în vigoare a noului Cod civil, regimul răspunderii delictuale în dreptul civil român a fost îmbogăţit cu un tip autonom de răspundere în cazul creării de prejudicii prin încălcarea drepturilor nepatrimoniale. În acest sens, în primul rând, trebuie avut în vedere faptul că există un temei legal de sine stătător în noul Cod civil dedicat reparării prejudiciilor, patrimoniale şi nepatrimoniale, create prin încălcarea drepturilor nepatrimoniale – art. 253 alin. (4) NCC. Acesta reprezintă o individualizare a temeiului general ce reglementează răspunderea delictuală în noul Cod – art. 1349 NCC.

În al doilea rând, trebuie avută în vedere reglementarea în noul Cod civil a unui sistem complex de reparaţie a prejudiciului cauzat prin încălcarea drepturilor nepatrimoniale – ce are în vedere atât măsuri nepatrimoniale obişnuite şi de urgenţă, cât şi măsuri compensatorii de natură patrimonială.

În al treilea rând, în urma analizei temeiului legal autonom, doctrinei semnificative în materia reparării daunelor morale, şi, mai ales, practicii instanţelor în ceea ce priveşte angajarea răspunderii pentru prejudiciul cauzat prin încălcarea drepturilor nepatrimoniale [căreia îi este dedicată o parte semnificativă a acestui capitol], rezultă o reconfigurare a condiţiilor generale clasice necesare angajării răspunderii delictuale. Acestea trebuie supuse unei verificări complexe, ce are în vedere jurisprudenţa Curţii Europene a Drepturilor Omului, şi care va trebui să aibă în vedere jurisprudenţa Curţii de Justiţie a Uniunii Europene în materia drepturilor fundamentale, dar şi limitele drepturilor nepatrimoniale reglementate exhaustiv în noul Cod civil.

În concluzie, răspunderea pentru prejudiciului cauzat prin încălcarea drepturilor nepatrimoniale are un loc autonom, caracterizat de multe particularităţi, în regimul legal al răspunderii delictuale din dreptul civil român.

Astfel, temeiul legal autonom pentru angajarea răspunderii operatorilor de date pentru prejudiciile cauzate prin prelucrarea ilegală de date personale trebuie aplicat şi interpretat în sistemul complex al întregului mecanism al răspunderii delictuale reglementat în dreptul civil român. Acest sistem, în cazul protecţiei datelor, poate fi imaginat ca o păpuşă Matrioşka. Cea mai mică dintre „păpuşi" este reprezentată de ipoteza art. 18 alin. (1) şi alin. (2) al Legii nr. 677/2001, care este cuprinsă de ipoteza răspunderii delictuale pentru încălcarea drepturilor nepatrimoniale conform art. 253 alin. (4) NCC, şi care, la rândul său, este cuprinsă de prevederea generală a răspunderii delictuale, conform art. 1349 NCC. Aşadar, fiecare dintre ipoteze are propria individualitate şi existenţă de sine stătătoare. Ele pot fi însă utilizate şi ca un tot, această caracteristică fiind cea care conferă întregului sistem unicitate, şi eficienţă în ocrotirea drepturilor persoanei vizate de prelucrările datelor personale şi, în ultimă instanţă, a dreptului la protecţia datelor personale.

Având în vedere că dreptul la protecţia datelor personale este un drept subiectiv nepatrimonial, dispoziţiile art. 252-256 NCC îi sunt aplicabile, pornind de la regulile privind sistemul mixt de reparare a prejudiciului nepatrimonial, până la regulile privind grila de condiţii necesare pentru angajarea răspunderii delictuale a celui care încalcă acest drept şi creează, astfel, cel puţin un prejudiciu nepatrimonial. Iar specializarea răspunderii delictuale pentru prejudiciile cauzate prin prelucrarea nelegală de date personale, conform art. 18 al Legii nr. 677/2001, are drept consecinţă aplicarea sistemică a prevederilor legale privind protecţia datelor, conţinute în legile speciale, pentru determinarea caracterului ilicit al faptei prejudiciabile.

Capitolul 8 detaliază mijloacele de apărare a drepturilor persoanei vizate pe cale administrativă, introducând Autoritatea Naţională pentru Supravegherea Prelucrării Datelor cu Caracter Personal, competenţele acesteia şi procedurile sale specifice.

Conform punctului 62 al Preambulului Directivei 95/46, în general, autorităţile de supraveghere a prelucrării datelor personale sunt fundamentale pentru un sistem de protecţie a datelor eficient. Rolul lor nu este doar acela de a sancţiona administrativ nerespectarea drepturilor persoanelor vizate, ci acela de a fi o parte integrantă a sistemului de protecţie a datelor, acţionând pe mai multe nivele: sancţionator, normativ, consultativ. De aceea înfiinţarea autorităţilor naţionale de supraveghere a fost impusă ca standard de armonizare în UE prin art. 28 al Directivei 95/46. Conform acestuia, fiecare stat membru prevede una sau mai multe autorități publice care să fie responsabile de supravegherea aplicării pe teritoriul său a dispozițiilor

adoptate de statele membre în temeiul directivei şi care acţionează în condiţii de independenţă deplină în exercitarea atribuţiilor cu care sunt învestite.

Competenţele minime pe care o agenţie de supraveghere a unui stat membru trebuie să le aibă, conform art. 28 alin. (3) al Directivei 95/46 sunt (i) competenţe de investigare, (ii) competenţe efective de intervenţie – precum competenţa de a emite avize înainte de începerea prelucrării, de a ordona blocarea, ştergerea sau distrugerea datelor, şi (iii) competenţa de a acţiona în justiţie în cazul încălcării dispoziţiilor legii naţionale a protecţiei datelor. La acestea se adaugă competenţa de organ consultativ legislativ (iv), conform art. 28 alin. (2).

Sancţiunile care pot fi aplicate pentru nerespectarea obligaţiilor ce decurg din legile privind protecţia datelor sunt stabilite de statele membre, fără ca acestora să le fie impus vreun prag de valoare pentru amenzi sau tipul de răspundere care poate fi angajată de către operatori. Conform unui raport al Agenţiei Drepturilor Fundamentale a UE („Data Protection in the European Union: The role of Data Protection Authorities, 2010) „implementarea acestei prevederi generale la nivel naţional a dus la variaţii semnificative", la care a contribuit şi influenţa legislaţiilor domestice în materie administrativă şi penală, atât în momentul adoptării legilor naţionale privind protecţia datelor, cât şi în aplicarea subsecventă a acestora.

România a ales iniţial să confere rolul de autoritate de supraveghere în materia protecţiei datelor Avocatului Poporului, conform primei forme a Legii nr. 677/2001 adoptată de Parlament. Această opţiune s-a dovedit a fi însă defectuoasă, patru ani mai târziu Parlamentul adoptând o lege specială pentru înfiinţarea unei autorităţi publice noi – ANSPDCP.

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal are, din punct de vedere legal, mijloace eficiente şi în concordanţă cu dreptul Uniunii Europene pentru a asigura o protecţie efectivă a drepturilor persoanei vizate.

Cu toate acestea, activitatea ANSPDCP nu se ridică de multe ori la nivelul competenţelor sale şi rolului fundamental pe care îl are în ocrotirea drepturilor fundamentale ale persoanelor cu privire la prelucrarea datelor personale. Agenţia Drepturilor Fundamentale a Uniunii Europene remarca în raportul citat mai sus, cu privire la activitatea autorităţilor de supraveghere, că „în multe state membre, acestea nu se află în poziţia de a-şi duce la îndeplinire sarcinile în întregime datorită resurselor financiare şi umane limitate pe care le au la îndemână", enumerând şi România printre aceste state membre. Mai mult, Agenţia observă că în mai multe state, printre care Bulgaria, Danemarca, Slovacia şi România, „există un gol între protecţia dreptului la viaţă

privată în teorie, care poate din punct de vedere formal să fie conformă cerinţelor dreptului UE şi dreptului internaţional, şi protecţia acestuia în practică".

Drept concluzie a Părţii a III-a, se poate susţine că persoanele vizate de prelucrarea datelor private au la dispoziţie o panoplie de mijloace juridice pentru a-şi ocroti drepturile ce decurg din materia protecţiei datelor personale. În acest întreg sistem, ele însele au rolul fundamental, întrucât pe măsură ce vor conştientiza riscurile la care se supun prin prelucrarea nelegală a informaţiilor din viaţa privată de către diferiţi operatori de date, vor realiza şi că iniţiativa de a-şi ocroti drepturile fundamentale prin intermediul acestor drepturi procedurale conţinute în dreptul la protecţia datelor personale le aparţine chiar lor. Numai astfel acest sistem normativ extrem de detaliat şi bine construit va putea căpăta şi fond.

În **concluzie**, teza a arătat că drepturile persoanei vizate de a controla prelucrarea datelor sale – respectiv dreptul la informare şi de acces, dreptul de rectificare, dreptul de opoziţie la prelucrare şi dreptul de a se opune unor decizii individuale automatizate, sunt prerogative din conţinutul dreptului subiectiv la protecţia datelor private. De asemenea, a analizat în detaliu particularităţile de transpunere a acestor drepturi din Directiva 95/46 în sistemul de drept român, influenţa pe care jurisprudenţa CEDO o are asupra acestora, cu precădere asupra dreptului de acces la propriile date, dar şi modalitatea în care ele vor fi reglementate în viitorul apropiat în Uniunea Europeană, conform pachetului de reformă a protecţiei datelor în UE. Întregul demers duce la concluzia că persoana are suficiente instrumente juridice pentru a-şi proteja drepturile personalităţii în societatea informaţională. Pentru ca acestea să fie eficiente, trebuie ca persoana să conştientizeze, pe de o parte, riscurile pe care le presupune prelucrarea şi stocarea digitală a datelor sale personale, şi, pe de altă parte, existenţa drepturilor sale şi modalităţile în care pot fi folosite.