REALIZAREA DREPTULUI LA PROTECŢIA DATELOR CU CARACTER PERSONAL

Gheorghe AVORNIC,
doctor habilitat în drept, profesor universitar (USM)
Veronica MOCANU,
doctorand (USM)

SUMMARY

The recent institutionalisation of protection of data with a personal character as a juridical reality in the Republic of Moldova determines the necessity of the elaboration of some evaluation studiies of the regulation framwork and the interpretation of the prescribed norms.

The defense of the right of protection of data with a personal character is a rather important subject, because the existence of such a mechanism contributes to the realization de facto of the law.

There have been analyzed the modalities of defending the of the right of data protection with a personal character, institutionalized and state defense; instruments that can be utilized by the subject referred in the realization of defense.

Some norms are proposed to be introduced in the chapter "the obligations of the operator" in order to take adequate measures as to the protection of data with personal character.

Instituţionalizarea recentă a protecţiei datelor cu caracter personal ca realitate juridică în Republica Moldova determină necesitatea elaborării unor studii de evaluare a cadrului de reglementare şi de interpretare a normelor prescrise, indicând, în caz de necesitate, lacunele şi perspectivele în dezvoltare.

Dreptul protecţiei datelor cu caracter personal se prezintă ca totalitatea normelor juridice stabilite sau sancţionate de stat, care fixează cadrul juridic de protecţie a datelor cu caracter personal, stabilind căile şi mijloacele de apărare, în vederea asigurării exercitării libere a acestor date, ca atribute indispensabile fiinţei umane, care la nevoie pot fi impuse prin forţa de constrângere a statului.

Apărarea dreptului la protecţia datelor cu caracter personal este un subiect destul de important, căci anume existenţa unui astfel de mecanism contribuie la realizarea de facto a dreptului. Abordând problematica apărării dreptului la protecţia datelor cu caracter personal, se va ţine cont de complexitatea dreptului şi de caracterul conex al acestuia. În cele ce urmează, vom concepe modalităţi de apărare a dreptului la protecţia datelor cu caracter personal ca un sistem de măsuri individuale, instituţionale sau statale, îndreptate spre prevenirea prejudicierii şi/sau sancţionarea comportamentului fraudulos şi/sau recompensarea prejudiciului adus. Totodată, considerăm necesar a deosebi noţiunea de „modalităţi de apărare a dreptului" de cea de „mijloace de apărare a dreptului", ele fiind privite ca noţiuni întreg-parte. Mijloacele de apărare a dreptului protecţiei datelor le vom privi ca pe nişte instrumente de realizare a apărării dreptului de protecţie a datelor.

Pornind de la cele indicate, constatăm că modalităţile de apărare a dreptului protecţiei datelor cu caracter personal sunt determinate de subiecţii ce le exercită. Vom deosebi: *autoapărarea, apărarea instituţionalizată* şi *apărarea statală*. Mijloacele de apărare însă desemnează instrumentele care pot fi utilizate de subiectul vizat în realizarea apărării. Astfel, vom deosebi *răspunderea penală, administrativă, disciplinară* şi *civilă.*

În sensul celor indicate, autoapărarea va fi privită ca una dintre principalele modalităţi de exercitare a apărării datelor cu caracter personal, fiind percepută ca un set de acţiuni ale persoanei vizate, îndreptate spre preîntâmpinarea prejudicierii datelor sale personale sau acţiuni legate de recunoaşterea şi recompensarea prejudiciului suferit. Ca exemplificare a acţiunilor de autoapărare preventive pot servi măsurile de precauţie necesare a fi luate de persoana vizată în contextul exploatării datelor personale, exercitarea cu diligenţă a drepturilor sale, realizarea controlului asupra oricărui proces de prelucrare de date, verificarea scopului prelucrării, identităţii operatorului, pertinenţei acţiunilor întreprinse de operator vizavi de datele sale.

Acţiunile legate de recunoaşterea şi recompensarea prejudiciului suferit vor fi realizate prin utilizarea normelor de procedură civilă şi adresarea în instanţele de judecată. Art. 11 CC RM prevede metodele de apărare a drepturilor civile: recunoaşterea dreptului, restabilirea situaţiei anterioare încălcării dreptului şi suprimarea acţiunilor prin care se încalcă dreptul sau se creează pericolul încălcării lui; recunoaşterea nulităţii actului juridic civil; declararea nulităţii actului emis de o autoritate publică; impunerea la executarea obligaţiei în natură; autoapărarea; repararea prejudiciului; încasarea clauzei penale; repararea prejudiciului moral; desfiinţarea sau modificarea raportului juridic; neaplicarea de către instanţa de judecată a actului ce contravine legii, emis de o autoritate publică. În art. 10-13 CC RM sunt reglementate modalităţile generale de apărare a tuturor drepturilor civile.

Codul civil al RM prevede şi modalităţi speciale de apărare a drepturilor personale nepatrimoniale. Art. 15 din CC RM prevede că drepturile personale nepatrimoniale şi alte valori nemateriale sunt apărate în cazurile şi în modul prevăzut de cod şi de alte legi, în limita în care folosirea modalităţilor generale de apărare a drepturilor civile reiese din esenţa dreptului încălcat şi din caracterul consecinţelor acestei încălcări. În atare context, se poate face trimitere la normele Legii privind protecţia datelor cu caracter personal. Totodată, art. 14 CC RM conţine reglementări cu privire la repararea prejudiciului. Persoana lezată într-un drept al ei poate cere repararea integrală a prejudiciului cauzat. În explicaţia dată de Comentariul Codului civil al RM, posibilitatea persoanelor juridice de a apela la metoda de reparare a prejudiciilor rezultă din faptul lezării lor în drepturi, indiferent de faptul dacă norma Codului conţine sau nu asemenea prevederi. Metodei de reparare a prejudiciului îi este atribuit un caracter universal de apărare a drepturilor civile. Această metodă poate fi combinată cu alte metode de apărare[1]. Constatăm că una dintre metodele de realizare a autoapărării datelor personale este atragerea la răspunderea civilă, iar ca finalităţi ale acesteia, potrivit legislaţiei civile a RM, pot fi percepute acţiunile legate de recunoaşterea dreptului, restabilirea situaţiei anterioare încălcării dreptului şi suprimarea acţiunilor prin care se încalcă dreptul sau se creează pericolul încălcării acestuia, recunoaşterea nulităţii actului juridic încheiat în temeiul unei evaluări eronate de date, declararea nulităţii actului emis de o autoritate publică în temeiul unei aprecieri incorecte de date, impunerea la executarea anumitei obligaţii de prejudiciere (ca, de exemplu, publicarea sau difuzarea unei informaţii ce ar dezminţi o informaţie prezentată anterior, formată în urma unei aprecieri greşite de date), încasarea clauzelor penale în cazul în care există oarecare acorduri în acest sens între operator şi persoana vizată, repararea prejudiciului moral, desfiinţarea sau modificarea anumitor raporturi juridice formate între operator şi persoana vizată ş.a.

Autoapărarea ca mijloc de exercitare a apărării drepturilor este prevăzută şi de legislaţia RM, art.11 lit.f) CC RM, ea fiind percepută ca o nouă modalitate de apărare a drepturilor atât patrimoniale, cât şi personale nepatrimoniale. Această modalitate trebuie deosebită de extrema necesitate şi legitima apărare, deoarece exclude situaţii extremale. Persoanele pot să înceapă apărarea de sine stătător în condiţii normale. De exemplu, să ia bunul ce-i aparţine cu drept de proprietate de la persoana care îl posedă nelegal. Nu vom fi de acord cu abordarea dată de Comentariul Codului civil al RM, precum că autoapărarea este exclusiv o măsură prealabilă de apărare şi se realizează fără adresarea în instanţa de judecată sau la alt organ competent, care realizează apărarea drepturilor civile încălcate[2]. Ne vom argumenta poziţia pornind de la ideea că adresarea cu o plângere către o autoritate de supraveghere sau adresarea unei cereri de chemare în judecată, de asemenea, sunt nişte mijloace de autoapărare, căci nu în tot cazul intervin autorităţile statale, de multe ori acestea trebuie sesizate pentru ca să intervină. Mai mult decât atât, răspunderea juridică civilă nu se declanşează din oficiu, ci doar la cererea titularului dreptului subiectiv lezat. De multe ori, autoapărarea este un imbold şi pentru declanşarea celorlalte modalităţi de apărare a datelor, inclusiv instituţionale şi statale.

Conform logicii propuse, o altă modalitate de apărare a datelor cu caracter personal este cea instituţională. Datorită faptului că controlul asupra prelucrării de date se realizează atât din interior, cât şi din exterior, propunem diferenţierea modalităţilor de apărare a datelor cu caracter personal instituţionale în *interne* şi *externe*. La rândul lor, ele putând fi realizate prin diferite mijloace – cea internă poate face recurs la normele disciplinare, cea externă poate fi realizată prin intermediul trimiterii la răspunderea administrativă şi penală.

Realizarea sistemului de apărare instituţională internă este fundamentată pe principiul responsabilităţii, presupunând atribuirea unui set de obligaţii operatorilor de date sau persoanelor împuternicite de către instituţia în care aceştia activează şi cărora li se impune urmarea unui anumit comportament[3].

De obicei, nerespectarea normelor interne atrage răspunderea disciplinară, dar nu se exclude şi utilizarea celorlalte forme de apărare a dreptului de proprietate, înaintarea acţiunii reparatorii, sau autosesizarea organelor de control şi aplicarea sancţiunilor penale în cazul în care legislaţia permite acest fapt.

La categoria mijloacelor instituţionale de apărare externă, putem atribui acţiunile autorităţilor de control şi supraveghere, de adresare în judecată în vederea apărării intereselor persoanei vizate, sau acţiunile organelor de ocrotire a normelor de drept ce se autosesizează în contracararea unui comportament fraudulos – dacă legea naţională prevede această posibilitate.

După cum se vede din definiţia dreptului protecţiei datelor cu caracter personal, enunţată la început, unul dintre elementele principale ce caracterizează dreptul protecţiei datelor este forţa de constrângere a statului. Prin esenţa sa, forţa de constrângere a statului reprezintă o totalitate de măsuri, acţiuni concepute în vederea realizării dreptului. Pe de altă parte, constrângerea caracterizează răspunderea juridică, aceasta fiind definită ca o măsură coercitivă aplicată de către stat pentru comiterea unei fapte ilicite şi exprimată prin aplicarea unor sancţiuni cu caracter material, organizaţional sau de ordin personal[4]. În cele ce urmează, ne propunem să abordăm constrângerea statală ca modalitate de apărare a dreptului la protecţia datelor cu caracter personal şi să identificăm formele de realizare a acesteia în contextul protecţiei datelor cu caracter personal. Totodată, pornind de la ideea că ne-am propus să realizăm o abordare teoretico-juridică a domeniului protecţiei datelor cu caracter personal, vom încerca să clarificăm aplicabili-

tatea fundamentelor teoretice generale asupra conţinutului instituţiei cercetate, evidenţiind particularităţile specifice.

Analizând răspunderea juridică în domeniul protecţiei datelor cu caracter personal, ne propunem să elucidăm problematica principiilor răspunderii juridice în acest domeniu, condiţiile şi formele, ori examinarea răspunderii juridice prin prisma teoriei generale a dreptului, a filosofiei dreptului şi a sociologiei juridice, cu depăşirea graniţelor, de altfel fireşti şi necesare, ale abordării în cadrul disciplinelor juridice de ramură ce favorizează aprofundarea cercetării[5]. Există diferite viziuni în ceea ce priveşte tratarea noţiunii şi conţinutului răspunderii juridice, însă în general aceasta este privită ca o instituţie, o totalitate de norme sau un mecanism de atragere la răspundere, de sancţionare a tuturor celor care încalcă sau ignoră ordinea de drept, în scopul asigurării respectării şi promovării ordinii de drept şi binelui public[6]. În sensul celor indicate, ţinând cont de complexitatea instituţiei, vom menţiona că răspunderea juridică în domeniul protecţiei datelor cu caracter personal poate fi privită ca un mecanism de atragere la răspundere, de sancţionare a tuturor celor care încalcă sau ignoră normele de protecţie a datelor cu caracter personal.

Abordând problema răspunderii ca modalitate de apărare a dreptului protecţiei datelor cu caracter personal, considerăm necesar a cerceta condiţiile răspunderii juridice şi considerăm important să ne oprim asupra tratării următoarelor: fapta ilicită, existenţa prejudiciului sau rezultatului dăunător, materializarea legăturii cauzale dintre fapta ilicită şi consecinţele care au survenit, vinovăţia.

Din perspectivele domeniului de protecţie a datelor cu caracter personal, fapta ilicită va fi percepută ca orice conduită contrar dispoziţiilor normelor juridice. În acest context, ţinem să remarcăm că vor fi percepute ca fapte ilicite atât acţiunile, cât şi inacţiunile. Inacţiunea sau omisiunea, ca şi acţiunea, are un caracter conştient şi voluntar, îndreptat spre realizarea unui scop, care poate fi şi pasivitatea faţă de o îndatorire[7].

În contextul indicat, neîndeplinirea obligaţiei de către operatorul de notificare a subiectului vizat, faţă de prelucrarea ce se realizează asupra datelor sale, de asemenea va fi privită ca o faptă ilicită. Tot la categoria de fapte ilicite, va fi atribuită şi acţiunea (inacţiunea) operatorului legată de neîntreprinderea măsurilor de securizare a datelor, lipsa dotărilor tehnice prescrise ca necesare, ori „a nu evita un efect, cu toate că există o obligaţie juridică de a-l împiedica să aibă loc, este acelaşi lucru cu a-l cauza”[8]. Totodată, ţinem să remarcăm că va fi percepută ca faptă ilicită orice conduită contrar dispoziţiilor oricăror norme juridice. Se vor lua în calcul atât normele voluntare ca norme cu prescripţie obligatorie, cât şi cele normative publice, iar în caz de suprapunere, se vor aplica ambele seturi de norme, ca exemplu poate servi destituirea din funcţie ca sancţiune disciplinară conform normelor voluntare şi aplicarea privaţiunii de libertate ca normă penală. În acelaşi timp, vor fi luate în calcul şi normele naţionale, şi cele internaţionale. Datorită specificului domeniului, se pot întâmpla situaţii când se aplică simultan normele naţionale publice şi normele internaţionale private. Unui operator de date i se poate aplica drept sancţiune naţională lipsirea de dreptul de a fi operator de date, iar ca sancţiune la nivel internaţional, aplicată de o entitate privată internaţională, poate fi lipsirea de dreptul de a face parte dintr-o anumită entitate cu jurisdicţie regională sau internaţională.

Prin esenţa lor, normele juridice protejează un anumit set de valori, iar fapta ilicită se prezintă ca un atentat sau o fraudare a acestor valori. Din perspectiva celor indicate, o problemă importantă de clarificat ține de calificarea comportamentului ilicit. Regula generală prescrie că calificarea faptei se realizează ținându-se cont de valorile asupra cărora se reflectă prejudiciul. În dependenţă de domeniul care a fost prejudiciat, vom identifica diferite forme ale răspunderii juridice.

A doua condiţie determinantă a răspunderii juridice este legată de rezultatul pe care-l produce sau poate să-l producă fapta ilicită. Prejudiciile se diferenţiază în dependenţă de natura lor, identificându-se *prejudicii patrimoniale* şi *nepatrimoniale.* Prejudiciul patrimonial este consecinţa săvârşirii faptei ilicite, ce constă într-o pierdere patrimonială, adică prejudiciul patrimonial are un conţinut economic, putând fi evaluat pecuniar[9]. Prejudiciul nepatrimonial, sau dauna morală, este consecinţa dăunătoare care nu poate fi evaluată în bani şi rezultă din atingerile şi încălcările drepturilor personale nepatrimoniale (dreptul la viaţă, sănătate, integritate corporală, demnitate, prestigiu)[10]. În contextul protecţiei datelor cu caracter personal, suntem de părerea că se pot materializa atât prejudicii materiale şi nemateriale, cât şi complexe. Ca exemplu ar fi situaţia în care datorită difuzării unor date cu caracter personal, individului i s-a lezat demnitatea, dar în acelaşi timp acesta a fost şi concediat, suportând astfel pe lângă prejudiciile nepatrimoniale şi prejudicii patrimoniale. Determinarea caracterului prejudiciului este importantă şi din perspectiva încadrării juridice a faptei şi delimitării formei de răspundere necesară a fi aplicată.

Rezultatul socialmente periculos este legat de săvârşirea conduitei ilicite, cu care se află într-o strânsă legătură de cauzalitate[11]. În sensul protecţiei datelor cu caracter personal, nu va fi considerat necesar de atras la răspundere operatorul, a cărui sistem de protecţie aplicabil unei baze de date a fost afectat de o situaţie de forţă majoră care nu putea fi preîntâmpinată. Noţiunea de vinovăţie este mai mult caracteristică pentru răspunderea penală şi administrativă, noi însă vom insista asupra abordării acesteia ca o condiţie obliga-

torie a răspunderii juridice, indicând că în contextul răspunderii civile va fi evaluat caracterul culpabil al faptei.

După N. Popa, vinovăţia este percepută ca o atitudine psihică faţă de fapta ilicită şi urmările acesteia, însă o anumită atitudine psihică, şi anume, o atitudine subiectiv negativă de ignorare a regulilor juridice instituite de societate, considerate valabile şi acceptate ca valoroase la un anumit moment dat, în sistemul general axiologic al acelui moment[12]. Ca forme de materializare a vinovăţiei în determinarea comportamentului fraudulos în domeniul protecţiei datelor cu caracter personal vom lua în considerare atât intenţia, cât şi culpa. Culpa este acea formă a vinovăţiei în care autorul unei fapte ilicite nu prevede consecinţele faptei sale, deşi trebuia să le prevadă sau prevăzându-le spera în mod uşuratic că ele nu se vor produce[13]. Prin luarea în calcul a culpei ca o condiţie obligatorie în determinarea răspunderii juridice, se realizează responsabilizarea subiecţilor implicaţi în realizarea prelucrării de date, aceştia vor fi cointeresaţi nu doar în prelucrarea de date, dar şi de securizarea procesului, în aşa fel încât nici chiar din imprudenţă să nu fie afectate datele personale ale individului. Ca determinante ale caracterului culpabil sau vinovat, vom lua în considerare atât factorul intelectiv, cât şi cel volitiv.

Analizând problema vinovăţiei, este necesar a identifica subiecţii cărora aceasta li se poate imputa. Din perspectiva legislaţiei europene, subiecţi ai răspunderii în domeniul protecţiei datelor cu caracter personal întotdeauna sunt persoanele ce prelucrează date, noi însă propunem realizarea unei diferenţieri a subiecţilor faţă de care poate fi aplicată răspunderea juridică în dependenţă de statutul. Vom deosebi subiecţi autorizaţi, dar care au un comportament ilicit, şi subiecţi neautorizaţi cărora, de asemenea, le poate fi prescris un comportament fraudulos.

În contextul subiecţilor autorizaţi, vom identifica în general operatorii de date şi persoanele împuternicite. Acestora le poate fi aplicată una din formele răspunderii juridice, atunci când comportamentul lor se abate de la cel prescris sau autorizat. Din perspectiva Directivei, va fi considerată ca persoană căreia i se poate aplica una din formele răspunderii juridice orice operator ce nu şi-a îndeplinit obligaţiile prescrise de art.6 al Directivei 46/95. Printre aceste obligaţii indicăm prelucrarea corectă şi legală a datelor, realizarea colectării doar în scopuri determinate, explicite şi legitime şi cu condiţia neprelucrării ulterioare într-un mod incompatibil cu aceste scopuri. Colectarea de date trebuie să fie adecvată, pertinentă şi neexcesivă. În caz de necesitate, operatorul trebuie să actualizeze datele colectate şi să ia toate măsurile ca datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate să fie şterse sau rectificate. Tot în contextul detalierii comportamentului prescris, Directiva la art.17 indică statelor-membre obligaţia de a impune operatorilor imperativul asigurării măsurilor tehnice şi organizatorice de protecţie, adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat, în special atunci când prelucrarea presupune transmiterea datelor într-o reţea, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Dacă analizăm sistemul răspunderii juridice aplicabil operatorilor şi persoanelor împuternicite, stabilim de fapt că aceasta este construită în temeiul principiului responsabilităţii. În acest context, Grupul de lucru indică că există mijloace de stimulare a responsabilităţii proactive şi reactive. În primul caz, acestea urmăresc să asigure aplicarea eficientă a măsurilor de protecţie a datelor şi mijloace suficiente de tragere la răspundere a operatorilor. În al doilea caz, acestea pot implica răspunderea civilă şi sancţiuni pentru a asigura compensarea oricăror prejudicii relevante şi luarea unor măsuri adecvate în vederea corectării erorilor sau greşelilor[14]. Constatăm, de fapt, că realizarea mecanismului de apărare a dreptului la protecţia datelor cu caracter personal este structurat pe două nivele, şi anume, nivelul unu – legat de responsabilizarea operatorilor, şi nivelul doi – legat de recurgerea la constrângere. Totodată, menţionăm că din perspectiva legislaţiei protecţiei datelor cu caracter personal, subiect al răspunderii poate fi atât persoana fizică, cât şi juridică. Se admit şi situaţiile în care întreprinderile şi organismele publice desemnează o anumită persoană ca fiind responsabilă pentru punerea în aplicare a operaţiunilor de prelucrare. Totuşi, chiar şi în cazul în care este desemnată o anumită persoană fizică pentru asigurarea conformităţii cu principiile de protecţie a datelor sau pentru prelucrarea de date cu caracter personal, aceasta din urmă nu va avea rolul de operator, ci va acţiona în numele entităţii juridice (întreprinderea sau organismul public) care, în calitatea sa de operator, va fi răspunzătoare în cazul încălcării principiilor. În special, în cazul structurilor mari şi complexe, este esenţial din perspectiva „guvernanţei protecţiei datelor" să se asigure atât o responsabilitate clară a persoanei fizice care reprezintă întreprinderea, cât şi responsabilităţi funcţionale concrete în cadrul structurii, de exemplu, prin desemnarea altor persoane care să acţioneze în calitate de reprezentanţi sau puncte de contact pentru persoanele vizate. În cazurile în care o persoană fizică din cadrul unei persoane juridice utilizează date în scopuri proprii, în afara domeniului de activitate şi a controlului posibil al activităţilor persoanei juridice, se impune realizarea unei analize speciale. În astfel de situaţii, persoana fizică în cauză ar fi operatorul în legătură cu prelucrarea asupra căreia s-a luat decizia şi ar fi responsabilă pentru această utilizare a datelor cu caracter personal. Totuşi, opera-

torul iniţial ar putea să poarte o anumită responsabilitate dacă noua prelucrare ar avea loc, din cauza lipsei unor măsuri adecvate de securitate[15]. Ţinând cont de faptul că viaţa contemporană are un caracter complex şi de multe ori, înainte de a beneficia de anumite servicii, se impune ca necesitate prelucrarea unui anumit pachet de date de către mai mulţi operatori, în cazul prejudicierii unor interese, apare problema identificării subiectului vinovat şi limitele vinovăţiei sale. În asemenea situaţii, în primul rând, ar trebui să se precizeze că, în special în cazurile în care există un control comun, incapacitatea de îndeplinire directă a tuturor obligaţiilor aferente operatorului (asigurarea informaţiilor, dreptul de acces etc.) nu exclude statutul de operator. Practic, acele obligaţii ar putea fi cu uşurinţă îndeplinite de alte părţi, care sunt uneori mai apropiate de persoana vizată, în numele operatorului. Totuşi, operatorul este cel care va răspunde, în cele din urmă, de îndeplinirea obligaţiilor şi care va fi răspunzător în cazul încălcării acestora. Consecinţele juridice sunt legate şi de răspunderea operatorilor, punându-se în special problema dacă acel „control comun" prevăzut în Directivă atrage întotdeauna răspunderea în solidar. Art.26 cu privire la răspundere utilizează termenul de „operator" la singular, ceea ce indică un răspuns pozitiv. După cum s-a menţionat deja, în realitate pot exista diferite moduri de a acţiona „împreună". Aceasta ar putea determina în anumite cazuri răspunderea în solidar, însă nu în mod necesar: de multe ori, diferiţi operatori pot fi responsabili şi răspunzători pentru prelucrarea datelor personale în diferite etape şi în grade diferite.

Concluzia ce se impune este că, la determinarea persoanei responsabile, trebuie să se ţină seama de statutul juridic al subiectului. Astfel, mai mult decât oricând, este important ca persoanele vizate să fie informate clar cu privire la diferitele etape şi diferitele părţi implicate în prelucrare. În plus, ar trebui precizat dacă fiecare operator are competenţa de a respecta toate drepturile persoanei vizate şi dacă acesta este competent[16].

În cazul celei de a doua categorii de subiecţi, subiecţi neautorizaţi, cărora de asemenea le poate fi prescris un comportament fraudulos din perspectiva exploatării datelor personale, poate fi identificată orice persoană ce prelucrează datele cu caracter personal nu în interes personal, dar de obicei pentru realizarea unor scopuri, profituri. Am insistat asupra acestei deosebiri, deoarece considerăm că normele legale trebuie să prevadă aceste situaţii şi ar trebui să realizeze o diferenţiere expresă de sancţionare şi de existenţă a unor pârghii de sancţionare şi a subiecţilor neautorizaţi. Mai mult decât atât, suntem de părerea că utilizării de date neautorizate trebuie să i se aplice şi răspunderea penală.

Pe lângă existenţa condiţiilor ce determină atragerea la răspundere există şi condiţii ce înlătură răspunderea juridică. La calificarea unei fapte ca faptă ilicită e important să fie luate în considerare toate circumstanţele. Se impune ca necesitate să se ţină cont de cauzele, care exclud răspunderea juridică. Vom admite cauze ce înlătură răspunderea juridică: starea de extremă necesitate, constrângerea fizică sau psihică, riscul întemeiat, forţa majoră. Pornind de la ideea că datele cu caracter personal desemnează o varietate destul de mare de raporturi, constatăm că şi prejudicierea acestor raporturi poate fi destul de diferită, atrăgând diferite reacţii de penalizare din partea statului, materializându-se prin răspunderea administrativă, penală, civilă, materială, disciplinară. Calificarea unei fapte ilicite din domeniul protecţiei datelor cu caracter personal ca infracţiune, contravenţie sau abatere disciplinară variază de la stat la stat, în dependenţă de cultura juridică, practică, abordarea axiologică ş.a. Spre exemplu, în Franţa, împiedicarea controlului efectuat de Comisia Naţională de Informatică şi Libertăţi sau refuzul de a colabora cu membrii ei, persoanele abilitate sau magistraţii şi să-i ofere documentele necesare sau folosirea documentelor, neintroduse în cerere, se sancţionează cu o amendă în valoare de până la 15.000 euro. Cât priveşte Spania, putem remarca următoarele încălcări, care sunt sancţionate pe cale administrativă de către autoritatea de protecţie a datelor cu caracter personal: încălcarea obligativităţii pentru păstrarea confidenţialităţii datelor cu caracter personal; nerespectarea sau împiedicarea sistematică a exercitării dreptului la acces, rectificare, retragere sau protest; ori nerespectarea sistematică a atribuţiei de a notifica persoana privind introducerea datelor cu caracter personal în baza de date, aplicându-se amenzi ce variază de la 600 euro pentru încălcări uşoare şi până la 600.000 euro, pentru încălcări deosebit de grave[17].

Suntem de părerea că faptelor ilicite ce atentează sau prejudiciază datele personale ar trebui să li se prescrie răspunderea penală, administrativă, disciplinară şi civilă ca forme de asigurare şi ocrotire a dreptului la protecţia datelor cu caracter personal.

Mai mult decât atât, legislaţia europeană conţine exemple utile de criterii de atribuire a răspunderii penale, în special atunci când o infracţiune este comisă în folosul persoanei juridice: răspunderea poate fi atribuită în acest caz oricărei persoane, „acţionând fie individual, fie ca parte a unui organ al persoanei juridice, care deţine o poziţie de conducere în cadrul persoanei juridice, bazată pe unul dintre următoarele elemente: puterea de reprezentare a persoanei juridice, puterea de a lua decizii în numele persoanei juridice sau puterea de a exercita controlul în cadrul persoanei juridice[18].

Totodată, insistăm ca răspunderea penală să intervină şi în situaţiile în care prelucrarea de date se realizează de persoane neautorizate în scopul de a obţine

profituri. Ţinând cont de faptul că dreptul protecţiei datelor este un drept conex, adică prin esenţa sa el protejează alte valori, credem că nu ar fi cazul de dublat prevederile legale, atunci când există anumite forme de sancţionare a comportamentului fraudulos ce atentează asupra demnităţii spre exemplu. Soluţia care o propunem se referă la completarea normelor existente, şi nu obligatoriu, instituirea unor norme noi.

Abordarea mijloacelor de protecţie a datelor susceptibile persoanei vizate este o problemă destul de importantă. Importanţa acesteia rezultă şi din faptul că la moment protecţia datelor cu caracter personal are mai mult un caracter declarativ, neexistând nişte pârghii bine definite de atragere la răspundere sau responsabilizare. În contextul reformării domeniului de protecţie a datelor cu caracter personal, cadrul european este preocupat, în primul rând, de reformarea practicilor de responsabilizare şi răspundere. Acţiunile de reformare în domeniul protecţiei datelor cu caracter personal sunt îndreptate, în primul rând, spre responsabilizarea operatorilor şi persoanelor împuternicite de aceştia. Noua „arhitectură juridică" a mecanismelor de responsabilitate în domeniul protecţiei datelor ar putea să prevadă două niveluri: primul nivel ar consta în cerinţele juridice minimale obligatorii pentru *toţi* operatorii de date. Acesta ar cuprinde două elemente: punerea în aplicare a măsurilor/procedurilor şi păstrarea unei evidenţe a lor. Acest prim nivel ar putea fi completat cu cerinţe suplimentare. Al doilea nivel ar cuprinde sisteme voluntare de responsabilitate, care merg dincolo de aceste cerinţe juridice minimale, în ceea ce priveşte principiile subsecvente protecţiei datelor (care prevăd standarde mai ridicate decât cele necesare conform normelor în vigoare) şi/sau în ceea ce priveşte modalităţile de punere în aplicare sau de garantare a eficacităţii măsurilor (punerea în aplicare a cerinţelor care depăşesc nivelul minim)[19]. Totodată, implementarea noilor propuneri se justifică prin faptul că acestea vor conţine mecanisme clare de control chiar în timpul derulării proceselor de prelucrare. La capitolul „obligaţiile operatorului" se propune introducerea unor astfel de norme:

- necesitatea ca operatorul de date să ia măsuri adecvate şi eficiente în vederea aplicării principiilor privind protecţia datelor;
- necesitatea de a demonstra la cerere că au fost aplicate măsuri adecvate şi eficiente. În consecinţă, operatorul de date furnizează dovezi privind îndeplinirea cerinţei punctului de mai sus.

Din cele elucidate, constatăm că cercetarea modalităţilor, mijloacelor şi metodelor de apărare a datelor cu caracter personal este o sarcină destul de importantă, mai ales în condiţiile în care domeniul protecţiei datelor cu caracter personal este unul în formare, iar cercetările ştiinţifice din domeniu s-ar putea impune ca un reper reglementărilor normative sau cel puţin ca nişte puncte de plecare.

Note:

[1] Baieş A., Baieş S., Buruiana O., Buruiană M., Cebotari V., Creţu V., Eşanu N., Efrim O., Gladei R., Mămăligă S., Roşca N., Tabuncic T., Trofimov I., Volcinschi V., *Comentariul Codului civil al RM*, Tipografia Centrală, Chişinău, 2006, vol. I, p.51. – 816 p.

[2] *Ibidem,* p.50.

[3] Avizul 3/2010 privind principiul responsabilităţii. Direcţia C (Drepturi fundamentale şi cetăţenia Uniunii Europene) a Comisiei Europene, Direcţia Generală Justiţie, B-1049 Bruxelles, Belgia, Biroul nr. LX-46 01/190. 2010. p.12, 20 p. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_ro.pdf (vizitat 04.05.2011)

[4] Avornic Gh., Aramă E., Negru B., Costaş R., *Teoria generală a dreptului,* Cartier juridic, Chişinău,2004, p.490.

[5] Popescu S., *Fundamentele răspunderii juridice. Câteva remarci în studiul de drept,* vol. II, Ed. Universitatea Timisiensies, Timişoara, 1998, p.220. – 366 p.

[6] Barac. L., *Câteva consideraţii cu privire la definirea răspunderii juridice,* în *Dreptul,* 1994, nr. 4, p.29.

[7] Vonică R., *Introducere în drept,* Lumina Lex, Bucureşti, 2000, p. 545-546. – 599 p.

[8] Moruzi J., *Problema cauzalităţii în dreptul penal. Raport de cauzalitate,* în *Revista de drept penal*, 1983, nr.4.

[9] Legea Republicii Moldova, Codul civil al Republicii Moldova nr. 726-XII din 04.06.2002, în *Monitorul Oficial al Republicii Moldova,* 22.06.2002, nr. 82-86 (967-971), art.14.

[10] *Ibidem*, art.15.

[11] Popa C., *Teoria generală a dreptului,* Lumina Lex, Bucureşti, 2001, p.287. – 320 p.

[12] Popa N., *Teoria generală a dreptului,* Ed. Actami, Bucureşti, 1998, p.206-207. – 336 p.

[13] Avornic Gh., Aramă E., Negru B., Costaş R., *op.cit.,* p.502.

[14] Avizul Grupului de Lucru nr.1/2010 privind conceptele de „operator" şi „persoană împuternicită de către operator", 16.02.2010, Direcţia D (Drepturi fundamentale şi cetăţenie) a Comisiei Europene, Direcţia Generală Justiţie, Libertate şi Securitate, B-1049 Bruxelles, Belgia, Biroul nr.LX-46 01/190. p.5, 34 p.http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (vizitat 02.08.2011)

[15] *Ibidem.*

[16] *Ibidem,* http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (vizitat 02.08.2011)

[17] Notă de argumentare privind necesitatea modificării şi completării unui şir de acte normative întru asigurarea implementării modificărilor şi completărilor care se propun a fi operate în Legea cu privire la protecţia datelor cu caracter personal http://www.datepersonale.md/file/nota%20de%20argumentare%20alte%20acte11%20-005.pdf (vizitat 009.05.2012)

[18] Avizul Grupului de Lucru nr. 1/2010 privind conceptele de „operator" şi „persoană împuternicită de către operator", 16.02.2010, p.16, 34 p. http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (vizitat 02.08.2011)

[19] Avizul 3/2010 privind principiul responsabilităţii. Direcţia C (Drepturi fundamentale şi cetăţenia Uniunii Europene) a Comisiei Europene, Direcţia Generală Justiţie, B-1049 Bruxelles, Belgia, Biroul nr.LX-46 01/190. 2010, p.6. – 20 p. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_ro.pdf (04.05.2011)