SECURITATEA DATELOR CU CARACTER PERSONAL ÎN CADRUL SISTEMELOR INFORMAȚIONALE

SECURITY OF PERSONAL DATA WITHIN THE INFORMATION SYSTEMS

Teodor CÂRNAȚ, Dr. hab., prof. univ.
USM
Ion COBÎȘENCO, Doctorand
USM

Abstract
The origins of privacy regulation and the establishment of a data protection system have been the need for individuals to establish what they can reveal about themselves. In this sense, we are talking about a system of personal data protection aimed at a contemporary society, a value normally protected in a democratic society, but we must also ignore the right of individuals to free expression. Compliance with these rights to an "equal" is impossible, and this is also the main reason why privacy is not an absolute national or supra-national right.
Keywords: *privacy, personal data, security, information system, democratic society.*

În viața noastră de zi cu zi, computerele au devenit un lucru firesc, ba chiar ceva indispensabil. Nu putem nega faptul că trăim într-o societate informatizată. Dezvoltarea tehnico–științifică, direct sau indirect, afectează securitatea, confidenţialitatea şi integritatea datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale de date cu caracter personal.

La originea reglementării intimității și stabilirea unui sistem de protecție a datelor a stat nevoia indivizilor de a stabili ceea ce pot dezvălui despre ei înșiși. În această accepțiune, vorbim despre un sistem de protecție a datelor cu caracter personal vizând o societate contemporană, valoare protejată în mod normal într-o societate democratică, însă nu trebuie să ignorăm nici dreptul persoanelor la libera exprimare. Respectarea acestor drepturi într-o măsură „egală” este imposibilă, or, acesta este și motivul principal pentru care intimitatea nu este un drept absolut la nivel național sau supra-național (Carp, Șandru, 2004, p.5).

La nivel Constituțional există mai multe articole care reglementează aspecte ale vieții private, în sensul larg al termenului. Potrivit art. 28 din Constituția Republicii Moldova, statul respectă şi ocroteşte viaţa intimă, familială şi privată. Suplimentar, Legea fundamentală a statului asigură o protecție vieții private prin art. 29 „Inviolabilitatea domiciliului” și art. 30 „Secretul corespondenţei”. În concepția Curții Europene chiar și dreptul la un mediu sănătos ține tot de viața privată a persoanei, astfel încât ar fi incidentă în

cauză și reglementarea acestui drept în Constituția Republicii Moldova, respectiv art. 39 intitulat „Dreptul la un mediu înconjurător sănătos” (Răduleț, 2008, p. 205).

Teoria fundamentelor constituționale impune încadrarea dreptului la respectarea vieții private în sistemul drepturilor fundamentale orientat către perceperea în plan juridic a persoanei umane. Conținutul dreptului la respectarea vieții private în plan constituțional trebuie poziționat în raport de necesitatea demarării unui proces general al constituționalizării personalității umane prin prisma libertății personale sau individuale, raportate la demnitatea umană sau a liberei dezvoltări (Drăghici, 2011, p. 29).

Actele internaționale, inclusiv cele la nivel continental statuează că drepturile omului, în general, să unească profiluri diferite referitoare la dreptul la viața privată, să statueze dreptul la respectarea vieții private și familiale, a domiciliului și corespondenței. Acest lucru nu împiedică specificarea respectării vieții private ca drept la protecția datelor personale: în acest caz, deci, fără dubiu, dreptul însuși este configurabil ca un drept al persoanei (Losano, *trad*. Lazăr, 2004, p.321-322).

Prin art. 8 din Convenția Europeană a Drepturilor Omului este protejată o sferă largă de interese de natură personală, legate unele de altele, uneori chiar suprapunându-se, cuprinse în noțiunea generală de *drept la viață privată*, *viață de familie*, *corespondență* și *domiciliu*. Aceste interese nu sunt definite strict de Convenție. Pentru păstrarea unei flexibilități necesare dezvoltării jurisprudenței sale, Curtea a evitat, de asemenea, să le definească de o manieră strictă, preferând să le utilizeze, adeseori, o terminologie dublă, sau chiar triplă, același act încălcând atât dreptul la viață privată, cât și dreptul la viață familială ori la corespondență (Bogdan, 2005, p. 344 – 345).

Pentru început, în scopul elucidării obiectului prezentei teze, considerăm că urmează mai întâi de toate să stabilim cum definește legiuitorul noțiunea de *date cu caracter personal* și *sistem informațional*. În art. 3 din Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal,*datele cu caracter personal* sunt definite ca fiind orice informaţie referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal).Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale. Sistemul informațional reprezintă un ansamblul de elemente implicate în procesul de colectare, transmisie și prelucrare de informații. Potrivit pct. 3al Hotărârii de Guvern Nr. 1123 din 14.12.2010 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, *sistem informaţional de date cu caracter personal* este definit ca fiind *totalitatea resurselor şi tehnologiilor informaţionale*

interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal.

Având aria de acoperire a acestor noțiuni, vom identifica cerințele prevăzute de lege ce vizează operatorii de date cu caracter personal pentru a asigura securitatea acestor date.

Potrivit art. 7 din Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, ratificată prin Hotărârea Parlamentului Republicii Moldova nr.483 din 02.07.1999, trebuie să fie luate măsuri corespunzătoare de securitate pentru protejarea datelor cu caracter personal înregistrate în fișierele automatizate de date contra distrugerii accidentale sau neautorizate, sau pierderii accidentale, cât şi contra accesului, modificării sau difuzării neautorizate.

Articolul 23 și articolul 28 ale Legii privind protecţia datelor cu caracter personal impun obligația ca, anterior inițierii operaţiunilor de prelucrare a datelor cu caracter personal într-un sistem de evidență automatizat sau manual, operatorii să notifice Centrul Național pentru Protecția Datelor cu Caracter Personal.

O dată cu depunerea acestei notificări, subiecții vizați vor întocmi și vor prezenta Centrului o Politică de securitate. Această obligație este stabilită de pct. 15 al Hotărârii de Guvern Nr. 1123 din 14.12.2010, potrivit căruia fiecare deţinător de date cu caracter personal, reieşind din specificul activităţii, elaborează şi organizează implementarea prevederilor documentului care stabileşte politica de securitate a datelor cu caracter personal, inclusiv procedurile şi măsurile legate de realizarea acestei politici, cu aplicarea soluţiilor practice cu un nivel de detalizare şi complexitate proporţional, în partea ce ţine de identificarea şi autentificarea utilizatorilor; de reacţionare la incidentele de securitate; de protecţie a TI şi comunicaţiilor; de asigurare a integrităţii informaţiei care conţine date cu caracter personal şi TI; de administrare a accesului; de audit şi asigurare a evidenţei. Operatorul de date cu caracter personal este obligat să informeze toate persoanele care sunt antrenate în acest proces de conținutul acestui document. Suplimentar, deţinătorul de date cu caracter personal va numi o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.

Politica de securitate va conține în mod obligatoriu următoarele:

1) identitatea persoanei responsabile de politica de securitate;
2) măsurile de securitate;
3) mecanismul de punere în aplicare a măsurilor de securitate;
4) nomenclatorul datelor cu caracter personal prelucrate, a localizării acestora şi a operaţiunilor efectuate asupra lor;

5) lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal;
6) configurarea sistemului informațional de date cu caracter personal şi a reţelei;
7) descrierea detaliată a criteriilor, în conformitate cu care sunt accesibile datele cu caracter personal prelucrate în registrul ţinut manual;
8) documentația tehnică cu privire la controalele de securitate;
9) orarul controalelor de securitate;
10) măsurile de detectare a cazurilor de acces şi/sau de prelucrare neautorizată a datelor cu caracter personal;
11) rapoarte despre incidentele de securitate.

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate, atât în cadrul prelucrării manuale, cât și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe TI. Baza unei securităţi TI adecvate o constituie respectarea unei asemenea Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor TI împotriva influenţelor naturale, erorilor umane și tehnice, precum și împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranţa TI nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice. Aceasta vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură. Operatorul va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a angajaților săi.

Reglementările Politicii reprezintă un standard minim pentru clienți/consumatori, inclusiv toți angajații. Pornind de la această reglementare, toți angajații urmează să respecte strict prevederile Politicii și regulile interne privind protecția datelor cu caracter personal.

Operatorul de date cu caracter personal, reieșind din specificul activităţii, prin Politica de securitate, transpun procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.

Politica de securitate a datelor cu caracter personal se va revizui cel puţin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității, fiind pusă în sarcina conducătorilor, de a desemna persoana/-ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

Politica de securitate, în mod obligatoriu, va fi adusă la cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal.

Responsabil de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, va fi desemnată persoana care, conform fișei postului și/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducătorului (administratorului) sau persoanei care îndeplinește interimatul funcției.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări. Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală, va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal, va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal, astfel încât să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

Protecţia datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sunt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal,păstrate pe:

- suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

- sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

- preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaționale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program,
- preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program,
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal,transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum și utilizarea canalelor VPN,
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiva programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă,
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.
- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal,prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni, cât și pentru cei externi. (pct. 4-10 din Hotărârea de Guvern Nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal).

În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art. 12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptând cazul în care el deţine deja informaţiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

- existenţa drepturilor la informare și de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) și de opoziţie, precum și condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

b) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fișele personale (alte materiale), cu excepţia cazurilor în care solicitanţii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertăţile fundamentale ale subiectului datelor cu caracter personal.

Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură mentenanța sistemului și/sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.

În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat etc.), modificarea urmând a fi efectuată în toate sistemele informaţionale și de evidenţă gestionate.

REFERINȚE BIBLIOGRAFICE

1. Carp, Radu, Șandru, Simona, Dreptul la intimitate și protecția datelor cu caracter personal, București, Ed. All Beck, 2004.
2. Răduleț, Sebastian, Libertăți Fundamentale, București, Ed. Didactică și Pedagogică R.A., 2008.
3. Losano, Mario G., trad. Lazăr, Alina, Legea italiană în privința protecției vieții private, București, Ed. All Beck, 2004.
4. Drăghici, Sonia, Efectele dreptului la respectul vieții private și a demnității asupra dreptului civil, București, Ed. Universul Juridic, 2011.
5. Bogdan, Dragoș, Drepturi și libertăți fundamentale în jurisprudența Curții Europene a Drepturilor Omului, București, Ed. All Beck, 2005.

Resurse web:

http://lex.justice.md/document_rom.php?id=44B9F30E:7AC17731
http://lex.justice.md/md/340495/; _http://lex.justice.md/md/337094/
http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=309121