



Protecția datelor cu caracter personal (II)

Pentru a avea o viziune clară asupra modalității de respectare de către autoritățile de aplicare a legii a dreptului sus - menționate, trebuie avute în vedere și următoarele două aspecte:

● Conținutul articolului 5 din Legea 677/2001. Acesta prevede că „*orice prelucrare de date cu caracter personal, cu excepția categoriilor de date menționate la articolul 7 alin. (1) i (categorii de date interzise la prelucrare), articolul 8 (codul numeric personal) și 10 (cazierul judiciar) poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.*” Cu toate acestea există și excepții în care consimțământul persoanei vizate nu este cerut de lege. Dintre acestea prezintă interes pentru activitățile de aplicare a legii cele prevăzute la articolul 5, alin. (2), literele b, c și d. Astfel, consimțământul persoanei vizate nu este necesar atunci când prelucrarea se efectuează în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate, în vederea îndeplinirii unei obligații legale a operatorului sau când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de

interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sunt dezvăluite datele.

● Conținutul articolului 16 din Legea 677/2001. Conform tezei de la alin. (1), prevederile referitoare la dreptul la informare, dreptul de acces la date, dreptul la opoziție precum și obligația operatorului de a comunica numele terțului căruia i-au fost dezvăluite datele cu caracter personal nu se aplică dacă ne aflăm într-una din situațiile enumerate de articolul 2, alin. (5) (articol dezbătut anterior), în condițiile în care aceasta ar prejudicia eficiența acțiunii sau obiectivul urmărit în îndeplinirea atribuțiilor legale ale autorității publice. Astfel, autoritățile de aplicare a legii nu sunt obligate să informeze persoana vizată despre prelucrarea datelor sale cu caracter personal, dacă această prelucrare a fost efectuată în cadrul activităților de prevenire, cercetare și reprimare a infracțiunilor și de menținere a ordinii publice, ceea ce acoperă peste 90% din sfera de activitate a acestora. Această excepție de la obligațiile operatorului nu are însă caracter permanent. Astfel, aceste prevederi sunt aplicabile strict pentru perioada necesară

atingerii obiectivului urmărit prin desfășurarea activităților menționate la articolul 2, alin. (5), iar după încetarea situației, operatorul trebuie să ia măsurile necesare pentru asigurarea drepturilor persoanei vizate.

În cadrul operațiunilor de colectare a datelor, autoritățile de aplicare a legii au dreptul să colecteze date cu caracter personal numai în scopuri:

a) **determinate, explicite și legitime.** Gama acestor scopuri este foarte variată, de la activități generice de prevenire, combatere și descoperire a infracțiunilor (cum este cazul bazelor de date referitoare la persoane urmărite ori la autovehiculele furate) și până la baze de date constituite în vederea asigurării respectării cadrului normativ în vigoare (evidența personalului de pază atestat, registrul național al armelor sau evidența deținătorilor de aparate/detectoare de metale).

b) **adecvate, pertinente și ne-excesive.** Nu pot fi colectate decât acele date cu caracter personal necesare atingerii scopului inițial urmărit. Astfel, în cazul aplicării unei sancțiuni contravenționale la regimul circulației nu se va prelucra, spre

exemplu, categoria de date personale referitoare la venit.

c) **exacte, și dacă este cazul, actualizate.** Se va acorda atenție asupra corectitudinii datelor colectate, iar în cazul în care se constată că acestea sunt inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și ulterior valorificate să fie șterse sau completate.

d) **stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate și în care vor fi ulterior prelucrate;** stocarea datelor pe o durată mai mare decât cea menționată, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

O categorie aparte de operațiuni de prelucrare a datelor cu caracter personal este reglementată prin Decizia 100 din 2007 a ANSPDCP. Aceasta se referă la acele operațiuni de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea. Astfel, notificarea nu este necesară pentru operațiuni de prelucrare a datelor cu caracter personal efectuate cu scopul de îndeplinire a obligațiilor salariale prevăzute de lege față de proprii angajați (o baza de date financiar - contabilă), operațiuni legate de personal cum ar fi prelucrarea datelor persoanelor fizice înscrise la concursuri sau examene în vederea ocupării locurilor de muncă vacante sau prelucrarea datelor participanților la simpozioane ori conferințe (în ceea ce privește M.I.R.A. o astfel de bază de date este cea constituită la nivelul direcțiilor responsabile de managementul resurselor umane).

Dincolo de obligațiile ce revin operatorului de date cu caracter personal în relația sa cu persoana vizată, trebuie să avem în vedere și obligațiile ce revin acestuia prin Ordinul Avocatului Poporului nr. 52 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal. Aceasta cu atât mai mult cu cât majoritatea prelucrărilor de date cu caracter personal realizate de către autoritățile de aplicare a legii sunt efectuate în cadrul unui sistem informatic, prin aplicații ce gestionează baze de date specifice. Fiecare operator de date cu caracter personal trebuie să aibă în vedere ca nivelul de securitate al sistemelor sale informatice în care sunt prelucrate date cu caracter personal să îndeplinească o serie de cerințe minime, cerințe ce acoperă următoarele aspecte: a) identificarea și autentificarea utilizatorului; b) tipurile de acces;

c) colectarea datelor; d) execuția copiilor de siguranță; e) computerele și terminalele de acces; f) sistemele de telecomunicații; g) folosirea computerelor; h) imprimarea datelor.

Operatorul de date cu caracter personal trebuie să se asigure că operațiunile de prelucrare nu sunt și nici nu pot fi efectuate decât de personal anume autorizat (identificarea utilizatorului) pe baza unei parole (autentificarea utilizatorului). La rândul lor, utilizatorii pot avea **acces deplin** (dreptul de a introduce un not set de date personale sau de modifica un set preexistent), **acces limitat** (poate folosi baza de date numai spre consultare/interogare) ori cu **acces controlat** (cei ce asigură funcționarea aplicației corespondente bazei de date – de obicei administratorii și dezvoltatorii aplicației). De asemenea, orice operațiune automată (actualizare, consultare, interogare, etc.) trebuie înregistrată într-un fișier jurnal (log) care să permită ulterior identificarea utilizatorului, a datelor accesate, a datei și momentului accesului.

Îndeplinirea tuturor acestor obligații trebuie privită nu numai ca o obligație națională ci și ca o necesitate impusă de aderarea României la Uniunea Europeană și de integrarea în spațiul Schengen. Aceste aspecte sunt de natură să genereze amplificarea deosebită a cooperării polițienești internaționale, îndeosebi sub aspect transfrontalier, precum și din punctul de vedere al schimbului de date și informații de interes operativ, între care se regăsesc și cele cu caracter personal. De altfel, una dintre prioritățile aflate pe agenda președinției germane a UE a reprezentat-o tocmai finalizarea unui proiect de Decizie - cadru a Consiliului, privind protecția datelor procesate în cadrul cooperării polițienești și judiciare în materie penală. În măsura în care astfel de instrumente juridice comunitare vor deveni obligatorii pentru statele membre, prin prisma atribuțiilor ce-i revin, dar și din nevoia de a asigura un nivel de protecție adecvat acestor categorii de date, la standarde europene, instituțiile M.I.R.A. vor trebui să facă față acestor noi cerințe.

Și în perioada următoare se vor crea noi evidențe, noi baze de date ce vor presupune asigurarea unei protecții adecvate la prelucrarea diferitelor categorii de date cu caracter personal,

iar acest proces va impune uniformizarea modului de lucru, respectiv reformarea sistemului actual, în sensul înregistrării centralizate a tuturor sistemelor de date electronice sau a celor gestionate manual existente în cadrul diferitelor instituții componente M.I.R.A., precum și în cadrul structurilor subordonate, în care sunt sau vor fi prelucrate date cu caracter personal. Mai mult, așa cum s-a procedat în unele cazuri, este necesar ca orice activitate de constituire a unei baze de date să fie precedată de elaborarea unui cadru metodologic prin care să se reglementeze modul de colectare, stocare, utilizare, modificare, corectare, blocare, transmitere și ștergere a datelor.

În vederea asigurării respectării cadrului legal în vigoare dar și a îndeplinirii obligațiilor legate de aderarea României la spațiul Schengen, la nivelul Ministerului Internelor și Reformei Administrative a fost numit un responsabil pe protecția datelor la nivelul M.I.R.A. În îndeplinirea atribuțiilor sale, responsabilul este ajutat de Oficiul Responsabilului pentru Protecția Datelor Personale. La nivelul structurilor subordonate există compartimente / persoane responsabile pe linia protecției datelor cu caracter personal. Atribuțiile acestora sunt de a acorda sprijin ANSPDCP în îndeplinirea atribuțiilor legale ce-i revin dar și de a asigura implementarea la nivelul M.I.R.A. a măsurilor tehnice și organizatorice necesare în vederea asigurării legalității prelucrărilor de date cu caracter personal și a măsurilor minime de securitate corelate acestora.

■ Mihai Lucian Friptu

