

**AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

R A P O R T A N U A L

2014

Raportul de activitate este prezentat Senatului României, în temeiul art. 5 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare.

București

CUVÂNT ÎNAINTE

Stimate Domnule Președinte al Senatului,

Stimați senatori,

Vă supun atenției raportul cu privire la activitatea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal în anul 2014.

În cursul acestui an, activitatea instituției noastre a avut ca finalitate consolidarea respectării regulilor aplicabile în materia dreptului la viață privată și a dreptului la protecția datelor cu caracter personal.

Astfel, eforturile Autorității naționale de supraveghere s-au concentrat pe intensificarea atribuțiilor legale de monitorizare și control al prelucrărilor de date cu caracter personal, desfășurate pentru soluționarea plângerilor și sesizărilor primite, dar și pentru verificarea din oficiu a unor aspecte legate de prelucrarea datelor personale, în scopul asigurării respectării și aplicării principiilor de protecție a datelor de către operatorii din domeniul public și privat.

Investigațiile efectuate din oficiu au urmărit, cu precădere, verificarea respectării regulilor de prelucrare a datelor personale în activitatea desfășurată de către unități sanitare și de învățământ, de către entități din sfera financiar-bancară și de către societăți de transport public urban. În vederea soluționării plângerilor și a sesizărilor ce ne-au fost adresate, au fost efectuate investigații, în special, în domenii legate de transmiterea datelor personale către sisteme de evidență de tipul biroului de credit, de utilizarea mijloacelor de comunicație electronică în prelucrarea datelor personale sau a mijloacelor de supraveghere video.

Ca rezultat al activității de control desfășurate în anul 2014, se remarcă o dublare a cuantumului amenziilor aplicate prin comparație cu anul anterior și o sporire, de asemenea, semnificativă a numărului plângerilor și sesizărilor adresate de cei interesați.

Având în vedere deciziile importante pronunțate de Curtea de Justiție a Uniunii Europene în materia dreptului la protecția datelor personale în anul 2014, în privința reținerii datelor de trafic, a "dreptului de a fi uitat pe Internet" și a utilizării mijloacelor de supraveghere video de către persoanele fizice, instituția noastră a preluat în activitatea sa specifică liniile principale dezvoltate în această jurisprudență.

În aceeași perioadă, Autoritatea națională de supraveghere a intensificat activitățile și modalitățile de comunicare destinate informării publicului larg cu privire la regulile specifice de prelucrare a datelor cu caracter personal. Astfel, pe lângă organizarea de evenimente specifice, cum a fost Ziua Europeană a Protecției Datelor sau reuniunile de informare a autorităților publice locale și serviciilor publice deconcentrate județene, un rol semnificativ în activitatea de conștientizare a publicului larg l-a avut difuzarea unui clip de informare privind datele personale pe posturile de televiziune, în mijloacele de transport în comun și pe anumite rețele de televiziune cu circuit închis amplasate în locuri accesibile publicului.

În cursul anului 2014, instituția noastră a continuat să se implice în procesul de reformă a reglementărilor europene privind protecția datelor personale, declanșat la nivelul Uniunii Europene și al Consiliului Europei, în vederea asigurării unei poziții de substanță în cadrul organismelor europene, în colaborare cu celelalte instituții publice din România, cu rol de reprezentare la acest nivel.

În acest context, considerăm ca fiind necesară consolidarea capacității administrative a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, prin alocarea unor resurse materiale, financiare și umane adecvate exercitării atribuțiilor sale specifice, în conformitate cu standardele impuse de legislația europeană, în scopul adaptării din punct de vedere legislativ și instituțional la noul cadru ce va fi creat în baza pachetului legislativ de reformă la nivel european.

Pe baza experienței acumulate până în prezent, Autoritatea își propune ca în perioada următoare să monitorizeze verificarea respectării condițiilor de prelucrare a datelor personale, prin intensificarea investigațiilor în sectorul public și privat, alături de sporirea gradului de informare publică a tuturor entităților implicate și a persoanelor vizate cu privire la modalitățile de exercitare a drepturilor conferite în domeniul protecției datelor personale.

Îmi exprim convingerea că vom beneficia de sprijinul dumneavoastră pentru realizarea acestor proiecte de viitor, în scopul de a ne exercita pe deplin rolul de garant al dreptului la viață privată.

Ancuța Gianina OPRE,
Președinte

CUPRINS

CAPITOLUL I

PREZENTARE GENERALĂ	6
----------------------------------	---

CAPITOLUL II

INIȚIATIVE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secțiunea 1 Propunerea de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și Propunerea de Directivă privind protecția datelor prelucrate în scopul prevenirii, detectării, investigării și punerii sub urmărire a infracțiunilor și a altor activități judiciare.....	8
--	---

Secțiunea a 2-a Propunerea de Directivă a Parlamentului European și a Consiliului privind prevenirea utilizării sistemului financiar în scopul spălării banilor, inclusiv al finanțării terorismului și Propunerea de Regulament al Parlamentului European și al Consiliului cu privire la informațiile privind plătitorul care însoțesc transferurile de fonduri.....	10
---	----

Secțiunea a 3-a: Propunerea de Regulament privind cerințele de omologare de tip pentru instalarea unui sistem eCall la bordul vehiculelor și de modificare a Directivei 2007/46/CE de stabilire a unui cadru pentru omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective și Propunerea de Decizie privind implementarea sistemului eCall interoperabil la nivelul Uniunii Europene	12
---	----

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Acte administrative cu caracter normativ	15
Secțiunea a 2-a Avizarea actelor normative.....	16
Secțiunea a 3-a Puncte de vedere privind diverse chestiuni de protecția datelor.....	28
Secțiunea a 4-a Activitatea de reprezentare în fața instanțelor de judecată.....	42
Secțiunea a 5-a Informare publică	52

CAPITOLUL IV ACTIVITATEA DE CONTROL

Secțiunea 1	Prezentare generală.....	56
Secțiunea a 2-a	Investigații din oficiu.....	57
Secțiunea a 3-a	Activitatea de soluționare a plângerilor și sesizărilor.....	74

CAPITOLUL V ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE.....106

CAPITOLUL VI ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRIILOR DE DATE CU CARACTER PERSONAL

Secțiunea 1	Activitatea de înregistrare a prelucrărilor de date.....	115
Secțiunea a 2-a	Transferul datelor cu caracter personal în străinătate.....	118
Secțiunea a 3-a	Puncte de vedere referitoare la activitatea operatorilor	121

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII.....	125
--	-----

CAPITOLUL VIII

PROPUNERI DE LEGE FERENDA.....	127
---------------------------------------	-----

CAPITOLUL I PREZENTARE GENERALĂ

Raportul de activitate pe anul 2014 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea națională de supraveghere) este structurat pe șapte capitole, după cum urmează:

Capitolul I asigură o prezentare sintetică a raportului pe principalele aspecte.

În cuprinsul **Capitolului al II-lea** sunt cuprinse aspecte relevante ale inițiativelor cu impact în domeniul protecției datelor cu caracter personal la nivelul Uniunii Europene.

Capitolul al III-lea cuprinde activitatea în domeniul reglementării, avizării și consultării referitoare aplicarea regulilor de protecție a datelor personale, inclusiv cu privire la proiectele actelor normative asupra cărora sunt incidente principiile de prelucrare a datelor personale, precum și clarificarea unor chestiuni semnalate de diverși operatori. Aceasta s-a concretizat în emiterea de avize asupra proiectelor de acte normative, de decizii administrative cu caracter normativ și a unui număr semnificativ de puncte de vedere.

Prin petițiile transmise, persoanele fizice și operatorii de date au solicitat, în special, informații referitoare la incidența legislației privind protecția datelor asupra activității desfășurate de operatori, condițiile prelucrării datelor cu caracter special, legalitatea dezvoltării unor date și la transferul acestora în străinătate.

În secțiunea referitoare la reprezentarea în fața instanțelor de judecată, sunt prezentate litigiile relevante aflate pe rolul instanțelor judecătorești în care a fost parte Autoritatea națională de supraveghere și sunt evidențiate soluțiile pronunțate.

Secțiunea privind informarea publică reliefează principalele modalități de popularizare a domeniului protecției datelor cu caracter personal, utilizate în cursul anului 2014.

Capitolul al IV-lea constă într-o prezentare a activității de control, în privința investigațiilor din oficiu și a celor efectuate pe baza plângerilor ori sesizărilor primite. Această activitate constă în verificarea modalității în care operatorii din România efectuează operațiuni de prelucrare a datelor cu caracter personal cu scopul de a verifica modul de aplicare a dispozițiilor legale în materie. În cadrul investigațiilor efectuate în anul 2014, au fost aplicate sancțiuni contravenționale constând în avertismente și amenzi în cuantum total de 282.000 lei.

Investigațiile efectuate din oficiu au vizat verificarea respectării de către operatori a dispozițiilor Legii nr. 677/2001, precum și a celorlalte acte normative care privesc domeniul datelor cu caracter personal.

În unele cazuri s-a dispus, prin decizia președintelui Autorității naționale de supraveghere, încetarea prelucrării sau ștergerea datelor.

Capitolul al V-lea prezintă activitatea de relații externe a Autorității naționale de supraveghere.

Capitolul al VI-lea privind activitatea de supraveghere a prelucrărilor de date cu caracter personal prezintă concluziile rezultate din analizarea formularelor transmise de operatorii de date, persoane fizice și juridice, care au avut obligația depunerii acestora. Au fost înregistrate un număr total de 8590 de notificări privind prelucrările de date realizate atât pe teritoriul României, cât și în statele membre, ori transferuri în state terțe.

Capitolul al VII-lea referitor la resursele materiale și financiare conține informații referitoare la creditele bugetare puse la dispoziția Autorității naționale de supraveghere și sumele cheltuite pe fiecare articol al clasificăției bugetare.

Capitolul al VIII-lea conține propuneri de modificări legislative referitoare la cadrul național în domeniul protecției datelor.

CAPITOLUL AL II-LEA

INIȚIATIVE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secțiunea 1: Propunerea de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și Propunerea de Directivă privind protecția datelor prelucrate în scopul prevenirii, detectării, investigării și punerii sub urmărire a infracțiunilor și a altor activități judiciare

Pachetul legislativ propus de Comisia Europeană cuprinde două propuneri de acte normative:

- o propunere de Regulament privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- o propunere de Directivă privind protecția datelor prelucrate în scopul prevenirii, detectării, investigării și punerii sub urmărire a infracțiunilor și a altor activități judiciare.

Referitor la natura instrumentului juridic, Comisia Europeană a propus un regulament, act normativ de aplicabilitate directă, cu intenția declarată de a asigura o unitate de reglementare și abordare a domeniului protecției datelor personale la nivelul Uniunii Europene.

Capitolul din proiectul de Regulament privind modalitățile de efectuare a transferurilor de date cu caracter personal a suscitat un interes deosebit, iar mecanismul autorității-lider propus de Comisia Europeană a fost intens dezbătut, reliefându-se aspectele pozitive, dar și implicațiile negative din perspectiva asigurării eficiente a drepturilor persoanelor vizate.

În ceea ce privește propunerea de Directivă privind protecția datelor prelucrate în scopul prevenirii, detectării, investigării și punerii sub urmărire a infracțiunilor și a altor activități judiciare, Comisia Europeană a subliniat că scopul acesteia îl constituie asigurarea unui nivel unitar și ridicat de protecție a datelor cu caracter personal ale persoanelor fizice în domeniul cooperării polițienești și judiciare în materie penală.

Astfel, se intenționează ca nivelul de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile

competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, să fie similar în toate statele membre.

Protecția efectivă a datelor cu caracter personal la nivelul Uniunii Europene implică consolidarea drepturilor persoanelor vizate și a obligațiilor celor care prelucrează date cu caracter personal, precum și stabilirea de competențe echivalente pentru monitorizarea și asigurarea conformității cu reglementările în materie de protecție a datelor cu caracter personal din statele membre.

În consecință, scopul propunerii este de a asigura un nivel ridicat de protecție a datelor în acest domeniu, pentru creșterea încrederii reciproce între autoritățile polițienești și cele judiciare din diferitele state membre, facilitând libera circulație a datelor și cooperarea între aceste autorități.

În privința acestei propuneri, Autoritatea națională de supraveghere și-a menținut rezervele exprimate față de extinderea domeniului de aplicare a Directivei și la activitatea de menținere și asigurare a ordinii publice, întrucât implică o scădere a actualului nivel de protecție a datelor conferit prin Directiva 95/46/EC.

În cadrul dezbaterilor celor două proiecte în Grupul de Lucru Dapix de la nivelul Consiliului Uniunii Europene un accent deosebit s-a pus pe reglementarea drepturilor persoanelor vizate, prin raportare la exigența stabilirii unui nivel adecvat de protecție a datelor personale.

Un alt aspect deosebit de dezbătut l-a constituit stabilirea mecanismului one-stop-shop, prin care se intenționează să se asigure un tratament unitar de abordare a transferurilor cu impact transfrontalier, în contextul mai larg al reglementării situațiilor de transfer de date cu caracter personal, inclusiv în state terțe.

În cursul anului viitor, se preconizează că acest pachet legislativ va intra în faza negocierilor în cadrul dialogului Parlament European - Consiliului Uniunii Europene – Comisia Europeană, în vederea stabilirii formei finale.

Secțiunea a 2-a: Propunerea de Directivă a Parlamentului European și a Consiliului privind prevenirea utilizării sistemului financiar în scopul spălării banilor, inclusiv al finanțării terorismului, și Propunerea de Regulament al Parlamentului European și al Consiliului cu privire la informațiile privind plătitorul care însoțesc transferurile de fonduri

În cursul anului 2014 au continuat discuțiile referitoare la propunerile legislative adoptate de Comisia Europeană, în scopul consolidării normelor Uniunii Europene existente cu privire la combaterea spălării banilor și transferurile de fonduri.

Întrucât trasabilitatea completă a transferurilor de fonduri poate reprezenta un instrument extrem de important și valoros în materie de prevenire, cercetare și descoperire a activităților de spălare a banilor sau de finanțare a terorismului, dată fiind necesitatea asigurării transducerii corespunzătoare a informațiilor cu privire la plătitor pe parcursul lanțului de plăți, s-a considerat oportun să se prevadă un sistem care să impună prestatorilor de servicii de plată obligația de a se asigura că transferurile de fonduri sunt însoțite de informații exacte și utile cu privire la plătitor.

Referitor la protecția datelor cu caracter personal, Autoritatea națională de supraveghere a comunicat că proiectul de Directivă privind prevenirea utilizării sistemului financiar în scopul spălării banilor și al finanțării terorismului, prin scopul propus, va avea ca rezultat colectarea și prelucrarea unui volum foarte mare de informații, respectiv date cu caracter personal. În acest context, vor exista implicații majore în ceea ce privește drepturile fundamentale ale persoanelor fizice, iar în cazul nerespectării legislației în materia protecției datelor, se va ajunge la grave atingeri aduse dreptului la viață privată a acestora.

În ceea ce privește termenul de reținere al datelor prevăzut în proiectul de Directivă, Autoritatea națională de supraveghere a considerat că termenul de 10 ani este excesiv, raportat la natura și tipurile de date prelucrate în scopul prevenirii utilizării sistemului financiar în scopul spălării banilor și al finanțării terorismului.

De asemenea, s-a atras atenția asupra necesității limitării accesului la date strict la FIUs, entitățile competente și cele raportoare, în contextul în care Parlamentul European a propus ca la aceste date să se permită accesul și "publicului care are un interes legitim" (de ex. ONG, jurnaliști, etc.

În ceea ce privește accesul diverșilor actori implicați în prevenirea utilizării sistemului financiar în scopul spălării banilor și al finanțării terorismului la datele din sistemul financiar s-a subliniat că trebuie să se ia în considerare și în acest caz limitarea accesului la sistem în contextul necesității asigurării securității și confidențialității datelor, în considerarea dispozițiilor art. 17 din Directiva 95/46/EC a Parlamentului European.

În ceea ce privește noțiunea de interes legitim și aplicabilitatea acesteia în cadrul prelucrărilor de date cu caracter personal efectuate pentru prevenirea utilizării sistemului financiar în scopul spălării banilor și al finanțării terorismului, Autoritatea națională de supraveghere a subliniat că Grupul de Lucru Art. 29 a emis Opinia 6/2014 cu privire la noțiunea de interes legitim, prin raportare la art. 7 din Directiva 95/46/EC.

În lumina acestui document, o dezvăluire de date către terți, fără consimțământul persoanei vizate, se poate realiza în situația de excepție menționată, însă numai în măsura în care există un echilibru între satisfacerea unui interes, de altfel considerat a fi legitim de către terțul care solicită dezvăluirea datelor și prejudiciul ce poate fi adus, prin dezvăluirea de date cu caracter personal, interesului sau drepturilor și libertăților fundamentale ale persoanei vizate.

Însă, dacă există interes legitim al operatorului sau terțului căruia îi sunt dezvăluite datele, acesta trebuie temeinic justificat și dovedit, concomitent cu respectarea drepturilor persoanelor vizate, în special dreptul de informare și opoziție. Deci, persoana vizată trebuie informată cu privire la dezvăluire a unor informații referitoare la ea, pentru a i se da posibilitatea ca, din motive întemeiate legate de situația sa particulară, să se opună la dezvăluirea datelor.

Autoritatea națională de supraveghere a recomandat, în legătură cu existența interesului legitim ca temei de prelucrare, ca acesta:

- să fie legal (în acord cu legislația aplicabilă la nivel European și național);
- să fie suficient de clar, articulat, astfel încât să permită un real echilibru între interesul invocat și drepturile fundamentale ale persoanelor vizate (să fie suficient specificat, în acord cu art. 7 lit. (f) din Directiva 95/46/EC astfel încât "interesul legitim invocat să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate");
- să reprezinte un interes real și prezent (un interes nespeculativ).

În legătură cu acest aspect, în procedura de supunere a adoptării prin procedura scrisă, a dosarului conținând pachetul legislativ format din propunerea de Directivă a Parlamentului

European și a Consiliului privind prevenirea utilizării sistemului financiar în scopul spălării banilor și al finanțării terorismului și propunerea de Regulament al Parlamentului European și al Consiliului cu privire la informațiile privind plătitorul care însoțesc transferurile de fonduri, s-a stabilit că se va lăsa posibilitatea statelor membre de a trata la nivel național noțiunea de "interes legitim", ceea ce va permite acestora să transpună textul Directivei conform opțiunii naționale și să introducă în legislația națională o definiție a "interesului legitim" considerată adecvată.

Secțiunea a 3-a: Propunerea de Regulament privind cerințele de omologare de tip pentru instalarea unui sistem eCall la bordul vehiculelor și de modificare a Directivei 2007/46/CE de stabilire a unui cadru pentru omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective și Propunerea de Decizie privind implementarea sistemului eCall interoperabil la nivelul Uniunii Europene.

Pentru atenuarea consecințelor accidentelor rutiere grave din Uniunea Europeană, Comisia Europeană a adoptat două propuneri de acte normative, propunerea de Regulament privind cerințele de omologare de tip pentru instalarea unui sistem eCall la bordul vehiculelor și de modificare a Directivei 2007/46/CE de stabilire a unui cadru pentru omologarea autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective și propunerea de Decizie privind implementarea sistemului eCall interoperabil la nivelul Uniunii Europene, pentru a asigura ca, până în 15 octombrie 2015, autovehiculele să apeleze automat serviciile de urgență, în cazul unui accident grav.

Sistemul eCall apelează automat numărul european unic de urgență 112, în cazul unui accident grav și transmite serviciilor de urgență locul în care se află vehiculul chiar în cazul în care conducătorul auto este inconștient sau în imposibilitatea de a efectua un apel telefonic.

Astfel, toate modelele noi de vehicule de pasageri și de vehicule ușoare ar trebui să fie echipate cu sistemul eCall 112, fapt pentru care ar trebui să fie creată infrastructura necesară pentru preluarea și gestionarea adecvată a apelurilor sistemului eCall în centre de preluare a apelurilor de urgență – asigurând compatibilitatea, interoperabilitatea și continuitatea serviciului eCall la nivelul Uniunii Europene.

Așadar, Comisia Europeană a promovat două propuneri de acte legislative pentru a ajuta la înființarea și punerea în aplicare a sistemului.

În ceea ce privește prelucrarea de date cu caracter personal în sistemul eCall, Grupul de Lucru Art. 29 a făcut recomandări prin „Documentul de lucru referitor la protecția datelor și la implicațiile asupra vieții private în cadrul inițiativei privind eCall”. Astfel, s-a recomandat ca orice prelucrare a datelor cu caracter personal efectuată prin intermediul sistemului eCall încorporat la bordul vehiculului să fie conformă cu normele de protecție a datelor prevăzute în Directiva 95/46/CE și în Directiva 2002/58/CE a privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice, în special pentru a garanta că vehiculele dotate cu sisteme eCall încorporate la bordul vehiculului, în starea normală de funcționare legate de un apel eCall 112, nu pot fi urmărite și nu fac obiectul unei urmăriri constante și că setul minim de date trimise de sistemul eCall include informațiile minime necesare pentru tratarea corespunzătoare a apelurilor de urgență.

Autoritatea națională de supraveghere a propus următoarele:

- introducerea în textul propunerii de Regulament privind cerințele de omologare de tip pentru instalarea unui sistem eCall la bordul vehiculelor și de modificare a Directivei 2007/46/CE, la articolul privind protecția datelor, a unei referințe prin care să se prevadă, ca regulă generală, faptul că Directiva 95/46/EC și regulile naționale de implementare a acesteia reprezintă cadrul legal aplicabil prelucrărilor de date cu caracter personal la care se referă propunerea de Regulament.

- includerea unor prevederi concrete privind protecția datelor, acestea nefiind dezvoltate suficient în textul propunerii (de exemplu, introducerea unei prevederi distincte referitoare la limitarea scopului, care să se aplice atât situațiilor privind prelucrarea datelor în cazul sistemului 112 eCall cât și în cazul sistemului eCall privat)

- întrucât sistemul eCall, așa cum este acesta prevăzut în propunerea de Regulament, este, din punct de vedere tehnic, unul deschis și accesibil, fără discriminare, unor terțe părți, pentru service și mentenanță, spre exemplu, astfel încât se creează posibilitatea apariției unor riscuri suplimentare pentru viața privată, Autoritatea națională de supraveghere a solicitat introducerea în conținutul propunerii de Regulament a unor prevederi exprese privind măsurile de securitate necesare a fi adoptate în contextul prelucrării datelor cu caracter personal atât în sistemul 112 eCall, cât și în cazul eCall privat.

- necesitatea limitării emiterii de acte delegate de către Comisia Europeană, precum și introducerea de prevederi exprese referitoare la măsuri privind protecția datelor, prin:

- desemnarea operatorilor de date cu caracter personal și a entităților responsabile cu soluționarea cererilor privind exercitarea dreptului de acces;

- detalierea într-o listă atât a setului minim cât și a celui maxim de categorii de date prelucrate în sistemul eCall;

- includerea posibilității ca persoana vizată să poată dezactiva sistemul privat eCall și să utilizeze servicii de tip eCall cu valoare adăugată;

- specificarea duratei de stocarea a datelor prelucrate în sistemul eCall;

- specificarea modalităților de exercitare de către persoanele vizate a drepturilor acestora, în contextul protecției datelor.

Întrucât în textul propunerii nu se regăsesc dispoziții referitoare la sistemul eCall privat care conține și alte servicii pe lângă cele de localizarea a autovehiculului în cazul situațiilor de urgență, de tip 112, și este, prin el însuși un sistem intruziv în viața privată și care presupune și existența unor servicii cu valoare adăugată față de sistemul 112 eCall, Autoritatea națională de supraveghere a solicitat reglementarea relațiilor juridice în contextul sistemului eCall privat, în completarea prevederilor referitoare la sistemul 112 eCall.

Ca urmare a negocierilor între Parlamentul European și Comisia Europeană, s-a comunicat statelor membre faptul că s-a obținut un acord de principiu cu privire la pachetul legislativ referitor la sistemul 112 eCall.

CAPITOLUL AL III-LEA

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Acte administrative cu caracter normativ

Pe parcursul anului 2014, în vederea reglementării activității operatorilor, Autoritatea națională de supraveghere a emis următoarele acte administrative cu caracter normativ:

1. Decizia nr. 41 din 18.03.2014 privind stabilirea unui model de autorizație pentru transferul în străinătate al datelor cu caracter personal în baza Regulilor Corporatiste Obligatorii (Binding Corporate Rules - BCR)

Această decizie a fost emisă în aplicarea dispozițiilor art. 26 alin. (2) din Directiva 95/46 CE, care prevede că un stat membru poate autoriza un transfer sau o serie de transferuri de date cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat atunci când operatorul oferă garanții suficiente privind atât protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor, cât și exercitarea drepturilor corespunzătoare; aceste garanții pot rezulta în special din clauze contractuale adecvate.

Autoritatea națională de supraveghere, în contextul prevederii legale sus menționate, corelate cu dispozițiile art. 29 alin. (1) și (4) din Legea nr. 677/2001, a emis Decizia nr. 41/2014 privind stabilirea unui model de autorizație pentru transferul în străinătate al datelor cu caracter personal în baza Regulilor Corporatiste Obligatorii (Binding Corporate Rules - BCR).

La emiterea deciziei ce reglementează transferul în străinătate efectuat în baza Regulilor Corporatiste Obligatorii au fost luate în considerare documentele care stabilesc elementele, principiile și structura Binding Corporate Rules elaborate de Grupul de lucru constituit în baza art. 29 din Directiva nr. 95/46/CE.

Noul act normativ a fost publicat în Monitorul Oficial al României nr. 218 din 27 martie 2014, Partea I.

2. Decizia nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile

aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice

Această decizie a fost emisă în considerarea calității României de stat membru al Uniunii Europene și în aplicarea prevederilor Regulamentului (UE) nr. 611/2013 al Comisiei Europene privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice, potrivit cărora autoritatea națională competentă pune la dispoziția tuturor furnizorilor stabiliți în statul membru în cauză un mijloc electronic sigur de notificare a încălcării securității datelor cu caracter personal de către furnizorii de servicii de comunicații electronice disponibile publicului.

Autoritatea națională de supraveghere a stabilit conținutul formularului de notificare a încălcărilor securității datelor cu caracter personal, în aplicarea prevederilor Regulamentului (UE) nr. 611/2013, prin raportare la prevederile Directivei 2002/58/CE, potrivit cărora furnizorii de servicii de comunicații electronice trebuie să notifice autorității naționale competente toate cazurile de încălcare a securității datelor cu caracter personal, precum și la legislația națională aplicabilă, respectiv Legea nr. 677/2001 și Legea nr. 506/2004.

Actul normativ a fost publicat în Monitorul Oficial al României nr. 964 din 30 decembrie 2014, Partea I.

Secțiunea 2 Avizarea actelor normative

În temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, Autoritatea națională de supraveghere a emis o serie de avize asupra unui număr de 32 de proiecte de acte normative elaborate de diverse instituții și autorități publice, care implicau diverse aspecte privind prelucrarea datelor cu caracter personal.

Autoritatea națională de supraveghere a formulat observații relevante referitoare la actele normative supuse avizării cu privire la protecția drepturilor și libertăților persoanelor fizice sub aspectul prelucrării datelor cu caracter personal.

Față de conținutul proiectelor actelor normative transmise Autorității naționale de supraveghere, în cursul anului 2013, au fost emise o serie de avize, dintre care le prezentăm pe cele mai relevante:

Avize favorabile, fără observații

În anul 2014, Autoritatea națională de supraveghere a emis avize favorabile, fără observații, pentru proiectele de acte normative care respectau reglementările în domeniul protecției datelor personale, dintre care enumerăm:

- Proiect de Ordonanță de urgență a Guvernului privind operaționalizarea Registrului electoral, modificarea Legii nr. 33/2007 privind organizarea și desfășurarea alegerilor pentru Parlamentul European, precum și unele măsuri pentru buna organizarea și desfășurare a alegerilor pentru Parlamentul European în 2014;

- Proiect de Hotărâre a Guvernului privind aprobarea modelului listei de susținători care va fi folosit la alegerile pentru membrii din Romania în Parlamentul European în anul 2014;

- Proiect de Hotărâre a Guvernului pentru desemnarea autorităților române competente în aplicarea prevederilor legale pentru facilitarea schimbului transfrontalier de informații referitoare la încălcările normelor de circulație care afectează circulația rutieră;

- Proiect de Hotărâre a Guvernului pentru aprobarea măsurilor, a bugetului și a cheltuielilor necesare pentru pregătirea, organizarea și desfășurarea alegerilor parțiale pentru Camera Deputaților și Senat din data de 25 mai 2014, a modelului timbrului autocolant, a modelelor listelor electorale, a modelului buletinului de vot, a modelelor ștampilelor electorale și ale altor documente care vor fi utilizate la aceste alegeri, precum și a condițiilor și duratei păstrării materialelor rezultate din procesul electoral;

- Proiect de Hotărâre de Guvern pentru modificarea anexei Hotărârii Guvernului nr. 244/2007 privind autoritățile competente responsabile cu aplicarea legislației din domeniul protecției consumatorilor și cooperarea dintre autoritățile naționale din acest domeniu;

- Proiect de Ordin pentru modificarea și completarea Ordinului ministrului administrației și internelor nr. 163/2011 privind preschimbarea permiselor de conducere naționale eliberate de autoritățile competente ale altor state cu documente similare românești;

- Proiect de Lege pentru modificarea și completarea Legii nr. 297/2004 privind piața de capital;

- Proiect de Hotărâre pentru aprobarea metodologiei privind realizarea obligațiilor ce revin autorităților și profesioniștilor implicați în prevenirea și intervenția în situația copiilor părăsiți în unități sanitare;

- Proiect de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind modalitatea de utilizare și completare a dosarului electronic de sănătate al pacientului.

Avize favorabile cu observații și propuneri

În cadrul avizelor favorabile emise în anul 2014, Autoritatea națională de supraveghere a formulat numeroase observații și propuneri care au avut ca scop asigurarea unei reglementări complete și redactarea clară a textelor legale, în scopul înțelegerii și aplicării corecte a acestora.

În acest context, precizăm faptul că majoritatea observațiilor și propunerilor formulate de către Autoritatea națională de supraveghere au fost însușite de către inițiatori. Dintre proiectele de acte normative asupra cărora Autoritatea națională de supraveghere a formulat propuneri, exemplificăm:

a) Proiectul revizuit al Acordului între Guvernul Republicii Bulgaria, Guvernul României și Guvernul Republicii Serbia privind înființarea și funcționarea Centrului Comun de cooperare polițienească și vamală

Autoritatea națională de supraveghere a subliniat că textul proiectului necesită o clarificare a dispozițiilor conținute și a recomandat reanalizarea textului de lege propus spre avizare.

S-a recomandat reformularea punctelor din proiect, în sensul că autoritățile competente ale părților contractante care transmit, respectiv primesc date cu caracter personal, sunt obligate să aplice măsurile tehnice și organizatorice adecvate pentru protejarea acestora împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispozițiile art. 17 alin. (1) din Directiva 95/46/EC a Parlamentului European și prevederile din legislația internă a fiecărei părți cu privire la asigurarea securității prelucrării datelor cu caracter personal.

S-a apreciat că este necesar ca autoritatea ce transmite datele să se asigure că acestea sunt adecvate, pertinente și neexcesive prin raportare la scopul pentru care au fost solicitate, autoritatea ce transmite datele trebuie să se asigure că datele sunt exacte și, dacă este cazul, actualizate.

Referitor la modalitățile de transmitere a datelor, a fost recomandată inserarea unor reguli mai detaliate privind modalitatea de transmitere a datelor în măsura în care există motive justificate de a presupune că astfel ar fi încălcate legislațiile naționale ale statelor semnatare ale Acordului sau interesele legitime ale persoanelor vizate ori cu privire la corectarea sau ștergerea datelor în situația în care se constată că au fost transmise date incorecte sau în privința cărora există interdicție de transmitere.

În plus, s-a evidențiat faptul că este necesară respectarea obligațiilor specifice privind drepturile persoanelor vizate, astfel încât o persoană vizată poate să obțină informații despre datele existente referitoare la ea și despre scopul folosirii acestor date, inclusiv că are posibilitatea exercitării dreptului de acces, rectificare sau ștergere, în condițiile legislației naționale a părții contractante, respectiv dacă furnizarea acestor informații nu afectează și activitățile de prevenire, cercetare și reprimare a infracțiunilor și de menținere a ordinii publice, precum și al altor activități desfășurate în domeniul dreptului penal, în limitele și cu restricțiile stabilite de lege.

În ceea ce privește dezvăluirea datelor unor terți așa cum era prevăzută în Acord, Autoritatea națională de supraveghere a precizat că datele cu caracter personal pot fi dezvăluite numai în vederea atingerii scopurilor pentru care datele au fost transmise inițial, cu acordul scris al autorității trimitătoare.

b) Proiectul Ordonanței Guvernului pentru reglementarea unor măsuri în domeniul financiar bancar

Autoritatea națională de supraveghere a subliniat că activitățile desfășurate în contextul reglementării domeniului bancar presupun efectuarea de operațiuni de prelucrare a unor categorii diferite de date cu caracter personal, printre care și date cu caracter special, precum codul numeric personal. Aceasta are implicații directe asupra drepturilor fundamentale ale persoanelor fizice și poate conduce la grave atingeri aduse dreptului la viață privată a cetățenilor, în ceea ce privește protecția datelor lor cu caracter personal.

Autoritatea națională de supraveghere a apreciat că este necesară definirea rolului și responsabilităților tuturor entităților implicate ce vor prelucra date cu caracter personal, stabilirea competențelor acestora în colectarea și prelucrarea datelor personale (administrator de portofoliu, agent, emitent, investitor, persoană afiliată, etc.), precum și clarificarea calității

acestora, respectiv de operatori sau împuterniciți, în sensul definițiilor date de Legea nr. 677/2001, modificată și completată.

Acestea se impun, cu atât mai mult cu cât operatorii de date cu caracter personal au o serie de obligații, printre care respectarea drepturilor și libertăților persoanelor vizate (de ex. deținătorii de obligațiuni – persoane fizice - garantate cu creanțe, și ale căror date vor fi prelucrate), precum și de a lua măsuri în vederea asigurării confidențialității și securității datelor colectate, stocate și utilizate.

S-a menționat că este necesară luarea în considerație a principiilor de protecție a datelor, în special prin stabilirea persoanelor autorizate, care vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate.

S-a semnalat faptul că activitățile desfășurate în legătură cu întocmirea și păstrarea anumitor registre, unele având caracter public (de ex. Registrul de evidență internă, sub-registre, Arhiva Electronică), dar și cu anumite raportări obligatorii către Banca Națională a României presupun efectuarea de operațiuni de prelucrare a unor categorii diferite de date cu caracter personal, inclusiv date având funcție de identificare de aplicabilitate generală (codul numeric personal).

Autoritatea națională de supraveghere a propus modificarea conținutului art. 53 din proiectul Ordonanței Guvernului pentru reglementarea unor măsuri în domeniul financiar bancar, în sensul că prelucrarea datelor cu caracter personal în legătură cu creanțele din portofoliul de creanțe de către agent, administratorul de portofoliu sau orice terț căruia îi sunt transferate obligațiile clientului față de deținătorii de obligațiuni garantate cu creanțe și/sau portofoliul de creanțe aferent, parțial sau în întregime, se va efectua în vederea realizării unui interes legitim, cu condiția ca acesta să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate.

Propunerea a avut la bază principiul proporționalității scopului, instituit prin art. 4 alin. (1) lit. c) din Legea nr. 677/2001 și s-a propus inserarea în cuprinsul art. 53 din proiectul Ordonanței Guvernului a unui nou alineat prin care să se stabilească că prelucrarea datelor este supusă regulilor prevăzute de Legea nr. 677/2001.

c) Memorandumul cu tema: Negocierea și semnarea Acordului între Ministerul Afacerilor Interne din România și Centrul Național Anticorupție al Republicii Moldova în domeniul prevenirii și combaterii corupției

Autoritatea națională de supraveghere a analizat conținutului documentului transmis spre avizare de Ministerul Afacerilor Interne și a considerat necesară reformularea unor prevederi ale acestuia în vederea oferirii unor garanții adecvate privind protecția datelor personale, în acord cu dispozițiile Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981 de către Consiliul Europei, în sensul adăugării Protocolului adițional la Convenție, cu privire la autoritățile de control și fluxul transfrontalier al datelor personale, adoptat la Strasbourg la 8 noiembrie 2001.

În același sens, Autoritatea națională de supraveghere a apreciat ca necesară introducerea în proiect de prevederi privind angajarea părților la respectarea drepturilor persoanelor vizate și a principiilor de prelucrare a datelor cu caracter personal în cadrul schimbului reciproc de date.

Cât privește dreptul de informare al persoanelor vizate, acesta trebuie asigurat prin precizarea că la cerere, acestea i se pot oferi informații despre datele care o privesc, precum și despre scopul folosirii datelor, numai dacă furnizarea acestor informații nu afectează activitățile desfășurate, în conformitate cu legislațiile statelor părților contractante, precum și la existența dreptului de a formula cerere pentru accesul, modificarea sau distrugerea ori ștergerea datelor.

Autoritatea națională de supraveghere a recomandat reformularea dispozițiilor din proiect privind transmiterea de date, în sensul introducerii de prevederi referitoare la obligațiile autorităților care transmit și primesc date de a aplica măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere obligațiile de securitate și confidențialitate prevăzute de art 19 și art. 20 din Legea nr. 677/2001, modificată și completată.

S-a considerat că este necesară introducerea de mențiuni exprese privind faptul că autoritățile competente care transmit și primesc date sunt obligate să țină o evidență a acestor activități, mențiuni referitoare la termenul de păstrare a acestora, la faptul că datele personale pot fi transmise altor entități prin canale care să asigure securitatea informațiilor, precum și

adăugarea măsurii de ștergere a datelor în situația în care se constată că au fost transmise date incorecte ori în privința cărora există interdicție de transmitere, motivat de comunicarea în sistem automatizat a acestora.

d) Proiectul Ordonanței de Urgență a Guvernului privind reținerea datelor necesare identificării consumatorilor în sectorul comunicațiilor electronice

Inițiativa legislativă a mai făcut obiectul unor propuneri legislative privind colectarea datelor personale ale utilizatorilor serviciilor de tip Prepay, dintre care ultima fiind în cursul anului 2013 (PLx. nr. 361/2013). Cu privire la textul acestei propuneri, Comisia pentru Tehnologia Informației și Comunicațiilor a Camerei Deputaților a emis un Raport de respingere, în conținutul căruia se precizează faptul că, Senatul, în calitate de primă Cameră sesizată, a respins propunerea legislativă. Comisia pentru Tehnologia Informației și Comunicațiilor a motivat respingerea, invocând printre altele, faptul că măsura colectării datelor personale este inutilă din punct de vedere practic deoarece pot fi achiziționate cartele prepay prin intermediul actelor de identitate false sau furate (pierdute) de către titulari ori cumpărate din alte state și utilizate pe teritoriul României. De asemenea, la nivelul Uniunii Europene nu există un act normativ obligatoriu de implementat în acest sens, iar în ceea ce privește Directiva 2006/24/CE privind reținerea datelor, Comisia Europeană a precizat în raportul de evaluare a acestei directive faptul că măsura înregistrării obligatorii a identității utilizatorilor nu a fost dovedită.

Autoritatea națională de supraveghere s-a pronunțat asupra textului proiectului Ordonanței de Urgență a Guvernului privind reținerea datelor necesare identificării consumatorilor în sectorul comunicațiilor electronice, față de care a formulat următoarele observații:

Titlul proiectului de act normativ face referire la „reținerea datelor” aspect care poate produce confuzie în contextul existenței reglementării distincte referitoare la reținerea datelor, și anume Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Autoritatea națională de supraveghere a subliniat necesitatea clarificării scopului colectării datelor de identificare a consumatorilor persoane fizice, respectiv utilizatorilor de servicii de comunicații electronice preplătite - „servicii de tip Prepay”, în contextul în care în proiectul de act normativ se face referire la „scopuri comerciale”, iar în Nota de fundamentare a proiectului se face referire la „stabilirea unui cadru juridic clar, bine definit în domeniul luptei împotriva criminalității organizate și în special a formelor sale grave ori cu caracter transfrontalier, precum și a actelor de terorism”.

În ceea ce privește definirea în proiect a anumitor termeni și expresii, s-a menționat că definițiile exprimate trebuie puse în acord cu termenii și expresiile definite în alte acte normative naționale în vigoare, referitoare la comunicațiile electronice, precum Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, Legea nr. 82/2012.

Autoritatea națională de supraveghere a apreciat că este necesară reanalizarea termenilor de consumator, utilizator, abonat raportat și la natura serviciilor de comunicații preplătite la care se referă proiectul ordonanței de urgență. În plus, s-a recomandat introducerea în textul propunerii a unor prevederi clare referitoare la datele personale și datele de identificare ale reprezentantului persoanei juridice ce ar urma să fie prelucrate în contextul achiziționării de servicii de comunicații preplătite, precum și modalitatea efectivă de colectare a datelor.

În ceea ce privește termenul instituit de proiect, de 3 ani, raportat la “datele reținute”, instituția noastră a subliniat că acesta este de natură a crea confuzie cu termenul de 6 luni prevăzut de Legea nr. 82/2012, fapt pentru care s-a recomandat utilizarea termenului de stocare, precum și precizarea clară a categoriilor de date care vor fi reținute pe o perioadă de 3 ani.

Prin instituirea obligației de furnizare a anumitor date cu caracter personal se restricționează accesul la anumite servicii de comunicații destinate publicului și, astfel, se poate aduce atingere libertății consumatorului de a lua decizii la achiziționarea de servicii de tip preplătit, dat fiind că, prin obligarea identificării poate fi influențată opțiunea consumatorului cu privire la achiziționarea sau nu a serviciului respectiv.

În acest context, s-a precizat că, potrivit art. 53 din Constituție, exercițiul unor drepturi sau al unor libertăți poate fi restrâns numai prin lege și numai dacă se impune, după caz, pentru apărarea securității naționale, a ordinii, a sănătății ori a moralei publice, a drepturilor și a libertăților cetățenilor; desfășurarea instrucției penale; prevenirea consecințelor unei calamități naturale, ale unui dezastru ori ale unui sinistru deosebit de grav.

Restrângerea poate fi dispusă numai dacă este necesară într-o societate democratică. Măsura trebuie să fie proporțională cu situația care a determinat-o, să fie aplicată în mod nediscriminatoriu și fără a aduce atingere existenței dreptului sau a libertății.

Cât privește stabilirea, prin proiectul supus avizării, în sarcina Autorității naționale de supraveghere de noi atribuții de constatare și sancționare a unor contravenții, s-a subliniat că aceste atribuții vin în contradicție cu rolul instituției noastre de a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a dreptului la viața privată, cu privire la prelucrarea datelor cu caracter personal.

e) Propunerea legislativă privind administrarea și gestionarea domeniului de nivel superior “.ro”.

În vederea stabilirii punctului de vedere al Guvernului, Autoritatea națională de supraveghere a formulat observații și propuneri.

Astfel, s-a apreciat că activitățile desfășurate în contextul reglementării administrării și gestionării a domeniului de nivel superior “.ro” presupun efectuarea de operațiuni de prelucrare a unor categorii diferite de date cu caracter personal (nume, adresă, număr de telefon, adresa de poștă electronică), care atrag incidența prevederilor Legii nr.677/2001.

S-a recomandat definirea rolului și responsabilităților tuturor entităților implicate în prelucrarea datelor cu caracter personal (Registrul pentru numele de domenii “.ro”- instituție publică cu rol în organizarea, administrarea și gestionarea domeniului de nivel superior “.ro”, registrari, etc.) stabilirea competențelor acestora, precum și clarificarea calității deținute.

De asemenea, s-a apreciat că ar putea fi luată în considerare introducerea unor prevederi referitoare la adoptarea de norme metodologice de aplicare a acestei legi, ținând cont de particularitatea obiectului acestei reglementări. S-a menționat faptul că în norme se pot stabili, în detaliu, prevederi referitoare la modalitatea de obținere a consimțământului persoanelor fizice, de exercitare a drepturilor persoanelor vizate, în special a dreptului de acces,

intervenție și de opoziție, precum și condițiile de încetare a operațiunilor de prelucrare a datelor cu caracter personal.

În concluzie, Autoritatea națională de supraveghere a apreciat că este necesar ca textul acestei propuneri legislative să se completeze în concordanță cu observațiile și propunerile de mai sus.

f) proiectul de Lege privind emisiunile de obligațiuni ipotecare

Autoritatea națională de supraveghere a avizat favorabil propunerea legislativă transmisă de Ministerul Finanțelor Publice, cu următoarele mențiuni:

Activitățile desfășurate de entități diverse (emitenții de obligațiuni, agenții, reprezentanții deținătorilor de obligațiuni, Banca Națională a României, etc.) în contextul reglementării emiterii de obligațiuni ipotecare presupun efectuarea de operațiuni de prelucrare a unor categorii diferite de date cu caracter personal. Aceasta poate avea implicații directe asupra drepturilor fundamentale ale persoanelor fizice și poate conduce la grave atingeri aduse dreptului la viață privată a cetățenilor, în ceea ce privește protecția datelor lor cu caracter personal.

În consecință, în prelucrarea datelor este necesară luarea în considerație a principiilor de protecție a datelor, în special prin stabilirea garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate și stabilirea persoanelor autorizate, care vor avea acces la date, în scopuri legitime.

S-a subliniat că activitățile desfășurate în legătură cu întocmirea și păstrarea anumitor registre, unele având caracter public (de ex. Registrul de evidență internă, sub-registre, Arhiva Electronică), dar și cu anumite raportări obligatorii către Banca Națională a României, presupun efectuarea de operațiuni de prelucrare a unor date având funcție de identificare de aplicabilitate generală (codul numeric personal), a căror prelucrare este supusă unor prevederi legale exprese.

Cât privește comunicările electronice a datelor între diverse entități la care face referire proiectul de Lege privind emisiunile de obligațiuni ipotecare, s-a precizat că o comunicare de acest tip se poate expune la o serie de riscuri, fapt pentru care trebuie să se aibă în vedere faptul că operatorii au obligația de a aplica măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal, în concordanță cu prevederile art. 20 din Legea nr. 677/2001.

În plus, s-a recomandat modificarea conținutului art. 53 din proiectul de Lege privind emisiunile de obligațiuni ipotecare, în sensul că „Prelucrarea datelor cu caracter personal în legătură cu creanțele din portofoliul de creanțe de către agent, administratorul de portofoliu sau orice terț căruia îi sunt transferate obligațiile emitentului față de deținătorii de obligațiuni ipotecare și/sau portofoliul de creanțe aferent, parțial sau în întregime, se efectuează cu respectarea prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare.”

g) Cartea verde privind sănătatea mobilă („m-sănătatea”)

La solicitarea Comisiei pentru afaceri europene din cadrul Senatului României, Autoritatea națională de supraveghere a făcut următoarele observații raportat la documentul intitulat Cartea verde privind sănătatea mobilă („m-sănătatea”)

În concordanță cu jurisprudența Curții Europene a Drepturilor Omului referitoare la încălcarea art. 8 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale, protecția oferită de acest articol ar fi diminuată în mod inacceptabil dacă folosirea de tehnici științifice moderne ar fi permisă cu orice preț și fără realizarea unui echilibru între beneficiile folosirii extensive a acestor tehnici și interesele importante legate de viața privată, iar orice stat care pretinde să aibă un rol de pionier în dezvoltarea noilor tehnologii poartă responsabilitatea obținerii unui echilibru corect în această problemă (Cauza S. și M. Marper contra Regatului Unit, 2008).

Implementarea în domeniul sănătate mobilă - „m-sănătatea” a unor soluții tehnologice (de ex. de tip smartphones) ce permit colectarea și prelucrarea unui număr considerabil de date, precum datele medicale, presupune o prelucrare pe scară largă a datelor personale și poate reprezenta o nouă situație de risc pentru protecția datelor cu caracter personal ale persoanelor fizice și, implicit, respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață privată.

Sistemele și tehnologiile folosite în *m-sănătate* se bazează pe colectarea și prelucrarea unor categorii variate de date cu caracter personal, mai ales dintre cele sensibile (date privind starea de sănătate, caracteristici fiziologice, date biometrice, etc.). Totodată, în conformitate cu art. 12 și art. 14 din Directiva 95/46/EC, dezvoltatorii și furnizorii de tehnologii din *m-sănătate*

trebuie să permită utilizatorilor de aplicații (persoane vizate) să își exercite drepturile de acces, de rectificare, de ștergere sau de blocarea datelor cu caracter personal în cazul în care acestea sunt incomplete, inexacte sau prelucrate necorespunzător.

O situație deosebită în *m-sănătate* este reprezentată de luarea unor decizii automatizate pe baza datelor agregate, caz în care operatorul de date trebuie să informeze, de asemenea, utilizatorul.

Referitor la comunicările electronice ale datelor privind starea de sănătate efectuate între persoane vizate ce utilizează soluții tehnologice de sănătate mobilă și diverse entități (medici, spitale, unități farmaceutice sau de cercetare, etc.), Autoritatea națională de supraveghere a subliniat că o comunicare de acest tip se poate expune la o serie de riscuri, fapt pentru care atât operatorii cât și persoanele împuternicite de către operatori au obligația de a aplica măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal, având în vedere dispozițiile art. 17 alin. (1) din Directiva 95/46/EC a Parlamentului European.

Pentru a se respecta obligațiile în materie de securitate și confidențialitate în *m-sănătate* este necesar ca dezvoltatorii și furnizorii de aplicații, producătorii de sisteme de operare și de dispozitive, precum și terții, să evalueze continuu atât riscurile existente, cât și riscurile viitoare în ceea ce privește protecția datelor.

Autoritatea națională de supraveghere a apreciat, în acest context, că trebuie să se țină seama de principiile referitoare la respectarea vieții private începând cu momentul conceperii („privacy by design”) sistemelor *m-sănătate* și referitoare la respectarea vieții private în setările standard („privacy by default”).

Conform acestor principii statuate în Directiva 2002/58/CE, producătorii de dispozitive sau de aplicații au obligația de a integra protecția datelor încă din momentul conceperii unui sistem/aplicație/dispozitiv. Prin urmare, producătorii de sisteme de operare și de dispozitive, în calitate de operatori, dețin o responsabilitate importantă în ceea ce privește garantarea protecției datelor cu caracter personal și a vieții private a utilizatorilor de aplicații. Aceasta include garantarea disponibilității mecanismelor corespunzătoare de informare a utilizatorilor finali cu privire la ceea ce pot face aplicațiile și la tipul de date care pot fi accesate, precum și cu privire la furnizarea setărilor corespunzătoare care permit utilizatorilor aplicației să modifice parametrii procesului de prelucrare a datelor.

Secțiunea a 3-a Puncte de vedere privind chestiuni de protecția datelor

A. Condiții generale de prelucrare a datelor cu caracter personal

1. O persoană fizică a solicitat un punct de vedere în legătură cu aplicabilitatea prevederilor Legii nr. 677/2001 în contextul alegerilor pentru Parlamentul European.

S-a comunicat solicitantului faptul că un candidat independent la alegerile europarlamentare are calitatea de operator de date cu caracter personal și este necesar să se notifice Autorității naționale de supraveghere prelucrarea efectuată, în vederea înscrierii acesteia în Registrul de evidență a prelucrărilor de date cu caracter personal.

De asemenea, au fost comunicate informații cu privire la procedura de notificare a prelucrărilor de date, în vederea obținerii înregistrării în Registrul electronic de evidență a prelucrărilor de date cu caracter personal.

În plus, au fost solicitate clarificări referitoare la situația în care un operator de date își va desemna un reprezentant care trebuie să fie o persoană stabilită în România. Prevederile Legii nr. 677/2001 aplicabile operatorului sunt aplicabile și reprezentantului acestuia.

Noțiunea de reprezentant prevăzută de Legea nr. 677/2001 se referă la situațiile în care operatorul este stabilit într-un stat terț, dar desfășoară în țara noastră prelucrări de date cu caracter personal. În acest caz, se impune desemnarea unui reprezentant (persoană fizică sau juridică) care va avea toate obligațiile ce subzistă în sarcina operatorului (de ex. depunerea notificării la Autoritatea de supraveghere).

S-a precizat că, ulterior dobândirii de către România a calității de membru cu drepturi depline al Uniunii Europene, având în vedere dispozițiile constituționale ale art. 148 din Constituție și făcând aplicarea principiului priorității dreptului comunitar statuat de Curtea de Justiție a UE, operatorul situat în state de pe teritoriul Uniunii Europene sau al Zonei Economice Europene nu are obligația desemnării unui reprezentant în sensul Legii nr. 677/2001. În notificarea efectuată de operator vor fi completate datele de identificare ale reprezentantului.

În ceea ce privește prelucrarea datelor prin împuternicit au fost făcute mențiuni, în sensul că, potrivit Legii nr. 677/2001, persoană împuternicită de către operator este o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și

structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului.

În cazul prelucrărilor de date prin împuterniciți, obligațiile privind notificarea prelucrărilor către Autoritatea națională de supraveghere, revin operatorilor de date cu caracter personal, iar nu împuterniciților acestora.

Efectuarea prelucrărilor prin persoane împuternicite trebuie să se desfășoare în baza unui contract încheiat în formă scrisă, care va cuprinde în mod obligatoriu obligația persoanei împuternicite de a acționa doar în baza instrucțiunilor primite de la operator și faptul că îndeplinirea obligațiilor privind aplicarea de măsuri de securitate revine și persoanei împuternicite.

2. Un operator de telefonie mobilă a solicitat un punct de vedere referitor la încadrarea în categoria de date cu caracter personal a următoarelor informații: numărul de telefon de la care se inițiază un apel, numărul de telefon care recepționează un apel, IP (sursă/destinație), alte date de trafic.

Autoritatea națională de supraveghere a subliniat că, prin prisma definiției datelor cu caracter personal din art. 3 lit. a) al Legii nr. 677/2001, atât numărul de telefon (indiferent dacă este cel de la care se inițiază un apel sau dacă este cel care recepționează un apel), cât și IP (sursă/destinație), în măsura în care sunt alocate unui abonat/utilizator persoană fizică, constituie informații ce pot conduce la identificarea persoanei, în mod direct sau prin asociere cu alte date. Ca atare, datele menționate anterior constituie date cu caracter personal, aflate sub incidența Legii nr. 677/2001.

În ceea ce privește interconectarea mai multor sisteme de evidență deținute de același operator, s-a precizat că este necesar ca acesta să analizeze în ce măsură scopul prelucrării datelor este același pentru sistemele deținute și, sub acest aspect, s-a subliniat că interconectarea nu se poate realiza dacă sistemele în cauză au fost constituite în scopuri incompatibile.

Autoritatea națională de supraveghere a apreciat că interconectarea mai multor sisteme de evidență, chiar și cele create în același scop, precum și comunicare electronică a datelor sunt operațiuni ce pot expune datele unei serii de riscuri fapt pentru care operatorii au obligația de a aplica măsuri în conformitate cu dispozițiile art. 20 din Legea nr. 677/2001.

S-a specificat faptul că operatorului de telefonie mobilă îi revin obligațiile specifice stabilite prin reglementările speciale incidente, iar în calitatea sa de operator de date cu caracter personal îi revin obligațiile prevăzute de Legea nr. 677/2011, inclusiv în ceea ce privește transmiterea de date în Uniunea Europeană.

B. Raportarea la biroul de credit

1. O persoană fizică a solicitat informații referitoare la raportarea sa, de către o instituție de credit, la biroul de credit, fără fi informată, potrivit dispozițiilor legale.

Autoritatea națională de supraveghere a specificat că, potrivit art. 8 alin. (2) din Decizia nr. 105/2007 a președintelui Autorității de supraveghere, datele negative, inclusiv cele rezultate din aplicarea comisioanelor sau din majorări ale ratei dobânzilor, se transmit către sistemele de evidență de tipul birourilor de credit numai după înștiințarea prealabilă, realizată de către participanți în scris, telefonic, prin SMS sau e-mail, a persoanei vizate cu privire la întârzierea la plată și transmiterea datelor, realizată cu cel puțin 15 zile calendaristice înainte de data transmiterii.

De asemenea, potrivit art. 4 alin. (4) din aceeași decizie, datele înregistrate în sisteme de evidență de tipul birourilor de credit pot fi actualizate, modificate, completate sau șterse fie direct de către participantul care a transmis datele (în speță instituția de credit – subl. ns.), fie de către biroul de credit la cererea sau în acord cu participantul.

În aplicarea art. 14 din Legea nr. 677/2001, orice persoană vizată are dreptul de a obține de la operator, la cerere și în mod gratuit după caz, rectificarea, actualizarea, blocarea sau ștergerea datelor a căror prelucrare nu este conformă prezentei legi, în special a datelor incomplete sau inexacte.

Acest drept se exercită printr-o cerere scrisă, datată și semnată, adresată în mod direct operatorului.

În consecință, s-a precizat că, în situația în care petiționarul apreciază că i s-au încălcat drepturile garantate, în sensul că nu a fost informat în legătură cu raportarea sa la biroul de credit și dorește ștergerea datelor din evidențele acestuia, în conformitate cu art. 25 alin. (3) din Legea nr. 677/2001, trebuie să se adreseze în prealabil instituției de credit în cauză.

2. O instituție financiar-bancară a solicitat opinia Autorității naționale de supraveghere cu privire la condițiile raportării clienților băncilor către biroul de credit în cazul întâzierilor la plată.

Au fost făcute precizări legate de condițiile legale de prelucrare a datelor cu caracter personal în sisteme de evidență de tipul birourilor de credit, care au fost reglementate de Autoritatea națională de supraveghere prin emiterea Deciziei nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit.

Astfel, art. 8 alin. (1) din Decizia nr. 105/2007 stabilește regula de raportare a datelor personale către sistemele de evidență de tipul birourilor de credit, respectiv numai cu acordul scris al persoanei vizate, obținut de participanți la data depunerii cererii de credit. În acest sens, la obținerea acordului este necesar să se realizeze și informarea persoanei vizate, pentru ca aceasta să își dea un consimțământ în cunoștință de cauză.

Potrivit art. 8 alin. (2) din Decizia nr. 105/2007, datele negative, inclusiv cele rezultate din aplicarea comisioanelor sau din majorări ale ratei dobânzilor, se transmit către sistemele de evidență de tipul birourilor de credit numai după înștiințarea prealabilă, realizată de către participanți în scris, telefonic, prin SMS sau e-mail, a persoanei vizate cu privire la întâziera la plată și transmiterea datelor, realizată cu cel puțin 15 zile calendaristice înainte de data transmiterii.

În consecință, Autoritatea națională de supraveghere consideră că înștiințarea prealabilă a persoanei vizate, cu cel puțin 15 zile înainte de data transmiterii la biroul de credit, trebuie să conțină informațiile stabilite la art. 9 din Decizia nr. 105/2007 și trebuie realizată înainte de fiecare transmitere a datelor negative.

C. Prelucrarea codului numeric personal si a unor categorii speciale de date

1. Un petent a solicitat Autorității naționale de supraveghere punctul de vedere cu privire la durata stocării datelor personale, inclusiv a CNP-ului, de către o bancă și cadrul legislativ aplicabil, solicitând în același timp și comunicarea modalității de a cere ștergerea acestor date.

Potentului i s-a comunicat că, în privința prelucrării codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, dispozițiile art. 8 alin. (1) din Legea nr. 677/2001 coroborate cu prevederile art. 2 alin (1) din Decizia nr.

132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, stabilesc că aceasta poate fi efectuată numai dacă persoana vizată și-a dat în mod expres și neechivoc consimțământul, dacă prelucrarea este prevăzută în mod expres de o dispoziție legală, ori în alte cazuri, cu avizul Autorității de Supraveghere și numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

În ceea ce privește durata stocării datelor cu caracter personal, Legea nr. 677/2001 nu conține dispoziții exprese privind instituirea în sarcina operatorului a obligației de a stoca datele cu caracter personal o anumită perioadă de timp.

Însă, potrivit art. 4 alin. (1) lit. e) din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul unei prelucrări trebuie să fie 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.

Petentului i s-a precizat că în ceea ce privește prelucrarea, de către o instituție financiară, a datelor clienților după încheierea relațiilor contractuale cu aceștia, potrivit art. 19 din Legea nr. 656/2002 pentru prevenirea și sancționarea spălării banilor, precum și pentru instituirea unor măsuri de prevenire și combatere a finanțării actelor de terorism, republicată, „ în fiecare caz în care identitatea este solicitată potrivit prevederilor prezentei legi, persoana juridică sau persoana fizică prevăzută la art. 10 (s.n. instituțiile de credit), care are obligația identificării clientului, va păstra o copie de pe document, ca dovadă de identitate, sau referințe de identitate, pentru o perioadă de minimum 5 ani, începând cu data când se încheie relația cu clientul. Persoanele prevăzute la art. 10 vor păstra evidențele secundare sau operative și înregistrările tuturor operațiunilor financiare ce decurg din derularea unei relații de afaceri ori a unei tranzacții ocazionale pe o perioadă de minimum 5 ani de la încheierea relației de afaceri, respectiv de la realizarea tranzacției ocazionale, într-o formă corespunzătoare, pentru a putea fi folosite ca mijloace de probă în justiție.”

2. O instituție publică a solicitat punctul de vedere cu privire la petiția unui angajat al său prin care se ridică problema colectării informațiilor privind religia.

Autoritatea națională de supraveghere a precizat că, raportat la dispozițiile Legii nr. 677/2001, solicitarea, de către angajator, a informațiilor referitoare la religia unui angajat reprezintă, în accepțiunea legii, o prelucrare de date cu caracter personal.

Legea nr. 677/2001 stabilește condițiile în care datele cu caracter personal pot fi prelucrate. Potrivit dispozițiilor acestui act normativ, regula generală ce guvernează prelucrarea datelor personale este consimțământul persoanei în cauză, dat în mod expres și neechivoc.

În mod excepțional însă, datele cu caracter personal pot fi prelucrate fără consimțământul persoanei vizate, în mai multe situații de excepție. Aceste cazuri, de strictă interpretare, sunt menționate în mod expres la art. 5 alin. (2) din Legea nr. 677/2001 (pentru datele care nu au caracter special, cum ar fi numele, prenumele, adresa poștală, e-mail, nr. de telefon), precum și la art. 7, 8, 9 și 10 din aceeași lege, pentru datele cu caracter special (spre exemplu, datele privind originea rasială sau etnică, convingerile religioase, apartenența sindicală, starea de sănătate, codul numeric personal, faptele penale sau contravențiile).

Astfel, potrivit art. 7 alin. (1) din Legea nr. 677/2001, prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenență sindicală, precum și a datelor cu caracter personal privind starea de sănătate sau viața sexuală este interzisă.

Prevederile alin. (1) nu se aplică în unele cazuri, precum cel în care prelucrarea este necesară în scopul respectării obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanțiilor prevăzute de lege; o eventuală dezvăluire către un terț a datelor prelucrate poate fi efectuată numai dacă există o obligație legală a operatorului în acest sens sau dacă persoana vizată a consimțit expres la această dezvăluire;

Prin urmare, s-a apreciat că în cazul pus în discuție devin aplicabile dispozițiile art. 7 alin. (2) lit. b), respectiv când prelucrarea este necesară în scopul respectării obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanțiilor prevăzute de lege.

Coroborat cu aceste dispoziții, pe de o parte, Codul muncii – Legea nr. 53/2003, republicată, cu modificările și completările ulterioare stabilește, în art. 139, obligația angajatorului de a acorda două zile libere pentru fiecare dintre cele 3 sărbători religioase

anuale, declarate astfel de cultele religioase legale, altele decât cele creștine, pentru persoanele aparținând acestora.

Pe de altă parte, Legea nr. 677/2001 instituie o serie de principii ale prelucrării datelor care trebuie respectate, indiferent de condițiile de legitimitate a prelucrărilor, respectiv pe baza consimțământului persoanei vizate sau pe baza situațiilor de excepție de la consimțământ.

Legea nr. 677/2001 garantează, de asemenea, o serie de drepturi persoanelor vizate (angajații), cum ar fi cel de informare și de opoziție (art. 12 și art. 15) și obligă operatorul (angajatorul) la asigurarea confidențialității și securității datelor.

De altfel, asigurarea dreptului la informare și a confidențialității datelor cu caracter personal se înscrie și printre obligațiile angajatorului stabilite în Codul muncii.

În consecință, solicitarea, de către angajator, a declarării religiei angajatului în cauză, în scopul îndeplinirii obligațiilor specifice ale operatorului în domeniul dreptului muncii se încadrează în dispozițiile legale sus-menționate, în sensul că această informație poate fi solicitată, cu respectarea garanțiilor prevăzute de lege.

3. O societate comercială a solicitat punctul de vedere în ceea ce privește utilizarea unui sistem de acces bazat pe amprentarea angajaților.

Autoritatea națională de supraveghere a subliniat că, potrivit Legii nr. 677/2001, reprezintă date cu caracter personal orice date referitoare la o persoană fizică identificată sau identificabilă, inclusiv datele biometrice.

În contextul necesității asigurării unei protecții eficiente a dreptului la viață privată, raportat la principiul proporționalității prelucrărilor instituit de art. 4 alin. (1) lit. c) din Legea nr. 677/2001, Autoritatea națională de supraveghere a interzis prelucrarea datelor biometrice în scop de control acces persoane și/sau pontaj, considerată o prelucrare excesivă raportat la scopul urmărit.

S-a recomandat folosirea unei soluții alternative la sistemul de control acces persoane și/sau pontaj bazat pe amprentarea angajaților, eventual un sistem bazat pe utilizarea unui cod PIN, asociat altor date de identificare ale angajaților. Totodată, s-a precizat că pentru accesul persoanelor în anumite locații se poate utiliza cardul magnetic la care faceți referire în adresa dumneavoastră.

D. Dezvăluirea datelor cu caracter personal în publicații oficiale și indexarea acestora de motoare de căutare

O persoană fizică a solicitat informații privind publicarea datelor cu caracter personal în Monitorul Oficial al României și indexate de motorul de căutare Google.

Autoritatea națională de supraveghere a subliniat că Legea nr. 677/2001 instituie principiul proporționalității scopului, care trebuie respectat, corelat cu condițiile de legitimitate a prelucrărilor, respectiv pe baza consimțământului persoanei vizate sau pe baza situațiilor de excepție de la consimțământ.

În consecință, datele cu caracter personal pot fi dezvăluite, în situația în care nu există consimțământul persoanei vizate, numai în condițiile legale de excepție, prevăzute mai sus, cu respectarea principiului proporționalității scopului. În acest sens, scopul solicitării datelor (sau al dezvăluirii lor) trebuie încadrat în una dintre situațiile de excepție de la consimțământ.

În ceea ce privește publicarea de date cu caracter personal în Monitorul Oficial al României, s-a precizat că editarea și punerea la dispoziție a publicației se face în temeiul art. 18 din Legea nr. 202/1998, republicată.

Autoritatea națională de supraveghere a solicitat informații suplimentare R.A. Monitorul Oficial S.A. care a precizat că „odată publicate în Monitorul Oficial al României, informațiile publicate devin publice, „Regia Autonomă Monitorul Oficial neputând restricționa circulația acestei informații”. De asemenea, s-a precizat că „Regiei Autonome Monitorul Oficial nu i se aplică dispozițiile Legii nr. 109/2007 privind reutilizarea informațiilor din instituțiile publice deoarece aceasta nu face parte din instituțiile publice la care face referire art. 4 lit. a pct. 3 întrucât scopul activității desfășurate are caracter comercial conform Legii nr. 50/1990, Hotărârii Guvernului nr. 358/1991, iar documentul în cauză nu este deținut de regie, acesta fiind o informație publică.”

În consecință, Autoritatea națională de supraveghere a apreciat că datele cu caracter personal publicate în Monitoarele Oficiale ale României (documente cu caracter de public) pot fi reutilizate numai cu respectarea principiilor și condițiilor referitoare la prelucrarea datelor personale prevăzute de art. 4 și art. 5 din Legea nr. 677/2001 și cuprinse în art. 6, art. 7 și art. 8 ale Directivei 96/45/EC a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date).

Cât privește datele cu caracter personal indexate de motorul de căutare Google, precum cele publicate în Monitoarele Oficiale ale României, petentului i-au fost furnizate următoarele informații, legate de cauza C-131/12, dintre Google Spain SL și Google Inc. împotriva Agenției Spaniole de Protecția Datelor, prin care Curtea de Justiție a Uniunii Europene (CJUE) a stabilit că:

- activitatea unui motor de căutare (care constă în găsirea informațiilor publicate sau introduse pe internet de către terți, indexarea acestora în mod automat și stocarea lor temporară și, în cele din urmă, punerea acestora la dispoziția utilizatorilor de internet într-o anumită ordine de preferință) trebuie calificată drept prelucrare a datelor cu caracter personal, în temeiul prevederilor art. 2 lit. (b) din Directiva 95/46/CE;

- operatorul acestui motor de căutare trebuie considerat „operator”, în sensul articolului 2 litera (d) din Directiva 95/46/CE;

- în cazul în care operatorul unui motor de căutare înființează într-un stat membru o sucursală sau o filială destinată promovării și vânzării spațiului publicitar de pe pagina acestui motor, a cărei activitate este orientată către locuitorii aceluși stat membru, atunci se consideră că prelucrarea datelor cu caracter personal este efectuată în cadrul activităților unui operator cu sediul pe teritoriul respectivului stat membru, în sensul prevederilor art. 4 alin. (1) lit. (a) din Directiva 95/46/EC;

- pentru respectarea drepturilor prevăzute de art. 12 lit. (b) și art. 14 primul paragraf lit. (a) din Directiva 95/46/EC (dreptul de intervenție și de ștergere), operatorul unui motor de căutare este obligat să elimine de pe lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele unei persoane, link-urile către paginile web publicate de terți și care conțin informații referitoare la respectiva persoană;

- art. 12 litera (b) și art. 14 primul paragraf lit. (a) din Directiva 95/46 trebuie interpretate în sensul că operatorul unui motor de căutare trebuie să se examineze în special dacă persoana vizată are dreptul ca informația respectivă referitoare la persoana sa să nu mai fie, în stadiul actual, asociată cu numele său de o listă de rezultate, afișată în urma unei căutări efectuate plecând de la numele său. Întrucât persoana vizată poate, având în vedere drepturile sale fundamentale prevăzute la articolele 7 și 8 din Carta Drepturilor Fundamentale a UE (dreptul la viață privată, dreptul la protecția datelor cu caracter personal), să solicite ca informația în cauză să nu mai fie pusă la dispoziția publicului prin intermediul includerii sale

Într-o asemenea listă de rezultate, aceste drepturi prevalează în principiu nu numai asupra interesului economic al operatorului motorului de căutare, ci și asupra interesului publicului de a avea acces la informația respectivă cu ocazia unei căutări referitoare la numele acestei persoane. Nu aceasta ar fi însă situația dacă ar reieși că, din motive speciale, precum rolul jucat de persoana respectivă în viața publică, ingerința în drepturile sale fundamentale este justificată de interesul preponderent al publicului menționat de a avea acces, prin intermediul acestei includeri, la informația în cauză.

(<http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=259474>)

În urma acestei hotărâri, Google Inc. a precizat că a efectuat diligențele necesare pentru a oferi persoanelor vizate posibilitatea de a formula către Google cereri de ștergere a datelor lor personale, prin accesarea link-ului:

https://support.google.com/legal/contact/lr_eudpa?product=websearch

În aplicarea acestei hotărâri a CJUE, Google Inc. a precizat că aceste cereri vor fi analizate pentru a se asigura echilibrul între dreptul la viață privată și dreptul la liberă informare, avându-se în vedere dacă există un interes public în menținerea unei informații, cum ar fi cele privind malpraxisul profesional al unei persoane, condamnări penale sau conduita funcționarilor publici.

F. Transmitere/transfer de date cu caracter personal

O societate comercială a solicitat informații privind condițiile transferului datelor cu caracter personal ale angajaților societății.

Respectându-se principiile comunitare enunțate de Directiva 95/46/EC, în Legea nr. 677/2001 au fost stabilite o serie de reguli și excepții cu privire la transferul datelor în străinătate, având în vedere, în primul rând, principiul conform căruia statele membre vor permite transferul doar dacă statele de destinație către care se transferă datele asigură un nivel de protecție adecvat al datelor cu caracter personal. Condițiile de efectuare a transferului în străinătate al datelor cu caracter personal sunt prevăzute la în art. 29 și art. 30 din Legea nr. 677/2001.

Regula generală menționată în art. 29 alin. (1) din Legea nr. 677/2001 prevede că transferul datelor poate avea loc cu respectarea cumulativă a două condiții, respectiv dacă nu

se încalcă legea română și statul către care se intenționează transferul asigură un nivel de protecție adecvat. În general, se consideră a avea un nivel de protecție adecvat toate statele membre ale Uniunii Europene, din zona economică europeană, precum și cele cărora Comisia Europeană le-a recunoscut, prin decizie, faptul că legislația internă adoptată prezintă condițiile necesare pentru protecția persoanelor cu privire la prelucrarea datelor lor personale.

Referitor la transferul datelor cu caracter personal către state a căror legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română (cum este, spre exemplu, Federația Rusă), acestea pot fi autorizate de către autoritatea de supraveghere dacă operatorul care exportă datele prezintă garanții suficiente cu privire la protecția drepturilor fundamentale ale persoanelor. Aceste garanții trebuie să fie stabilite prin contracte încheiate între operatorul care exportă datele și destinatarul din străinătate al acestor date. Precizăm că aceste contracte trebuie să respecte prevederile art. 29 alin. (4) din Legea nr. 677/2001 și ale deciziilor Comisiei Europene privind clauzele contractuale standard în cazul transferului datelor în străinătate către un operator sau către un împuternicit.

În același timp, art. 30 din Legea nr. 677/2001 prevede situațiile în care transferul este întotdeauna permis.

În cazul expus, societății comerciale din România îi revine obligația de a declara Autorității naționale de supraveghere, prin notificarea depusă înainte de efectuarea oricărei prelucrări ori a oricărui ansamblu de prelucrări având același scop sau scopuri corelate, în vederea autorizării, prelucrarea datelor angajaților săi și transferul acestora către o societate cu sediul într-un stat terț.

II. Aplicabilitatea Deciziei nr. 52/2012

1. O societate comercială a solicitat acordarea avizului Autorității naționale de supraveghere pentru prelucrarea datelor cu caracter personal ale angajaților, efectuată prin mijloace de supraveghere video, în temeiul art. 8 alin. (3) din Decizia nr. 52/2012.

Autoritatea națională de supraveghere, în contextul susținerilor societății și al necesității asigurării unei protecții eficiente a dreptului la viață privată a angajaților, raportat la caracterul determinat, explicit și legitim al scopului și al proporționalității prelucrării, față de solicitarea de acordare a avizului în temeiul art. 8 alin. (3) din Decizia nr. 52/2012, a considerat că elementele justificative prezentate nu justifică acordarea avizului.

Astfel, deși se solicita avizul în baza art. 8 alin. (3) din Decizia nr. 52/2012, se susținea că sistemul de supraveghere video nu are rolul de a monitoriza corectitudinea și eficiența cu care angajații își desfășoară activitatea și nu are nicio legătură cu activitatea lor profesională. În același timp, se menționa că există deja instalate camere de supraveghere video la intrarea în sediul societății.

Raportat la solicitarea societății și susținerile sale contradictorii, nu rezulta cu claritate care era scopul prelucrării datelor angajaților în birouri.

Nu au fost prezentate concret situații în care au fost săvârșite fapte penale de către angajați, soluționate definitiv de către organele competente și în urma cărora societatea ar fi suferit prejudicii importante. Mai mult, din cele prezentate de societate nu rezulta că ar fi fost efectuată consultarea sindicatului sau a reprezentanților salariaților, astfel cum prevăd dispozițiile legale din Codul muncii, atunci când sunt afectate drepturile angajaților.

În consecință, instituția noastră nu a acordat avizul solicitat.

2. O unitate medicală a solicitat acordarea avizului Autorității naționale de supraveghere, potrivit Deciziei nr. 52/2012, pentru prelucrarea prin mijloace de supraveghere video a datelor cu caracter personal ale angajaților acesteia, ce își desfășoară activitatea într-unul dintre pavilioanele unității.

Autoritatea națională de supraveghere a analizat solicitarea operatorului de date, în contextul prevederilor Legii nr. 677/2001 și ale Decizia nr. 52/2012, potrivit căreia se interzice efectuarea acestei prelucrări, excepțiile fiind situațiile expres prevăzute într-un act normativ care obligă angajatorul la instituirea sistemelor de supraveghere video sau cele autorizate de Autoritatea de supraveghere, potrivit art. 8 alin. (3) din Decizia nr. 52/2012, în situații temeinic justificate.

Preambulul Recomandării nr. R (89)2 a Comitetului de Miniștri al Consiliului Europei, cu privire la protecția datelor cu caracter personal utilizate în scopul angajării, se precizează că: "angajații ar putea liber deveni o populație captivă, care se află permanent sub supravegherea procedeelelor tehnologice, dacă nu este reamintit faptul că angajații sunt înainte de toate persoane care au nevoie de a întreține contacte sociale cu colegii lor cu privire la lucrul lor. Tehnologia nu ar trebui să fie utilizată în așa fel ca să împiedice relațiile sociale între angajați. Sub un alt aspect, respectarea demnității umane se referă la necesitatea de a evita dezumanizarea statistică, care poate aduce prejudiciu identității angajaților prin intermediul

tehnicienilor de prelucrare a datelor care permit să stabilească profilul angajaților sau luarea deciziilor fondate pe prelucrarea automată”.

Autoritatea națională de supraveghere, raportat la situația descrisă de operator, a apreciat că, pe de o parte, nu există obligație legală expresă a cărei îndeplinire să conducă la prelucrarea datelor cu caracter personal a angajaților prin mijloace de supraveghere video și, pe de altă parte, nu au fost prezentate argumente temeinice privind interesul legitim al instalării unui astfel de sistem de supraveghere al angajaților și care să prevaleze față de drepturile și libertățile fundamentale sau interesele acestora.

S-a luat în considerație și faptul că operatorul nu a făcut dovada consultării sindicatului sau a reprezentanților salariaților, astfel cum prevăd dispozițiile din Codul muncii menționat anterior ori cea a obținerii consimțământului expres și neechivoc al angajaților.

Față de solicitarea de acordare a avizului, în contextul necesității asigurării unei protecții eficiente a dreptului la viață privată a angajaților, raportat la caracterul determinat, explicit și legitim al scopului și al proporționalității prelucrării datelor lor cu caracter personal, s-a precizat că elementele prezentate de unitatea medicală în adresa transmisă nu îndeplinesc condițiile stipulate de art. 8 din Decizia nr. 52/2012 și, de asemenea, nu justifică acordarea avizului în temeiul alin. (3) al aceluiași articol.

III. Aplicabilitatea Legii nr. 238/2009

1. O structură de poliție a solicitat avizul potrivit art. 31 din Legea nr. 238/2009, în contextul necesității stabilirii anumitor perioade de stocare a datelor prelucrate în Sistemului Național de Raportare a Incidentelor (SNRI).

Autoritatea națională de supraveghere a precizat că, în conformitate cu art. 4 alin. (1) lit. e) din Legea nr. 677/2001, datele prelucrate trebuie 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.

Ca excepție, este permisă stocarea datelor pe o durată mai mare, în scopuri statistice, de cercetare istorică sau științifică, dar aceasta se va face cu respectarea garanțiilor legale stabilite în normele care reglementează aceste domenii.

În consecință, respectarea principiului duratei de stocare implică stabilirea, în mod justificat, a anumitor perioade de păstrare a datelor, cu excepția situațiilor în care o reglementare legală stabilește în mod expres aceasta.

Față de termenele stabilite de operator, s-a remarcat faptul că acestea nu se raportau la un anumit moment clar determinat de începere a curgerii lor.

Autoritatea națională de supraveghere nu a formulat un aviz favorabil, ci a solicitat precizarea argumentelor pe baza cărora au fost stabilite termenele de stocare pentru fiecare dintre componentele SNRI și a recomandat să se aibă în vedere stabilirea momentului de la care începe să curgă termenele stabilite, pentru toate situațiile în care acesta nu a fost menționat.

2. O altă structură de poliție a solicitat avizarea, potrivit art. 18 alin. (3) din Legea nr. 238/2009, a interconectării unor sisteme de evidență ale acesteia cu o altă instituție publică.

Art. 18 alin. (1) și alin. (2) din Legea nr. 238/2009 stabilește că interconectarea sistemelor de evidență a datelor cu caracter personal deținute de structurile/unitățile M.A.I. sau de alți operatori se poate efectua pentru realizarea activităților de cercetare și combatere a infracțiunilor.

Potrivit alin. (6) al aceluiași articol, accesul direct sau printr-un serviciu de comunicații electronice la un sistem de evidență a datelor cu caracter personal care face obiectul interconectării, potrivit alin. (1), este permis numai în condițiile legii și cu respectarea prevederilor art. 1 alin. (1) și ale art. 6-24 din Legea nr. 238/2009.

Autoritatea națională de supraveghere a solicitat să se precizeze explicit scopul urmărit de cele două autorități, pentru care se solicită această interconectare a sistemelor de evidență, să se detalieze, raportat prevederile din Legea nr. 238/2009, modalitatea de stocare și comunicare a datelor cu caracter personal conținute de acest sisteme de evidență, modalitatea de asigurare a respectării drepturilor persoanelor vizate, precum și modalitatea de îndeplinire a obligației de notificare.

În consecință, nu s-a acordat avizul solicitat.

Secțiunea a 4-a Activitatea de reprezentare în fața instanțelor de judecată

Soluțiile pronunțate de instanțele de judecată în cursul anului 2014, în litigiile aflate pe rolul acestora, confirmă existența unei abordări și interpretări similare cu aceea a Autorității naționale de supraveghere cu privire la aplicarea reglementărilor specifice domeniului protecției datelor cu caracter personal.

În ceea ce privește obiectul acțiunilor promovate în fața instanțelor de judecată, cele mai multe au avut ca obiect anularea proceselor-verbale de contravenție, prin care se constata săvârșirea contravențiilor de omisiune de notificare și de prelucrare nelegală de date cu caracter personal, inclusiv ca urmare a nerespectării drepturilor persoanelor vizate.

În continuare prezentăm câteva dintre situațiile relevante în care au fost contestate sancțiunile aplicate de Autoritatea națională de supraveghere, cu privire la care s-au pronunțat hotărâri definitive de către instanțele judecătorești, prin care s-a acordat câștig de cauză instituției noastre.

a) Hotărâri pronunțate în litigii privind prelucrarea de date cu caracter personal prin mijloace de supraveghere video

1. O curte de apel a respins plângerea contravențională formulată de o primărie împotriva procesului-verbal de constatare/sanționare încheiat de Autoritatea națională de supraveghere, prin care s-a reținut săvârșirea următoarelor contravenții:

- omisiune de notificare, prevăzută de art. 31 din Legea nr. 677/2001,
- prelucrare nelegală de date cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, în legătură cu instalarea și utilizarea unui sistem de supraveghere video în cadrul respectivei primării.

În procesul-verbal de constatare/sanționare s-a reținut că operatorul colecta imaginile angajaților în birouri fără existența unei prevederi legale care să permită o astfel de operațiune și fără a fi solicitat în prealabil avizul instituției noastre, în temeiul prevederilor Deciziei nr. 52/2012.

Mai mult, s-a reținut că prelucrarea nu a fost notificată Autorității naționale de supraveghere, potrivit legii.

Instanța a reținut, prin hotărâre irevocabilă, că s-a încălcat dreptul la viață privată a salariaților.

2. O instanță de fond a respins plângerea contravențională formulată de un operator împotriva procesului-verbal de constatare/sanționare încheiat de Autoritatea națională de supraveghere, prin care s-a reținut săvârșirea următoarelor contravenții:

- omisiune de notificare, prevăzută de art. 31 din Legea nr. 677/2001,
- prelucrare nelegală de date cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, în legătură cu instalarea și utilizarea unui sistem de supraveghere video în cadrul respectivului operator.

În procesul verbal de constatare/sanționare s-a reținut că operatorul avea montat un sistem de supraveghere video compus din 4 camere montate stradal, în interior și pe holurile de la etajul imobilului unde își desfășura activitatea.

De asemenea, s-a reținut că operatorul nu a notificat Autorității naționale de supraveghere, potrivit legii, prelucrarea datelor personale constând în imagini.

Operatorul a săvârșit fapte contravenționale prevăzute de legislația în materie, sancționate de către Autoritatea națională de supraveghere

Instanța a reținut, prin hotărârea pronunțată, existența contravențiilor constatate în sarcina operatorului, astfel că a respins plângerea acestuia.

b) Hotărâre pronunțată într-un litigiu privind transmiterea de mesaje comerciale nesolicitate

O petentă și-a exercitat dreptul de a depune plângere la Autoritatea națională de supraveghere, potrivit art. 25 din Legea nr. 677/2001, reclamând că a primit pe adresa sa de e-mail mesaje comerciale nesolicitate de la o entitate privată și că, în urma exercitării dreptului de opoziție, aceasta nu i-a răspuns.

Autoritatea națională de supraveghere a efectuat o investigație la operatorul reclamat, unde a constatat că aceasta a nesocotit dispozițiile art. 15 din Legea nr. 677/2001 și art. 12 alin. (1) din Legea nr. 506/2004. Prin procesul-verbal de constatare/sanționare încheiat, s-a reținut săvârșirea următoarelor contravenții:

- prelucrarea nelegală a datelor cu caracter personal prevăzută de art. 32 din Legea nr. 677/2001, întrucât operatorul nu a răspuns la cererile petentei de exercitare a dreptului de

opozitie, prin care aceasta a solicitat ștergerea adresei de e-mail din baza de date a operatorului, și nici nu a luat măsuri de încetare a prelucrării acesteia, trimițându-i încă două mesaje comerciale nesolicitate, încălcându-se astfel prevederile art. 15 din Legea nr. 677/2001;

- nerespectarea prevederilor art. 12 referitoare la comunicațiile nesolicitate prevăzută de art. 13 alin. (1) lit. g) din Legea nr. 506/2004, întrucât operatorul a trimis către adresa de e-mail a petentei mai multe comunicări comerciale nesolicitate, fără a avea consimțământul expres prealabil al petentei, încălcând astfel art. 12 alin (1) din Legea nr. 506/2004.

Din verificările efectuate de Autoritatea națională de supraveghere a rezultat că adresa de e-mail a petiționarei nu era ștearsă din baza de date a operatorului investigat, că acesta nu a răspuns la cererile petentei prin care aceasta își exercita dreptul de opoziție și nu a luat măsuri de încetare a prelucrării adresei acesteia de e-mail trimițându-i în continuare alte mesaje.

Mai mult, Autoritatea națională de supraveghere a constatat că operatorul nu a făcut dovada obținerii anterior prelucrării, a consimțământului expres cu privire la prelucrarea e-mailului petentei.

Faptele săvârșite au fost sancționate contravențional cu amendă. Operatorul a contestat în instanță procesul-verbal de constatare sancționare contravențională emis de Autoritatea națională de supraveghere.

Instanța a analizat probatoriul administrat în cauză și a constatat că procesul-verbal de constatare/sancționare este legal întocmit.

Prin hotărârea definitivă pronunțată, instanța a menținut sancțiunile contravenționale aplicate de Autoritatea națională de supraveghere.

c) Hotărâre pronunțată într-un litigiu privind dreptul de opoziție exercitat față de deținătorul unui site web. Aplicarea mutatis mutandis a Cauzei C-131/12 Google Spain SL, Google Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González.

O societate comercială a preluat pe site-ul său, automat, prin intermediul unui program informatic, toate informațiile postate pe portalul just.ro cu privire la dosarele instanțelor de judecată, fiind actualizate la interval de câteva ore, potrivit modificărilor care apar pe acest portal.

Aceste informații sunt stocate într-un sistem de evidență automatizat și puse la dispoziția publicului. Societatea oferă inclusiv abonamente contra cost pentru un serviciu intitulat „Dosarele mele”.

În cadrul unei secțiuni de pe site denumite “Dosare instanță”, pe baza unor criterii cum ar fi numele și prenumele unei persoane fizice, pot fi efectuate căutări directe, în urma cărora rezultă informații privind dosarele instanțelor de judecată în care persoana fizică respectivă este parte. Aceste informații apar și în urma unei căutări pe baza numelui și a prenumelui realizate cu ajutorul motorului de căutare Google, afișându-se un link către pagina web a operatorului, de unde rezultă că informațiile sunt indexate pe acest motor de căutare.

Raportat la dispozițiile Legii nr. 677/2001 și având în vedere activitatea pe care însăși societatea și-a ales să o desfășoare, operațiunile de preluare, înregistrare, organizare, stocare și dezvăluire a datelor din dosarele instanțelor de judecată reprezintă operațiuni de prelucrare a datelor personale, realizate într-un sistem de evidență automatizat.

Prin urmare, această societate are calitatea de operator de date cu caracter personal și, implicit, obligațiile stabilite de lege în sarcina sa, inclusiv sub aspectul legalității prelucrării datelor și al respectării drepturilor persoanelor vizate.

Nu are relevanță modul în care societatea a obținut datele, respectiv din surse publice și că acestea au fost deja publicate pe internet, nefiind absolutivă de obligațiile de a respecta dispozițiile Legii nr. 677/2001, inclusiv cele care garantează persoanei vizate dreptul de opoziție.

În contextul dat, o persoană fizică și-a exercitat dreptul de opoziție și a solicitat operatorului menționat ștergerea datelor sale (numele și prenumele) de pe site, motivându-și cererea prin faptul că este o persoană particulară, având dreptul la intimitate, la confidențialitate și la discreție privind datele sale biografice și nu dorește să se facă publice episoade din viața sa pe site, cu atât mai mult cu cât acestea sunt accesibile atât în România, cât și în afara țării, prin simpla căutare a numelui său pe motoarele de căutare.

Pe lângă faptul că operatorul nu a dat un răspuns persoanei vizate în termenul prevăzut de lege, cererea nu a avut o soluționare favorabilă, societatea motivând că furnizează informații legislative cu un caracter pur informativ, colectate din surse puse la dispoziția publicului de către autoritățile publice. Astfel, a susținut că nu poate să șteargă datele respective întrucât nu

exercită un control asupra datelor cu caracter personal publicate pe paginile web ale altor entități, date pe care însă, le preia și le prelucrează la rândul său.

Motivat de acest refuz, persoana vizată în cauză s-a adresat cu plângere instituției noastre care a considerat că cererea persoanei vizate este întemeiată, iar dreptul de opoziție trebuia respectat de către operator, sens în care acesta trebuia să asigure mijloacele necesare exercitării sale.

Prin procesul-verbal de constatare/sanționare încheiat de Autoritatea națională de supraveghere, cu ocazia investigației efectuate, operatorul menționat a fost sancționat cu amendă.

În cazul de față, între raporturile dintre persoana vizată și operator nu a fost invocată o dispoziție legală care să-l oblige pe acesta la înregistrarea și menținerea datelor personale în contextul furnizării serviciilor sale, respectiv de postare a informațiilor colectate din surse publice pe site-ul său și de punerea la dispoziția publicului sau a celor interesați.

Acest scop nu reprezintă o obligație legală pentru o societate comercială (astfel cum este cazul instanțelor de judecată), care și-a stabilit ea însăși scopul și mijloacele prelucrării datelor.

Din moment ce excepția nu este îndeplinită, persoana vizată a precizat o serie de motive pentru care dorește să-i fie șterse datele, în contextul în care aceasta nu este persoană publică și nu ocupă o funcție publică, datele respective fiind simple informații despre dosarele sale în instanță care nu trebuie să satisfacă interesul preponderent al publicului, s-a considerat că nu se poate refuza solicitarea acesteia pe considerentul că nu a arătat situația sa particulară.

Pe de altă parte, nici operatorul nu a justificat faptul că interesul său legitim (de altfel, unul pur comercial) este mai presus decât dreptul fundamental la viață privată al persoanei vizate, astfel încât acesta să fie îngăduit.

Prin urmare, trebuie stabilit un echilibru între, pe de o parte, drepturile de protecție a datelor aparținând persoanelor vizate și, pe de altă parte, drepturile legitime ale altor părți în cadrul procesului de prelucrare a datelor persoanei vizate.

Raportat la modalitatea de prelucrare a datelor, în sistem automatizat, operatorul trebuia să ia, încă de la crearea sistemului informatic, măsurile necesare astfel încât să poată asigura și din punct de vedere tehnic ștergerea informațiilor privind o persoană fizică, la cererea acesteia de opoziție la prelucrarea datelor sale.

A susține imposibilitatea asigurării drepturilor persoanelor vizate, pe motiv că sistemul de evidență al operatorului nu permite modificări, iar singura soluție pentru rezolvarea acestui tip de problemă este eliminarea respectivelor date de pe portalul instanțelor de judecată, conduce la nerespectarea obligațiilor prevăzute de lege în calitate de operator al societății comerciale și goleşte de conținut dreptul de opoziție garantat de Legea nr. 677/2001.

Art. 5 alin. (2) lit. f) din Legea nr. 677/2001, modificată și completată permite prelucrarea datelor (deci și colectarea acestora) fără consimțământul persoanei vizate, atunci când prelucrarea privește date obținute din documente accesibile publicului, conform legii. Aceste dispoziții, însă, nu înfrâng prevederile art. 12-17 din Legea nr. 677/2001, modificată și completată, care garantează drepturile persoanelor fizice ale căror date sunt prelucrate și nu absolvă operatorul de obligația de a respecta aceste drepturi, ulterior obținerii din surse publice a documentelor care conțin și date personale.

În Hotărârea din 13 mai 2014, în Cauza C-131/12 (<http://curia.europa.eu/juris/documents.jsf?num=C-131/12>), Curtea de Justiție a Uniunii Europene a statuat prevalența dreptului de opoziție asupra dreptului de a avea acces la informație, precum și asupra intereselor economice ale operatorului care furnizează informațiile respective.

Autoritatea națională de supraveghere a considerat faptul că motivarea Curții de Justiție a Uniunii Europene se aplică mutatis mutandis și cazului în speță.

Curtea de apel a statuat că ambele cerințe ale art. 15 din Legea nr. 677/2001 sunt îndeplinite, în sensul că motivele invocate de persoana vizată în sprijinul dreptului de opoziție sunt justificate și nu există dispoziții legale contrare care să permită să fie nesocotit acest drept.

Instanța a admis faptul că motivarea Curții de Justiție din hotărârea mai sus-menționată se poate aplica mutatis mutandis și în situația în care persoana fizică în cauză se adresează în mod direct deținătorului site-ului pe care se află datele sale și care se afișează în urma unei căutări simple realizate cu ajutorul motorului de căutare Google. S-a mai arătat că operatorul nu a luat nici măsura limitării publicității excesive invocând faptul că informațiile oricum sunt publice, apărând pe portalul instanțelor de judecată.

În același timp, instanța a reținut că, a susține că în virtutea principiului publicității ședințelor de judecată, operatorul nu este obligat să șteargă datele personale la cererea persoanelor vizate, ar însemna denaturarea acestui principiu care se manifestă în fața instanței

de judecată, iar nu în spațiul virtual. Mergând pe o asemenea interpretare, ar însemna că orice persoană ar putea înregistra audio ori video ședința de judecată și chiar să o ofere spațiului public virtual pe internet.

Decizia definitivă a instanței este deosebit de importantă, întrucât confirmă punctul de vedere al Autorității naționale de supraveghere în privința motivelor întemeiate și legitime ce pot fi invocate de o persoană vizată în exercitarea cu succes a dreptului de opoziție, cât și al respectării de către deținătorii de site-uri a principiilor prelucrării datelor prevăzute de Legea nr. 677/2001 și cele statuate de Curtea de Justiție a Uniunii Europene în jurisprudența sa în domeniu.

În concluzie, Autoritatea națională de supraveghere atrage atenția asupra faptului că activitatea unei entități, de preluare a unor documente care conțin date cu caracter personal, din surse publice și prelucrarea acestora în sistemele proprii de evidență intră sub incidența legislației privind protecția datelor personale, deoarece odată obținute aceste date, cu respectarea dispozițiilor legale în materie, persoana care le va deține va deveni operator de date cu caracter personal și va avea toate obligațiile stabilite de legislația din domeniul protecției datelor personale.

d) Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal de către o instituție bancară, fără informarea prealabilă a persoanelor vizate și fără exprimarea consimțământului în mod expres și neechivoc pentru această prelucrare

Un petent a semnalat Autorității naționale de supraveghere o posibilă „practică incorectă de business de largă adresabilitate” săvârșită de o instituție financiar-bancară.

Petentul a precizat că, în urma cumpărării on-line a unor bilete la cinema de pe site-ul www.cinemagia.ro, după efectuarea plății, a primit un e-mail prin care i se aducea la cunoștință că i-a fost deschis un cont într-o aplicație aparținând unei instituții financiar-bancare, cu ajutorul căreia va putea face plăți fără a fi în posesia cardului. Petentul a susținut că „această aplicație reține toate datele de pe card cu excepția codului CCV, urmând ca acestea să fie folosite pentru efectuarea de tranzacții”.

Prin sesizarea formulată petentul a precizat că, la momentul efectuării plății, ecranul era unul tipic plăților, condiții în care nu a sesizat existența vreunui text referitor la înrolarea într-un serviciu electronic tip wallet.

Prin procesul-verbal de constatare/sanționare s-a reținut în sarcina instituției financiar-bancare controlate, raportat la calitatea acesteia de operator de date cu caracter personal, săvârșirea contravențiilor prevăzute de art. 31 și art. 32 din Legea nr. 677/2001, constând în:

- omisiunea de notificare și notificarea cu rea credință în forma omisiunii de a efectua notificarea în condițiile art. 22,

- prelucrarea nelegală a datelor cu caracter personal prin încălcarea art. 12 pentru lipsa informării privind prelucrarea datelor personale

- prelucrarea nelegală a datelor cu caracter personal prin încălcarea art. 5 pentru lipsa consimțământului expres și neechivoc al utilizatorului privind prelucrarea datelor personale,

Pentru faptele reținute prin procesul-verbal de constatare/sanționare operatorul a fost sancționat cu două amenzi contravenționale și un avertisment.

S-a reținut că operatorul controlat a implementat în luna iulie 2012 serviciul de plăți de tip Wallet, dar, în contextul prestării acestui serviciu, nu a completat notificarea prelucrărilor de date cu caracter personal deja înscrisă în Registrul de evidență a prelucrărilor cu indicarea prelucrărilor efectuate.

Mai mult, s-a reținut că de la data implementării serviciului de plată on-line pentru cinemagia.ro și activarea implicită a opțiunii plăți rapide, instituția financiar bancară a prelucrat datele cu caracter personal a persoanelor vizate fără informarea acestora și fără exprimarea consimțământului în mod expres și neechivoc pentru această prelucrare.

Procesul-verbal de sancționare a fost contestat în instanță iar, instanța de fond a respins plângerea, reținând, cu privire la prima faptă că reclamanta avea obligația să notifice Autorității naționale de supraveghere în condițiile art 22 din Legea nr. 677/2001, înainte de efectuarea oricărei prelucrări de date cu caracter personal prin serviciul de tip Wallet.

În privința celei de-a doua fapte, respectiv încălcarea art. 32 din Legea nr. 677/2001, instanța de fond a reținut că și aceasta este imputabilă reclamantei, întrucât aceasta a prelucrat date în mod ilegal cu încălcarea art. 12 din legea nr. 677/2001.

Astfel, pentru efectuarea unei plăți cu cardul pentru un bilet cumpărat de pe cinemagia.ro, utilizatorul era direcționat automat pe pagina de internet a instituției financiar-bancare, unde i se prelucrau datele cu caracter personal, însă fără a fi informat în prealabil cu privire la prelucrare, efectuată în fapt de alt operator decât cel deținător al site-ului cinemagia.ro.

Cu privire la cea de-a treia faptă, respectiv încălcarea art. 32 din Legea nr. 677/2001, instanța a reținut că și aceasta a fost individualizată în mod corect în procesul-verbal. S-a reținut că instituția financiar bancară a prelucrat date în mod ilegal prin încălcarea art. 5 din Legea nr. 677/2001 pentru lipsa consimțământului expres și neechivoc al utilizatorului la efectuarea de prelucrări pentru servicii de plăți de tip wallet pay.

Instanța a reținut în hotărârea pronunțată că cerința consimțământului expres și neechivoc nu poate fi considerată ca îndeplinită doar pentru că beneficiarul serviciilor de plăți de tip wallet pay furnizate de instituția financiar bancară, persoană vizată în sensul Legii nr. 677/2001, nu și-a manifestat dezacordul cu privire la prelucrare.

În concluzie, instanța a apreciat că folosirea de date personale pentru crearea de conturi virtuale fără acordul persoanelor respective și fără informarea lor corectă și completă prezintă o gravitate sporită, fiind susceptibilă a aduce atingere dreptului la viață intimă, familială și privată.

Soluția a rămas definitivă prin respingerea apelului.

Decizia definitivă confirmă poziția instituției noastre în privința apărării principiilor prelucrării datelor prevăzute de Legea nr. 677/2001.

În concluzie, Autoritatea națională de supraveghere atrage atenția asupra faptului că activitatea unor instituții financiar-bancare, de prelucrare a unor date cu caracter personal, chiar și în situația în care acestea sunt colectate indirect din alte surse (ex: parteneri contractuali), intră sub incidența legislației privind protecția datelor personale, iar instituția financiar-bancară este ținută, în calitatea sa de operator de date, de respectarea tuturor obligațiilor stabilite de lege în sarcina sa.

e) Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal, sub forma dezvăluirii prin publicare pe Internet

Autoritatea națională de supraveghere a fost sesizată despre publicarea de către o societate comercială în presa locală on-line și pe site-ul propriu a unei liste cu datornici, conținând următoarele date cu caracter personal: nume, prenume, total factură restantă, localitate, stradă, număr facturi restante.

Prin procesul-verbal de constatare/sancționare operatorul controlat a fost sancționat cu amendă pentru săvârșirea contravenției prevăzută de:

- art. 32 din Legea nr. 677/2001, întrucât a prelucrat nelegal date cu caracter personal în sensul că a dezvăluit pe Internet datele unor debitori, fără a face dovada informării prealabile a acestora, fără ca prelucrarea să fie efectuată în baza unor prevederi legale sau alte temeiuri pe care să o justifice;

- art. 34 din Legea nr. 677/2001, pentru refuzul de a furniza Autorității naționale de supraveghere toate informațiile solicitate de aceasta cu ocazia controlului.

Procesul-verbal de sancționare a fost contestat în instanță de operatorul respectiv.

Instanța de fond a respins plângerea, reținând, cu privire la prima faptă că reclamantul a recunoscut săvârșirea contravenției reținută în sarcina sa. De asemenea, a apreciat că reclamantul nu a făcut dovada unei situații de fapt contrare celei reținute în procesul-verbal de contravenție, astfel că prezumția conform căreia situația reținută în procesul-verbal nu corespunde realității nu a fost răsturnată.

În privința individualizării sancțiunilor aplicate, instanța de fond a apreciat că amenzile aplicate corespund gradului de pericol social al faptelor, nefiind motive pentru înlocuirea sancțiunii amenzii cu ce a avertismentului.

Sentința a rămas definitivă, ceea ce dovedește corectitudinea abordării instituției noastre în privința aplicării principiilor prelucrării datelor prevăzute de Legea nr. 677/2001.

f) Hotărâri prin care s-a constatat încălcarea drepturilor persoanelor vizate

1. Prin decizie irevocabilă, o curte de apel a respins plângerea contravențională formulată de o instituție publică centrală împotriva procesului-verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere, prin care s-a constatat încălcarea dreptului de intervenție al unui magistrat în raporturile acestuia cu respectiva instituție.

Autoritatea națională de supraveghere a reținut nerespectarea prevederilor art. 14 alin. (3) din Legea nr. 677/2001, respectiv a dreptului de intervenție asupra datelor al magistratului respectiv, întrucât instituția publică centrală nu a răspuns, în termenul legal de 15 zile, cererii acestuia de ștergere a datelor sale personale (referiri la trăsături de personalitate și comportament) dintr-un raport, postat pe site-ul respectivei instituții, în condițiile în care dezvăluirea publică a respectivului raport a adus atingere vieții private a persoanei respective.

Prin decizia pronunțată, instanța de apel a menținut sancțiunea aplicată de Autoritatea națională de supraveghere.

Hotărârea a rămas definitivă.

2. O altă curte de apel a respins plângerea contravențională formulată de un serviciu deconcentrat al unui minister împotriva procesului-verbal de constatare/sanționare al Autorității naționale de supraveghere, prin care s-a reținut săvârșirea următoarelor fapte contravenționale:

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, întrucât au fost dezvăluite date cu caracter personal ale unui petent fără acordul acestuia, cu încălcarea prevederilor art. 5 alin. (1) din Legea nr. 677/2001,

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, ca urmare a nerespectării dreptului de intervenție prevăzut de art. 14 din Legea nr. 677/2001, întrucât nu s-a transmis un răspuns petentului în termenul legal de 15 zile.

Prin decizia definitivă pronunțată, instanța a menținut sancțiunile aplicate de Autoritatea națională de supraveghere.

Secțiunea a 5-a Informare publică

În cursul anului 2014, Autoritatea națională de supraveghere a intensificat activitățile și modalitățile de comunicare destinate informării publicului larg cu privire la regulile specifice de prelucrare a datelor cu caracter personal.

Astfel, pe lângă organizarea de evenimente specifice – Ziua Europeană a Protecției Datelor, reuniuni de informare la nivelul autorităților publice locale și serviciilor publice deconcentrate județene, un rol semnificativ l-a avut difuzarea unui clip de informare privind datele personale pe posturile de televiziune, în mijloacele de transport în comun și pe anumite rețele de televiziune cu circuit închis amplasate în locuri accesibile publicului larg.

De asemenea, instituția noastră a participat activ la cele mai importante evenimente la care a fost invitată.

Dintre evenimentele semnificative în care instituția noastră a fost implicată, evidențiem:

- Ziua Europeană a Protecției Datelor

Pe data de 28 ianuarie 2014 s-a marcat aniversarea a 33 de ani de la semnarea, la Strasbourg, în anul 1981, a Convenției 108 pentru protecția persoanelor referitor la prelucrarea

automatizată a datelor cu caracter personal, primul instrument legal adoptat în domeniul protecției datelor.

Scopul celebrării acestei zile este conștientizarea persoanele fizice de pe întreg cuprinsul Europei asupra importanței protecției datelor cu caracter personal și a drepturilor specifice pe care le pot exercita. Cu această ocazie, autoritățile naționale independente de protecția datelor din statele europene organizează evenimente specifice.

În cinstea Zilei Europene a Protecției Datelor, Autoritatea națională de supraveghere a organizat, la Palatul Parlamentului, Simpozionul cu tema „Protecția datelor personale - prezent și viitor”, care s-a bucurat de participarea prestigioasă a unor înalți oficiali și reprezentanți ai mediului academic, justiției și ai organizațiilor nonguvernamentale. Președintele Camerei Deputaților, dl. Valeriu Zgonea, și vicepreședintele Senatului, domnul Cristian Dumitrescu, au onorat cu prezența acest eveniment și și-au exprimat interesul pentru acest domeniu de impact la nivel european.

- Reuniune cu tema „Cloud Computing: provocări și oportunități din perspectiva protecției datelor”

Reprezentanții Autorității naționale de supraveghere împreună cu cei ai unor societăți ce activează în domeniul furnizării de servicii cloud au participat la evenimentul cu tema „Cloud Computing: provocări și oportunități din perspectiva protecției datelor”.

În cadrul acestei reuniuni a fost prezentat cadrul legal al prelucrărilor de date cu caracter personal în cloud computing și s-au discutat aspecte privind legislația aplicabilă în cazul transferurilor internaționale de date în cloud, relațiile dintre clienții serviciilor de cloud computing (operatori de date), furnizorii de astfel de servicii (împuterniciți) și sub-contractanții acestora, precum și cu privire la drepturile persoanelor vizate ale căror date sunt prelucrate de clienții serviciilor cloud.

Un alt subiect abordat a fost cel al soluțiilor tehnice și standardelor de securitate necesare în vederea asigurării securității și confidențialității datelor cu caracter personal.

Printre **alte manifestări** în cadrul cărora instituția noastră a susținut prezentări menționăm:

- Conferința „Marketing Online –Promovare pe internet”
- Ziua Mondială a Drepturilor Consumatorilor
- Conferința și Adunarea Generală a Asociației Aeroporturilor din România

- Dezbateră organizată de Biroul de Informare al Parlamentului European în România, în colaborare cu Institutul European din România și Centrul de Informare Europe Direct București, în vederea creării cadrului oportun discuțiilor asupra domeniilor ce definesc "Calitatea vieții" cetățenilor europeni, printre care și cel al protecției datelor cu caracter personal.

Pe de altă parte, în anul 2014, Autoritatea națională de supraveghere a demarat și o **campanie de informare, la nivel național, în sectorul public.**

Cu sprijinul Instituției Prefectului din județele Dâmbovița, Prahova și Argeș au avut loc mai multe reuniuni cu tema "Protecția datelor personale în administrația publică locală", în scopul creșterii gradului de informare a reprezentanților autorităților publice cu privire la regulile aplicabile prelucrării datelor cu caracter personal.

La aceste manifestări organizate la Târgoviște, Ploiești și Pitești au fost invitați reprezentanți ai administrației publice locale și ai serviciilor publice deconcentrate de la nivel județean.

Prin organizarea acestor evenimente Autoritatea națională de supraveghere a urmărit îmbunătățirea aplicării unitare a regulilor de prelucrare a datelor cu caracter personal, a gradului de informare publică privind asigurarea protecției datelor cu caracter personal, obligațiile ce revin operatorilor de date din sectorul public și drepturile de care beneficiază persoanele fizice.

Autoritatea națională de supraveghere a comunicat că, deși autoritățile publice locale și cele de la nivel județean sunt scutite de obligația de notificare, pentru prelucrările prevăzute de lege în sarcina acestora (raportat la obiectul de activitate), conform Deciziei nr. 23/2012, acestea trebuie să notifice prelucrările efectuate prin utilizarea sistemelor de supraveghere video, în concordanță cu prevederile Legii nr. 677/2001 și ale art. 14 din Decizia nr. 52/2012.

Însă, în ambele situații, se menține în sarcina autorităților publice locale și a celor de la nivel județean obligația respectării condițiilor de prelucrare a datelor personale, prevăzute de Legea nr. 677/2001, inclusiv cele referitoare la exercitarea drepturilor persoanelor vizate (dreptul de informare, acces, intervenție, opoziție, de plângere la Autoritate).

În același timp, prin **informațiile furnizate telefonic și în cadrul audiențelor** acordate la sediul Autorității naționale de supraveghere, s-a realizat informarea rapidă și eficientă a cetățenilor și a operatorilor, în sensul că au fost oferite, într-o manieră directă,

informații utile cu privire la drepturile persoanelor vizate și obligațiile specifice operatorilor, lămuriri cu privire la condițiile prelucrării datelor și dezvăluirii acestora către terți.

Prin intermediul site-ului propriu **www.dataprotection.ro**, instituția noastră a urmărit asigurarea unei informări adecvate a persoanelor fizice, cât și a operatorilor care ni se pot adresa, utilizând inclusiv adresa de poștă electronică: anspdc@dataprotection.ro.

În scopul popularizării activității instituției și a reglementărilor specifice în materie, au fost publicate, pe site-ul www.dataprotection.ro, comunicate de presă prin care au fost prezentate aspecte semnificative din activitatea de control sau din alte manifestări în care a fost implicată Autoritatea națională de supraveghere.

Comunicatele de presă sau răspunsurile la solicitările primite din partea mass-mediei s-au concretizat în mai multe articole publicate, care au adus în atenția publicului larg punctul de vedere al instituției noastre în ceea ce privește condițiile de dezvăluire a datelor personale, drepturile de care beneficiază cetățenii în acest domeniu, posibilitățile de valorificare a acestora și rolul Autorității naționale de supraveghere.

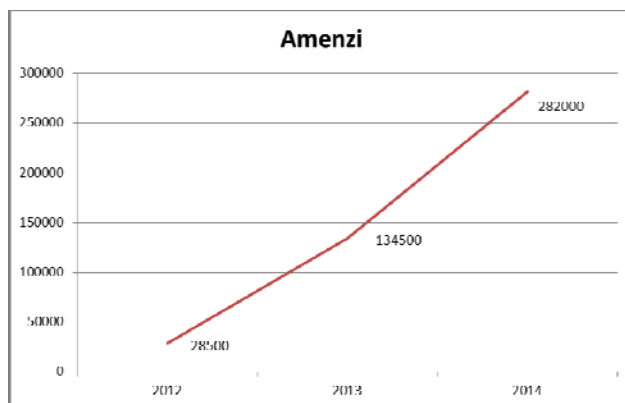
Interesul manifestat de **mass-media** față de domeniul protecției datelor cu caracter personal s-a reflectat în articolele de presă publicate și reportajele difuzate.

CAPITOLUL AL IV-LEA ACTIVITATEA DE CONTROL

Secțiunea 1: Prezentare generală

Verificarea respectării condițiilor de prelucrare a datelor personale prin intensificarea investigațiilor în sectorul public și privat, la nivelul activității desfășurate pentru soluționarea plângerilor și sesizărilor primite, dar și prin investigații din oficiu, în scopul asigurării aplicării principiilor de protecție a datelor de către operatori, este unul din principalele obiective ale instituției noastre. În acest sens, subliniem numărul semnificativ de investigații efectuate în anul 2014, față de anii precedenți, ceea ce a condus la un quantum al amenzilor considerabil crescut.

Astfel, quantumul total al amenzilor aplicate în 2014 în investigațiile din oficiu efectuate și al celor pentru soluționarea plângerilor și sesizărilor primite, este de 282.000 lei. Remarcăm o creștere cu 110% a quantumului amenzilor comparativ cu anul 2013.



Menționăm că în cursul anului 2014 au fost realizate 449 de investigații, din care 364 de acțiuni de control pe teren și 85 de investigații în scris. În același timp, se constată o creștere cu 96% a investigațiilor comparativ cu anul 2013.

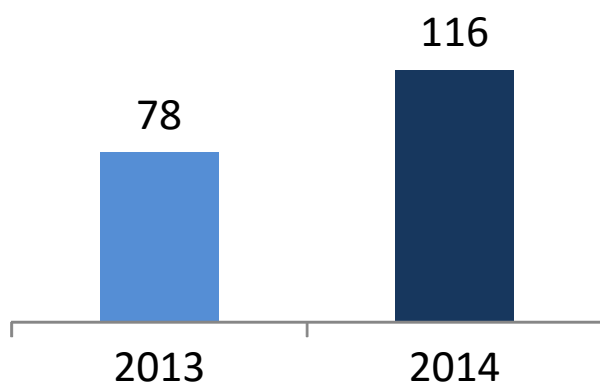


Pentru o descriere mai amplă, vom prezenta în continuare situația activităților de control efectuate și fișe de caz ale celor mai relevante investigații.

Secțiunea a 2-a: Investigații din oficiu

Activitatea de monitorizare și control desfășurată de Autoritatea națională de supraveghere are ca scop asigurarea aplicării și respectării prevederilor legislației existente în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal, precum și protejarea drepturilor și intereselor persoanelor vizate.

În cursul anului 2014, a fost efectuat un număr total de 116 acțiuni de control din oficiu, pe teren.



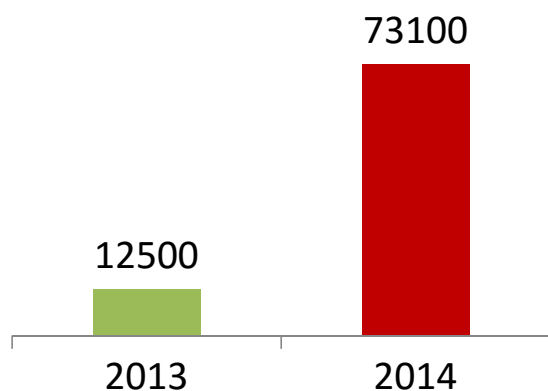
Raportat la anul 2013, investigațiile din oficiu au crescut cu un procent de aproximativ 50% (48,71%) în anul 2014.

Fig. I. Investigații din oficiu 2013 - 2014

Această creștere a investigațiilor din oficiu se datorează extinderii verificării prelucrărilor de date în mai multe domenii de activitate, abordării unui număr mai mare de obiective principale și a monitorizării adecvate a semnalărilor din mass-media.

Ca urmare a investigațiilor din oficiu efectuate, au fost aplicate sancțiuni contravenționale constând în amenzi (29) și avertismente (20).

Cuantumul total al amenzilor aplicate a fost de 73.100 lei (RON).



Comparativ cu anul 2013, cuantumul amenzilor aplicate în anul 2014 este de aproximativ 6 ori mai mare. Acest lucru se datorează și numărului mai mare de investigații din oficiu efectuate în 2014.

Fig. II. Cuantum amenzi 2013 - 2014

În activitatea de verificare a respectării dispozițiilor legale desfășurată pe parcursul anului 2014, Autoritatea națională de supraveghere a avut drept obiective principale:

- verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către misiunile diplomatice sau de către oficiile consulare ale României;
- verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către autoritățile publice;
- verificarea condițiilor care trebuie respectate în cazul prelucrării datelor privind starea de sănătate de către centrele medicale și unitățile spitalicești;
- verificarea condițiilor de prelucrare a datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video de către unitățile de învățământ;
- verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către societățile de transport public urban;

Totodată, s-a continuat investigarea modalității de prelucrare a datelor cu caracter personal de către entitățile care desfășoară activități de schimb valutar, inclusiv sub aspectul respectării prevederilor Deciziei nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

Alte investigații din oficiu s-au efectuat ca urmare a notificărilor transmise de către operatorii de date cu caracter personal, precum și ca urmare a unor articole apărute în presă, în ceea ce privește:

1. prelucrarea codului numeric personal și a altor date de identificare de aplicabilitatea generală, respectarea prevederilor Deciziei nr. 132/2011;
2. transferul de date cu caracter personal în baza unor contracte cu clauze standard;
3. dezvăluirea în presă a datelor cu caracter personal (număr de telefon) ale unor persoane cu statut de persoane publice;
4. dezvăluirea datelor cu caracter personal ale propriilor angajați pe website-ul unei societăți;
5. stabilirea calității de operator sau împuternicit a unor societăți care prelucrau și transferau date cu caracter personal în străinătate;

I. Respectarea prevederilor Legii nr. 677/2001 în cadrul activităților desfășurate de misiunile diplomatice sau de oficiile consulare ale României

În anul 2014, Autoritatea națională de supraveghere a decis efectuarea unor investigații din oficiu la misiunile diplomatice și oficiile consulare ale României pentru verificarea condițiilor de respectare a prevederilor Legii nr. 677/2001, inclusiv în ceea ce privește respectarea drepturilor persoanelor vizate și al măsurilor de securitate.

În cadrul acestor investigații, Autoritatea națională de supraveghere a avut în vedere și verificarea respectării condițiilor de prelucrare a datelor cu caracter personal cuprinse în Sistemul Național de Informații privind Vizele (SNIV), conform Legii nr. 271/2010 pentru înființarea, organizarea și funcționarea Sistemului național de informații privind vizele și participarea României la Sistemul de informații privind vizele și Regulamentului (CE) nr. 810/2009 privind instituirea unui Cod comunitar de vize.

Verificările efectuate au vizat, în principal, următoarele aspecte: notificarea datelor cu caracter personal la Autoritatea națională de supraveghere, realizarea informării persoanelor vizate potrivit art. 12 din Legea nr. 677/2001, scopul și calitatea datelor cu caracter personal prelucrate, respectarea măsurilor minime de securitate a prelucrărilor de date cu caracter personal, arhivarea datelor. De asemenea, s-au efectuat verificări și cu privire la realizarea

accesului în incinta oficiului consular, organizarea secțiilor de vize, prelucrarea cererilor de viză, respectarea măsurilor de securitate cu privire la accesul în Sistemul național de informații privind vizele și respectarea drepturilor persoanelor vizate.

Ca urmare a investigațiilor efectuate, s-a constatat că prelucrările de date cu caracter personal efectuate de către misiunile diplomatice și oficiile consulare ale României sunt notificate la Autoritatea națională de supraveghere de către Ministerul Afacerilor Externe.

În ceea ce privește metodologia de lucru pentru aplicarea Legii nr. 677/2001, aceasta a fost stabilită de către Ministerul Afacerilor Externe, care transmite misiunilor diplomatice și oficiilor consulare ale României, instrucțiuni periodice și manuale care cuprind proceduri referitoare la modul de utilizare a aplicațiilor informatice utilizate, măsurile minime de securitate potrivit Ordinului nr. 52/2002 privind cerințele minime de securitate. Instruirea personalului cu atribuții de prelucrare a datelor cu caracter personal se realizează de către Ministerul Afacerilor Externe, înainte de plecarea la post.

Informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, se realizează pe site-ul www.mae.ro și pe site-urile misiunilor diplomatice ale României, la avizierele misiunilor diplomatice, precum și prin intermediul formularelor utilizate pentru colectarea datelor cu caracter personal.

Cu privire la remedierea deficiențelor constatate, Autoritatea națională de supraveghere a efectuat recomandări privind realizarea adecvată a informării persoanelor vizate, potrivit art. 12 din Legea nr. 677/2001, în toate cazurile în care se prelucrează date cu caracter personal, organizarea adecvată a spațiilor în care sunt arhivate date cu caracter personal, instruirea periodică a personalului cu atribuții privind prelucrarea datelor cu caracter personal, precum și stabilirea și respectarea unei perioade limitate de stocare a acestora, care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate și ulterior prelucrate. Totodată, s-au efectuat recomandări privind securizarea accesului în secțiile consulare, spațiul de lucru cu publicul, conform cerințelor stabilite de Legea nr. 271/2010 pentru înființarea, organizarea și funcționarea Sistemului național de informații privind vizele și participarea României la Sistemul de informații privind vizele, precum și celor ale Regulamentului (CE) nr. 810/2009 privind instituirea unui Cod comunitar de vize.

Având în vedere complexitatea prelucrărilor de date cu caracter personal efectuate în cadrul activităților desfășurate de către misiunile diplomatice și oficiile consulare ale României, se intenționează continuarea acestora și în cursul anului următor.

FIȘĂ DE CAZ

În cadrul unei investigații efectuate la un oficiu consular al României, s-a constatat că acesta prelucra date cu caracter personal ale cetățenilor români care solicitau acordarea anumitor servicii consulare, precum întocmirea de acte notariale, stare civila și eliberarea de pașapoarte temporare și titluri de călătorie, corespunzătoare prelucrărilor notificate la Autoritatea națională de supraveghere de către Ministerul Afacerilor Externe.

Ca urmare a verificărilor efectuate, s-a constatat că în arhiva de la sediul oficiului consular se regăseau documente conținând date cu caracter personal ale cetățenilor români care au solicitat diverse servicii consulare (cerere pentru efectuarea de servicii consulare însoțită de documente justificative, copii ale actelor de identitate, declarații pe proprie răspundere în funcție de serviciul consular solicitat), datând de la înființarea oficiului consular, deși, potrivit art. 4 alin. (1) lit. e) din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata realizării scopurilor în care datele sunt colectate și ulterior prelucrate.

De asemenea, s-a constatat că la sediul oficiului consular era instalat un sistem de supraveghere video, însă nu exista nicio informare cu privire la efectuarea de astfel de operațiuni, deși imaginea este o dată cu caracter personal, iar prelucrările efectuate prin sistemul de supraveghere video intră sub incidența Legii nr. 677/2001.

Operatorul a fost sancționat contravențional, pentru săvârșirea faptei prevăzute de art. 32 din Legea nr. 677/2001, respectiv prelucrarea nelegală a datelor cu caracter personal, prin încălcarea art. 4 și art. 12 din aceeași lege, întrucât operatorul a stocat date cu caracter personal pe o perioadă nelimitată de timp, nefiind stabilită o perioadă de stocare care să permită identificarea persoanelor vizate strict pe durata realizării scopurilor în care datele sunt colectate și ulterior prelucrate și nu a informat persoanele vizate cu privire la prelucrarea datelor cu caracter personal prin intermediul sistemului de supraveghere video.

Totodată, s-a recomandat operatorului stabilirea unei perioade limitate de stocare pentru datele cu caracter personal prelucrate, care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate și ulterior prelucrate, realizarea instruirii personalului oficiului consular care are atribuții în ceea ce privește prelucrarea datelor cu caracter personal, conform Legii nr. 677/2001 și realizarea informării persoanelor vizate potrivit Legii nr. 677/2001 și prin afișare la locul unde se lucrează cu publicul în limba română, și, pe cât este posibil, în altă limbă vorbită în mod curent de solicitanți.

II. Respectarea prevederilor Legii nr. 677/2001 de către autoritățile publice

Entitățile supuse controlului au fost ministere, autorități și instituții publice centrale.

Ca urmare a controalelor desfășurate, s-a constatat că acestea prelucrează date cu caracter personal în baza actelor normative care le reglementează activitatea. Totodată, aceste entități prelucrează date cu caracter personal și în alte scopuri decât cele pentru îndeplinirea obligațiilor legale, de ex: monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private.

Potrivit Deciziei nr. 23/2012 a Președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, notificarea prelucrării datelor cu caracter personal nu este necesară când prelucrarea datelor cu caracter personal este efectuată de autoritățile administrației publice locale, precum și de autoritățile administrației publice de la nivel județean și al municipiului București, în scopul îndeplinirii atribuțiilor lor legale.

Cu toate acestea, excepțiile de la obligația de a notifica nu exonerează operatorul de îndeplinirea celorlalte obligații care îi revin potrivit dispozițiilor legale aplicabile în domeniul protecției datelor cu caracter personal (informarea persoanelor vizate, confidențialitatea și securitatea prelucrărilor, etc.).

În urma controalelor efectuate, principalele deficiențe constatate sunt următoarele: nerespectarea obligației privind informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, omisiunea de a notifica prelucrările efectuate în alte scopuri decât cele pentru

îndeplinirea obligațiilor legale, de ex. monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor pblice/private.

FIȘĂ DE CAZ

În cadrul unei investigații efectuate la o instituție publică din domeniul administrării sistemului public de pensii și sistemului de asigurări sociale, s-a constatat că aceasta prelucra date cu caracter personal în mai multe scopuri prevăzute de legile care îi reglementau activitatea. Datele cu caracter personal ale persoanelor vizate erau colectate prin intermediul formularelor de cerere privind acordarea pensiilor și altor prestații de asigurări sociale, precum și pe website-ul instituției.

La data efectuării investigației, s-a constatat că instituția publică investigată nu realiza informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, în nicio modalitate prevăzută de dispozițiile legale, deși în formularul de notificare depus la Autoritatea națională de supraveghere declarase că realizează această informare în scris, verbal, prin afișare la sediu și pe website-ul propriu.

Operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzută de art. 32 din Legea nr. 677/2001, respectiv prelucrarea nelegală a datelor cu caracter personal, prin încălcarea art. 12 din aceeași lege, întrucât operatorul nu a realizat informarea persoanelor vizate.

FIȘĂ DE CAZ

În urma efectuării unui control la o autoritate publică centrală, s-a constatat că aceasta nu a notificat la Autoritatea națională de supraveghere toate scopurile în care prelucra date cu caracter personal și nu realiza informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, deși în formularul de notificare menționase că realizează această informare.

De asemenea, deși autoritatea publică prelucra date cu caracter personal prin intermediul unor persoane împuternicite, nu le-a declarat în formularul de notificare, nu a inclus în contractele încheiate cu acestea clauzele obligatorii prevăzute de art. 20 din Legea nr. 677/2001 și nu a elaborat instrucțiuni pentru persoanele împuternicite care prelucrau date pe seama sa.

Față de cele de mai sus, autoritatea publică a fost sancționată contravențional, pentru săvârșirea contravenției prevăzută de art. 31 din Legea nr. 677/2001, omisiunea de a notifica și notificarea cu rea – credință, respectiv pentru prelucrare nelegală a datelor cu caracter personal - contravenția prevăzută de art. 32 din Legea nr. 677/2001, și pentru neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, contravenție prevăzută de art. 33 din Legea nr. 677/2001

FIȘĂ DE CAZ

O altă autoritate publică a fost sancționată pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, deoarece aceasta solicita și reținea copii de pe actele de identitate ale persoanelor vizate, cu încălcarea prevederilor art. 8 din Legea nr. 677/2001 și art. 2 și art. 6 din Decizia Autorității naționale de supraveghere nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

Totodată, operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzute de art. 33 din Legea nr. 677/2001, neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, deoarece acesta nu a stabilit măsuri cu privire la securitatea și păstrarea confidențialității datelor cu caracter personal.

FIȘĂ DE CAZ

În urma unei investigații desfășurate la un minister, în vederea verificării respectării prevederilor Legii nr. 677/2001, acesta a fost sancționat pentru săvârșirea contravenției prevăzută de art. 31 din Legea nr. 677/2001, sub forma omisiunii de a efectua notificarea prelucrărilor de date în condițiile art. 22 din aceeași reglementare, deoarece acesta nu a notificat la Autoritatea națională de supraveghere toate scopurile în care prelucra date cu caracter personal.

De asemenea, ministerul a fost sancționat contravențional pentru săvârșirea contravenției prevăzută de art. 32 - prelucrare nelegală a datelor cu caracter personal, deoarece nu realiza informarea persoanelor vizate, în concordanță cu art. 12 din Legea nr. 677/2001.

III. Verificarea condițiilor care trebuie respectate în cazul prelucrării datelor cu caracter personal privind starea de sănătate

Investigațiile desfășurate în anul 2014 la centrele de sănătate și unitățile sanitare au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 și a Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Entitățile supuse controlului au fost clinici medicale private din municipiul București, dar și unități sanitare din domeniul public.

Potrivit art. 1 lit. a) din Deciziei nr. 23/2012, notificarea Autorității naționale de supraveghere nu mai este necesară când prelucrarea datelor cu caracter personal este efectuată de persoanele fizice sau entitățile private care desfășoară o activitate independentă, autorizată în baza unei legi speciale, în scopul îndeplinirii atribuțiilor lor legale. Cu toate acestea, excepțiile de la obligația de a notifica nu exonerează operatorul de îndeplinirea celorlalte obligații care îi revin potrivit dispozițiilor legale aplicabile în domeniul protecției datelor cu caracter personal (informarea persoanelor vizate, confidențialitatea și securitatea prelucrărilor, etc.).

În urma controalelor efectuate s-a constatat că entitățile supuse controlului prelucrează date cu caracter personal numai în calitate de operatori. Acestea prelucrează date cu caracter personal în următoarele scopuri: îndeplinirea obligațiilor ce le revin în vederea oferirii serviciilor de sănătate (analize medicale, investigații medicale, activitățile de asistență medicală specializată, generală, spitalicească, stomatologică etc), reclamă, marketing și publicitate (carduri de fidelitate, transmitere newslettere), monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private.

Ca urmare a controalelor efectuate, s-a constatat că operatorii investigați nu au declarat la Autoritatea națională de supraveghere scopurile în care prelucrează date cu caracter personal și care nu se încadrau în cazurile de scutire de la notificare, prevăzute de Decizia nr. 23/2012, de ex. monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private, respectiv reclamă, marketing și publicitate. De asemenea, s-a constatat că aceștia nu realizau informarea persoanelor vizate, potrivit art. 12 din Legea nr. 677/2001.

Față de cele de mai sus, s-au aplicat sancțiuni contravenționale operatorilor investigați pentru săvârșirea faptei de omisiune de a notifica și notificarea cu rea-credință, pentru prelucrarea nelegală a datelor cu caracter personal, cu nesocotirea dreptului la informare prevăzut de art. 12 din Legea nr. 677/2001, precum și pentru nerespectarea prevederilor art. 12 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

De asemenea, au fost emise o serie de recomandări cu privire la următoarele aspecte: actualizarea formularului de notificare ca urmare a modificărilor intervenite în activitatea operatorului și a recomandărilor Autorității naționale de supraveghere, transmise cu ocazia depunerii formularului de notificare, notificarea prelucrării datelor cu caracter personal pentru scopul reclamă, marketing și publicitate, inclusiv transferul datelor în străinătate, monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private, informarea persoanelor vizate, conform art 12 din Legea nr. 677/2001, întocmirea unei proceduri de securitate a datelor cu caracter personale prelucrate potrivit Ordinului nr. 52/2002, stabilirea unei perioade de stocare a datelor colectate strict pe durata necesară realizării scopului.

FIȘĂ DE CAZ

Ca urmare a unei investigații la un operator de date cu caracter personal care are ca obiect principal de activitate asistență medicală generală, s-a constatat că acesta oferea clienților, persoane fizice, carduri de fidelitate pentru acordarea serviciilor de asistență medicală. Clienții aveau posibilitatea de a se înscrie pe site-ul operatorului în vederea transmiterii de newsletter, prin completarea unui formular electronic care conținea date cu caracter personal.

Totodată, s-a constatat că operatorul deținea un sistem de supraveghere video, instalat în scopul monitorizării/securității persoanelor, spațiilor și/sau bunurilor publice/private, prin utilizarea sistemului de supraveghere video.

Față de cele de mai sus, s-a constatat că operatorul controlat nu a notificat la Autoritatea națională de supraveghere prelucrarea datelor cu caracter personal în scop de reclamă, marketing și publicitate și nici în scop de monitorizare/securitate a persoanelor, spațiilor și/sau bunurilor publice/private, prin utilizarea sistemului de supraveghere video.

De asemenea, în urma verificărilor efectuate a reieșit că acesta nu realiza informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, în nicio modalitate prevăzută de lege, precum și faptul că a efectuat comunicări comerciale prin poșta electronică pentru oferirea de pachete medicale promoționale pacienților, fără consimțământul prealabil și expres al acestora și fără a le oferi posibilitatea de a se opune printr-un mijloc simplu și gratuit unei asemenea utilizări, la momentul obținerii adresei de poștă electronică.

IV. Verificarea condițiilor de prelucrare a datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video de către unitățile de învățământ

Investigațiile desfășurate în anul 2014 la unități de învățământ de stat și private care au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 și a Legii nr. 506/2004.

În urma controalelor efectuate s-a constatat că entitățile supuse controlului prelucrează date cu caracter personal, atât în calitate de operatori pentru scopurile educație și cultură (gestionarea bazei de date a cursanților, catalog on-line) și pentru monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private, dar și în calitate de împuterniciți ai inspectoratului școlar, în ceea ce privește monitorizarea prin intermediul camerelor de supraveghere video desfășurată pe perioada examenelor naționale.

Față de cele de mai sus, în unele cazuri, s-a constatat că monitorizarea prin intermediul camerelor de supraveghere video a elevilor și profesorilor se realizează permanent, astfel că unitățile școlare au calitatea de operatori în ceea ce privește prelucrarea datelor cu caracter personal, respectiv imaginea profesorilor și elevilor.

S-a considerat că, în această situație, unitățile școlare au prelucrat în mod excesiv raportat la scopul prelucrării (monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private), datele personale (imaginea) profesorilor și elevilor prin mijloace de supraveghere video în săli de clasă/laboratoare (locul în care se desfășoară activitatea de învățământ), fără a exista o situație expres prevăzută de lege și fără a avea avizul Autorității naționale de supraveghere, așa cum prevede art. 8 alin. (3) din Decizia nr. 52/2012. Ca atare, s-au aplicat sancțiuni contravenționale pentru încălcarea prevederilor din Legea nr. 677/2001.

Totodată, în urma controalelor efectuate a reieșit că operatorii investigați nu au declarat la Autoritatea națională de supraveghere prelucrările date cu caracter personal efectuate în scop de educație și cultură (gestionarea bazei de date a cursanților, catalog on-line) și de monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private.

FIȘĂ DE CAZ

Ca urmare a unei investigații la un operator de date cu caracter personal din domeniul învățământului, s-a constatat că acesta nu a notificat la Autoritatea națională de supraveghere prelucrarea datelor cu caracter personal pe care o realiza, respectiv gestionarea bazei de date a cursanților, catalog on-line și monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private. De asemenea, operatorul respectiv nu realiza informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001.

De asemenea, s-a considerat că unitatea școlară la care s-a desfășurat controlul prelucrării în mod excesiv raportat la scopul prelucrării, datele personale (imaginea) ale profesorilor și elevilor prin mijloace de supraveghere video în sălile de clasă și laboratoare (locul în care se desfășoară activitatea de învățământ), fără a exista o situație expres prevăzută de lege și fără a avea avizul Autorității naționale de supraveghere, așa cum prevede art. 8 alin. (3) din Decizia nr. 52/2012.

Față de cele de mai sus, operatorul a fost sancționat pentru săvârșirea contravenției de omisiune de a notifica și notificarea cu rea-credință, prevăzută de art. 31 din Legea nr. 677/2001, și pentru săvârșirea contravenției de prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din aceeași lege, prin încălcarea art. 12 și art. 4 alin. (1) lit. c) din Legea nr. 677/2001.

V. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către societățile de transport public urban

Autoritatea națională de supraveghere a inclus în planul tematic de investigații și verificarea respectării prevederilor Legii nr. 677/2001 de către societățile din domeniul transporturilor de călători. Astfel, s-au efectuat controale la societățile care asigură transportul local și interurban, atât din București, cât și din țară.

Aceste societăți emit abonamente și legitimații de călătorie persoanelor fizice, care conțin date cu caracter personal, respectiv nume, prenume, seria și numărul CI/BI, CNP-ul (cazuri izolate), numere ale legitimațiilor de veterani de război sau a deținuților politici, număr pașaport. Abonamentele și legitimațiile se emit în regim normal și special (pentru persoanele cu dizabilități, pensionari, elevi/studenti și alte persoane fizice).

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a efectuat o investigație la o societate de transport călători pentru a verifica modul de respectare și aplicare a prevederilor Legii nr. 677/2001, în ceea ce privește prelucrarea datelor cu caracter personal în desfășurarea activității de transport.

Operatorul investigat prelucra date cu caracter personal în scopul emiterii de abonamente și legitimații de călătorie. În acest scop operatorul colecta următoarele date cu caracter personal: numele, prenumele, seria și numărul cărții de identitate, fără a se efectua sau reține copie după CI/BI. Aceste date erau colectate la punctele de eliberare a legitimațiilor/abonamentelor de călătorie.

În situația legitimațiilor de călătorie gratuite sau cu tarif redus, emise în temeiul HCL nr. 261/2012, HG nr. 1364/2006, Legii nr. 118/1990, Legii nr. 44/1999, Legii nr. 189/2000, operatorul reținea copii ale CI/BI, precum și copii ale altor documente doveditoare a calității solicitantului, care îi confereau dreptul la o astfel de legitimație, deși aceste acte normative nu stabilesc reținerea copiilor actelor de identitate și nici posibilitatea de colectare a CNP-ului.

Operatorul a fost sancționat pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, deoarece aceasta solicita și reținea copii de pe actele de identitate ale persoanelor vizate, cu încălcarea prevederilor art. 8 din Legea nr. 677/2001 și art. 2 și art. 6 din Decizia nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

VI. Respectarea prevederilor Deciziei nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, de către entitățile care desfășoară activități de schimb valutar

Entitățile care desfășoară activități de schimb valutar prelucrează datele cu caracter personal ale persoanelor fizice în scopul desfășurării de tranzacții financiare. În acest scop sunt prelucrate următoarele date cu caracter personal: numele, prenumele, seria și numărul BI/CI, semnătura.

În momentul prezentării la ghișeul unde se desfășoară tranzacțiile financiare, clienților li se solicită un act de identitate, datele cu caracter personal fiind colectate prin intermediul formularului de acceptare a tranzacției, semnat de către persoanele vizate, și pe bonul fiscal. Datele cu caracter personal colectate sunt înregistrate și într-un sistem de evidență electronic. Ulterior completării formularului de acceptare a tranzacției, actul de identitate este returnat persoanei vizate, fără a se reține copii ale acestor documente.

Formularul de acceptare a tranzacției este un formular tipizat aprobat prin Ordinul nr. 632/2009 privind unele măsuri de informare a consumatorilor de către operatorii economici care desfășoară activități de schimb valutar, emis de președintele Autorității Naționale pentru Protecția Consumatorilor.

Principalele deficiențe constatate cu ocazia investigațiilor la entitățile care desfășoară activități de schimb valutar au fost nerespectarea art. 12 din Legea nr. 677/2001, în ceea ce privește informarea persoanelor vizate, precum și omisiunea de a efectua notificarea, conform art. 22 din aceeași lege.

FIȘĂ DE CAZ

În cadrul unei investigații efectuate la o entitate care desfășoară activități de schimb valutar, s-a constatat că aceasta prelucrează date cu caracter personal ale clienților, colectate prin intermediul formularului de acceptare a tranzacției și bonului fiscal, ulterior datele fiind înregistrate și într-un sistem de evidență electronic. Ulterior completării formularului de acceptare a tranzacției, actul de identitate era returnat persoanei vizate, fără a se reține copii ale acestor documente. Formularele de acceptare a tranzacției, generate de către aplicația

informatică după completarea datelor cu caracter personal ale persoanelor vizate, erau stocate pentru o perioadă de 10 ani, la sediul operatorului, într-un spațiu special destinat, cu acces restricționat.

La data efectuării investigației, s-a constatat că operatorul investigat nu realiza informarea persoanelor vizate conform art. 12 din Legea nr. 677/2001, deși notificase la Autoritatea națională de supraveghere prelucrarea datelor cu caracter personal în scopul desfășurării tranzacțiilor financiare.

Operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001 (prelucrare nelegală a datelor cu caracter personal), deoarece nu realiza informarea persoanelor vizate potrivit art. 12 din aceeași lege.

VII. Investigații din oficiu ca urmare a analizării anumitor notificări transmise de către operatorii de date cu caracter personal și a unor articole apărute în presă

1. Neîndeplinirea obligațiilor privind aplicarea măsurilor de securitate și de păstrare a confidențialității prelucrărilor de date

FIȘĂ DE CAZ

Am fost sesizați cu privire la faptul că, în containerele de colectare a deșeurilor aparținând unei instituții publice, s-au găsit documente care conțineau date cu caracter personal (nume, prenume, domiciliu și CNP).

Ca urmare a verificărilor efectuate, s-a constatat că la nivelul instituției publice investigate era întocmită o procedură de securitate privind prelucrarea datelor cu caracter personal conform Ordinului nr. 52/2002, însă aceasta nu prevedea mențiuni cu privire la manipularea documentelor pe suport de hârtie și nici cu privire la modalitatea de distrugere a acestora.

La nivelul instituției publice în cauză exista în derulare un contract cu o societate specializată în vederea colectării și topirii deșeurilor, conform căruia deșeurile de hârtie din birouri se colectau în coșuri de diferite culori și se evacua la terminarea programului de lucru de către personalul de întreținere și curățenie.

Instituția publică a fost sancționată pentru săvârșirea contravenției prevăzută de art. 33 din Legea nr. 677/2001, în forma neîndeplinirii obligațiilor privind aplicarea măsurilor de securitate și de păstrare a confidențialității prelucrărilor de date prevăzute de art. 20 din aceeași lege. S-a constatat că aceasta nu a aplicat măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat la documentele pe care le-a emis și care conțineau date cu caracter personal ale unor persoane fizice, iar acestea au ajuns în posesia unor persoane neautorizate.

2. Dezvăluirea în presă a datelor cu caracter personal a unor persoane publice

FIȘĂ DE CAZ

Într-o revistă săptămânală a fost publicat un editorial, care conținea o listă cu numele, prenumele și numărul de telefon mobil al unor persoane, cu statut de persoane publice. Acest editorial a apărut și în varianta on-line a săptămânalului respectiv.

S-a decis efectuarea unei investigații pentru verificarea următoarelor aspecte: sursa de colectare a datelor cu caracter personal, constând în numerele de telefon mobil ale persoanelor aflate pe lista publicată în editorial; scopul prelucrării datelor personale; temeiul legal în baza căruia s-au dezvăluit numerele de telefon mobil ale persoanelor aflate pe lista publicată în editorial; dovada obținerii consimțământului prealabil al persoanelor ale căror date au fost dezvăluite; modalitatea de informare a persoanelor vizate cu privire la prelucrarea datelor personale.

Deoarece, reprezentanții legali ai societății investigate au refuzat în repetate rânduri să furnizeze Autorității naționale de supraveghere informațiile și documentele solicitate, societatea a fost sancționată pentru săvârșirea contravenției de refuz de a furniza informații, conform art. 34 din Legea nr. 677/2001.

3. Dezvăluirea datelor cu caracter personal ale propriilor angajați pe website-ul societății

Principiile care trebuie respectate în ceea ce privește prelucrarea datelor cu caracter personal sunt stabilite prin art. 4 alin. (1) din Legea nr. 677/2001, modificată și completată,

astfel: prelucrarea datelor cu caracter personal trebuie să fie efectuată în conformitate cu dispozițiile legale în vigoare și cu bună-credință; datele să fie colectate în scopuri determinate, explicite și legitime; datele să fie adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate, iar ulterior prelucrate; datele să fie exacte și actualizate; datele trebuie să fie 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.

De asemenea, dispozițiile art. 10 din Legea nr. 677/2001, modificată și completată, legitimează prelucrarea datelor referitoare la fapte penale sau infracțiuni ori la sancțiuni administrative sau contravenționale aplicate persoanei vizate, numai de către sau sub controlul autorităților publice, în limitele puterilor ce le sunt conferite prin lege și în condițiile stabilite de legile speciale care reglementează aceste materii.

Totodată, prin Documentul de lucru privind listele negre nr. 65 din 3 octombrie 2002 adoptat de Grupul de Lucru Art. 29 constituit la nivelul Comisiei Europene, s-a stabilit că listele care conțin date ale angajaților sau ale candidaților la diverse locuri de muncă privind comportamentul acestora profesional reprobabil pot avea un impact foarte mare asupra intereselor persoanelor vizate aflate pe aceste „liste negre”, motiv pentru care aceste persoane necesită o protecție specială.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere s-a sesizat din oficiu cu privire la postarea pe website-ul unei societăți de transport, a unei liste care conținea numele, prenumele și adresa unor persoane, foști angajați ai societății, cărora li s-a încetat contractul de muncă în urma aplicării unor sancțiuni disciplinare.

Ca urmare a verificărilor efectuate s-a constatat că societatea investigată a creat un sistem de evidență cu foștii săi angajați, cărora le-a fost încetat contractul de muncă în urma creării anumitor prejudicii și aplicării unor sancțiuni disciplinare. Ulterior, lista conținând numele, prenumele și adresa de domiciliu a acestora a fost dezvăluită publicului larg, prin postarea pe website-ul societății a unui fișier în format pdf, într-o secțiune distinctă.

Operatorul a fost sancționat pentru săvârșirea contravenției prevăzută de art. 31 din Legea nr. 677/2001, omisiunea de a notifica și notificarea cu rea-credință, deoarece nu a notificat Autorității naționale de supraveghere prelucrarea datelor cu caracter personal în scopul

creării unei evidențe cu angajații cărora li s-a încetat contractul de muncă în urma aplicării unor sancțiuni disciplinare, anterior începerii prelucrării.

Totodată, operatorul a fost sancționat și pentru săvârșirea contravenției prevăzută de art. 32 din Legea nr. 677/2001, prin încălcarea art. 12 și art. 5 din aceeași lege, deoarece nu a putut face dovada informării persoanelor vizate în nicio modalitate prevăzută de lege și a dezvăluit pe website-ul propriu datele cu caracter personal prelucrate, fără a avea consimțământul expres și neechivoc al persoanelor vizate.

Secțiunea a 3-a Activitatea de soluționare a plângerilor și sesizărilor

I. Prezentare generală

În scopul apărării drepturilor și libertăților fundamentale ale persoanelor vizate, Autoritatea națională de supraveghere investighează orice încălcare a drepturilor persoanelor vizate și orice nerespectare a obligațiilor de către operatorii de date cu privire la prelucrarea datelor cu caracter personal.

Persoanele fizice pot sesiza instituția noastră asupra oricărui aspecte legate de prelucrarea datelor cu caracter personal de către operatorii de date sau pot adresa plângeri, în cazul în care se consideră lezate prin modul de prelucrare a datelor lor personale de către operatorii de date sau persoanele împuternicite de aceștia.

Legea prevede câteva condiții pe care trebuie să le îndeplinească persoanele vizate care adresează o plângere Autorității de supraveghere, respectiv să nu fi introdus anterior o acțiune în justiție cu același obiect și cu aceleași părți și să fi înaintat anterior (15 zile) o cerere cu același conținut către operatorul de date de la care nu a primit răspuns sau de la care a primit un răspuns nesatisfăcător.

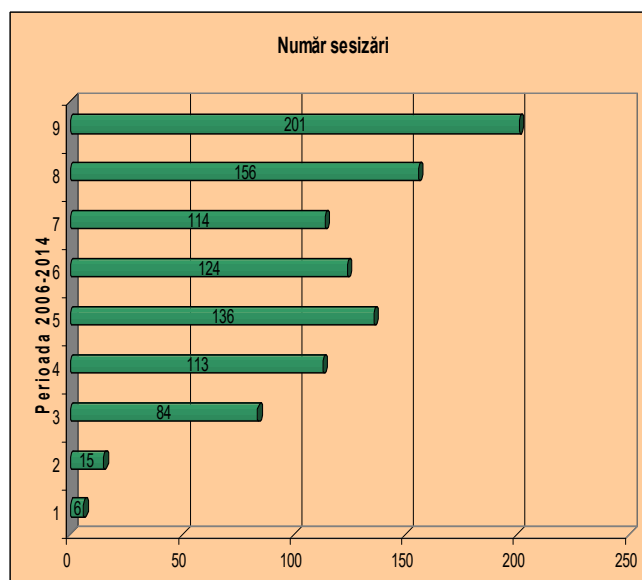
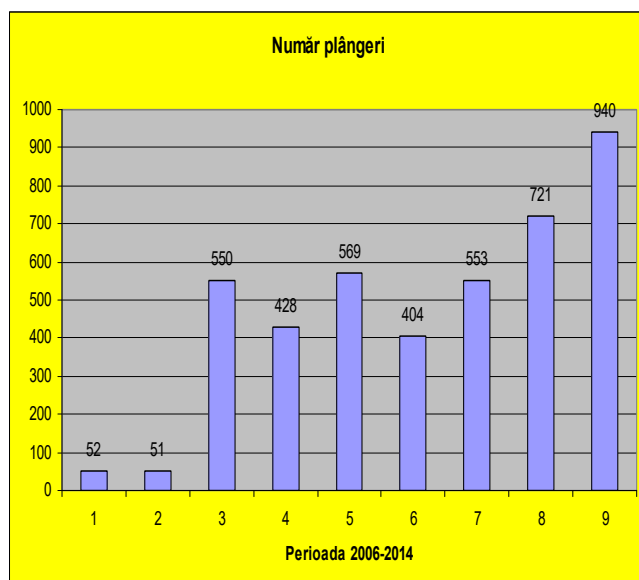
În aceste condiții, Autoritatea de supraveghere a primit și soluționat, în cursul anului 2014, un număr considerabil de **petiții**, respectiv **1243**, ceea ce reprezintă o creștere cu aproximativ 30% față de anul anterior.

Prin aceste petiții au fost sesizate aspecte legate de posibile încălcări ale drepturilor reglementate de Legea nr. 677/2001 și de Legea nr. 506/2004.

Creșterea numărului petițiilor primite în cursul anului 2014 demonstrează faptul că atribuțiile Autorității de supraveghere în domeniul protecției datelor cu caracter personal sunt mai bine cunoscute persoanelor fizice față de anii anteriori, iar cetățenii manifestă o încredere din ce în ce mai mare în eficiența acțiunilor derulate de către Autoritatea de supraveghere în ceea ce privește apărarea drepturilor și libertăților fundamentale ale persoanelor vizate.

Astfel, s-au primit **940 de plângeri, 201 sesizări, 102 solicitări** de informații privind activitatea de soluționare a plângerilor și sesizărilor.

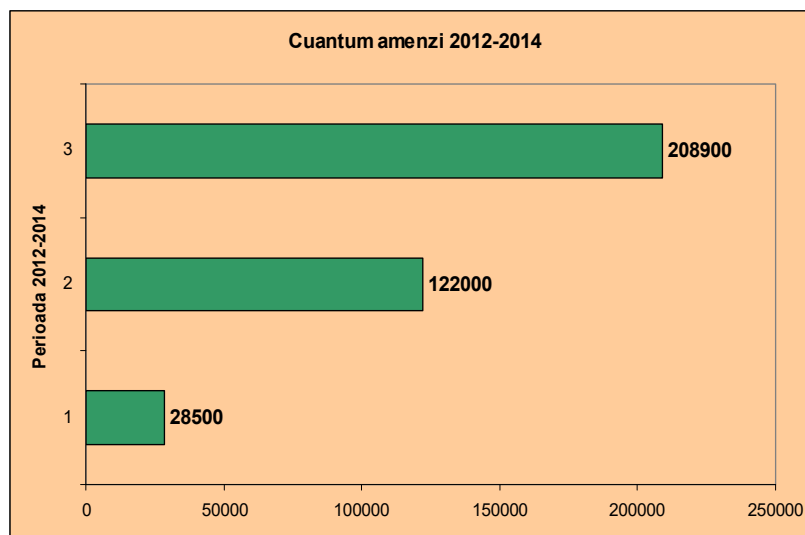
Figurile 1&2: Numărul plângerilor și al sesizărilor în perioada 2006-2014



Pentru soluționarea plângerilor și sesizărilor primite, au fost efectuate **248 de investigații pe teren și 85 de investigații în scris**. În cazurile în care autoritatea a considerat întemeiate aspectele verificate în cadrul investigațiilor, au fost aplicate sancțiuni contravenționale constând în **118 amenzi și 186 avertismente**.

Cuantumul total al amenzilor aplicate în 2014 în cadrul investigațiilor efectuate pentru soluționarea plângerilor și sesizărilor este de **208.900 lei**, în creștere față de anul 2013.

Figura 3: Cuantumul amenzilor aplicate în activitatea de soluționare a plângerilor și sesizărilor în perioada 2012-2014



Totodată, în urma demersurilor de soluționare a plângerilor și sesizărilor adresate autorității, au fost emise **11 decizii** de măsuri ale președintelui Autorității de supraveghere, prin care s-a dispus încetarea prelucrării și/sau ștergerea datelor sau a anumitor categorii de date, respectiv suspendarea prelucrării datelor cu caracter personal.

Plângerile și sesizările primite au vizat o gamă largă de domenii, raportat la obiectul de activitate al persoanelor juridice reclamate.

Ca și în anii precedenți, cele mai multe dintre plângeri au vizat prelucrarea datelor cu caracter personal în domeniul financiar-bancar, al monitorizării și securității spațiilor publice sau private prin mijloace de supraveghere video, al comunicațiilor electronice, precum și în ceea ce privește dezvăluirea datelor și nerespectării măsurilor de securitate și confidențialitate a prelucrării acestora.

Astfel, în domeniul financiar-bancar, în care operatorii sunt, în principal, bănci sau instituții financiare nebancare, s-a constatat o creștere semnificativă a numărului petițiilor față de anii anteriori. Principalul motiv de nemulțumire a persoanelor vizate, care a determinat sesizarea Autorității naționale de supraveghere, a fost legat de raportarea datelor cu caracter personal către sisteme de evidență de tip birou de credit, fără respectarea prevederilor Legii nr.

677/2001 și ale Deciziei nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit.

În urma investigațiilor efectuate, s-a constatat faptul că unii operatori nu au respectat prevederile legii și deciziei susmenționate, în special în ceea ce privește termenul de înștiințare prealabilă a persoanelor vizate cu privire la transmiterea datelor negative la biroul de credit (15 zile) și conținutul acesteia, termenul de transmitere a datelor raportat la data scadenței (după 30 de zile) și exactitatea datelor transmise. De asemenea, s-a constatat că nu există o practică unitară a participanților la biroul de credit (bănci sau instituții financiare nebankare) cu privire la mențiunile efectuate în cadrul unor secțiuni din cadrul raportului de credit sau cu privire la frecvența transmiterii datelor (ex. date negative, valoarea lunară programată), fiind astfel raportate mai multe date din aceeași categorie în cursul unei luni.

Transmiterea eronată a unor informații către biroul de credit sau fără asigurarea unei informări prealabile adecvate a persoanelor vizate, este de natură a aduce potențiale prejudicii acestora, prin posibilitatea de creare a unor profiluri de persoane rău-platnice cărora le va fi restricționat accesul la obținerea altor credite.

O pondere însemnată a plângerilor și sesizărilor adresate la Autoritatea națională de supraveghere în anul 2014 a avut ca obiect prelucrarea datelor personale prin mijloace de supraveghere video, instalate în diverse spații. Astfel, în multe dintre cazuri operatorii reclamați au fost asociații de proprietari. De asemenea, prin multe petiții instituția noastră a fost sesizată în legătură cu prelucrările de date efectuate prin intermediul sistemelor de supraveghere video instalate la locul de muncă. Ca urmare a montării sistemelor de supraveghere în unitățile de învățământ, fie în sălile de curs sau alte încăperi pentru supravegherea desfășurării examenelor naționale și de bacalaureat, fie în alte spații (ex. holuri), Autoritatea națională de supraveghere a fost sesizată cu privire la prelucrarea datelor colectate prin intermediul acestor sisteme. Totodată, prin multe petiții, persoanele fizice și-au exprimat nemulțumirea față de prelucrarea imaginii lor de către alte persoane fizice care și-au montat astfel de sisteme, colectând prin intermediul acestora și imagini din afara spațiilor lor private.

În urma investigațiilor realizate, s-a constatat că unii operatori nu cunosc, nu respectă sau ignoră dispozițiile legale aplicabile prelucrărilor de date prin mijloace de supraveghere video (ale Legii nr. 677/2001 și ale Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video), în special cele cu privire la

respectarea drepturilor persoanelor vizate și a condițiilor în care se poate efectua prelucrarea imaginilor, inclusiv sub aspectul notificării prelucrărilor la Autoritatea națională de supraveghere.

Având în vedere numărul mare de asociații de proprietari care au instalat sisteme de supraveghere video în condominiile pe care le reprezintă, aspectele semnalate instituției noastre de către tot mai mulți petiționari și constatările rezultate din investigațiile efectuate la nivelul asociațiilor de proprietari reclamate, Autoritatea națională de supraveghere a elaborat un Ghid privind prelucrările de date cu caracter personal efectuate prin intermediul sistemelor de supraveghere video instalate în cadrul asociațiilor de proprietari, destinat sprijinirii asociațiilor de proprietari în cazul în care decid instalarea și punerea în funcțiune a unui sistem de supraveghere prin mijloace video.

De asemenea, în anul 2014 a fost înregistrat, un număr mare de petiții având ca obiect dezvăluirea unor date cu caracter personal pe Internet și transmiterea de mesaje comerciale nesolicitate. Operatorii reclamați au fost, în principal, societăți care administrează diferite site-uri (de regulă, indexate pe motorul de căutare Google), care efectuează activități de comerț online sau marketing direct.

În urma investigațiilor efectuate, s-a remarcat faptul că datele personale ale persoanelor vizate au fost prelucrate fără consimțământul acestora și nu s-a dat curs cererilor de exercitare a drepturilor persoanelor vizate, în special a dreptului de opoziție sau de intervenție ce viza obținerea ștergerii datelor.

În ceea ce privește inadmisibilitatea petițiilor primite și în anul 2014, ca și în anii precedenți, principalul motiv de respingere a plângerilor a rămas neîndeplinirea procedurii legale prealabile de către petenți (dispozițiile art. 25 din Legea nr. 677/2001 care prevăd faptul că plângerea către Autoritatea națională de supraveghere nu poate fi înaintată mai devreme de 15 zile de la înaintarea unei plângeri cu același conținut către operator).

Totodată, plângerile și sesizările au mai fost respinse ca inadmisibile sau neîntemeiate în cazul neprezentării de dovezi în susținerea aspectelor prezentate, sesizării unor aspecte în legătură cu care Autoritatea națională de supraveghere nu avea competența materială sau teritorială să intervină, imposibilității identificării exacte a entității reclamate (spre exemplu, expeditorul unei comunicări comerciale electronice nesolicitate) sau introducerii în prealabil a unei acțiuni în justiție.

II. Principalele constatări rezultate din activitatea de soluționare a plângerilor și sesizărilor

1. Raportarea datelor personale către sisteme de evidență tip birou de credit

În anul 2014 numărul plângerilor ce vizează transmiterea datelor personale către biroul de credit a crescut față de anul precedent. Ca urmare a constatărilor din cadrul investigațiilor desfășurate, a rezultat o serie de aspecte privind nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul acestor sisteme, cu referire la:

- tipul de informații raportate de către bănci și instituțiile financiare nebancale,
- modalitatea și termenul de realizare a informării prealabile impuse de Legea nr. 677/2001 și de Decizia nr. 105/2007,
- termenul și frecvența raportărilor în cursul unei luni.

Aceste constatări denotă faptul că respectivii operatori (participanți la sistemul de evidență al biroului de credit) au încălcat prevederile Legii nr. 677/2001 și ale Deciziei nr. 105/2007 care reglementează obligațiile ce le revin cu privire la transmiterea datelor persoanelor vizate la biroul de credit.

În cazurile în care, în urma investigațiilor efectuate, s-a constatat că băncile/instituțiile financiare nebancale nu au dat curs în mod voluntar cererilor formulate de petenți, Autoritatea națională de supraveghere a dispus prin decizie a președintelui, ștergerea datelor transmise la biroul de credit fără respectarea legii.

FIȘĂ DE CAZ

Prin petiția transmisă, petenta și-a exprimat nemulțumirea față de raportarea unor date negative de către o bancă comercială la biroul de credit.

Astfel, petenta a menționat că a încheiat cu o bancă comercială un contract de credit; ulterior, pe parcursul executării contractului fiind înregistrate o serie de restanțe, datele sale au fost transmise la biroul de credit, fără a fi informată cu 15 zile înainte de raportarea datelor negative.

În cadrul investigației efectuate, banca nu a prezentat nicio dovadă din care să rezulte că a informat-o în prealabil pe petentă cu privire la transmiterea către biroul de credit a informațiilor legate de restanțele înregistrate (date negative), așa cum prevede art. 12 alin. (1) din Legea nr. 677/2001 și art. 8 alin. (2) din Decizia nr. 105/2007.

Față de această situație, banca în cauză a fost sancționată pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, pentru nerespectarea prevederilor acestei legi și ale Deciziei nr. 105/2007.

În baza acestor constatări, s-a dispus prin decizie ștergerea datelor negative, raportate către sistemul de evidență al biroului de credit fără respectarea prevederilor legale, operatorul dând curs măsurilor dispuse.

FIȘĂ DE CAZ

Prin petiția înregistrată la Autoritatea de supraveghere, petentul a sesizat faptul că banca i-a încălcat dreptul de intervenție, întrucât nu i-a rectificat datele cu caracter personal raportate la biroul de credit.

Potentul a susținut că a solicitat băncii să rectifice datele negative raportate la biroul de credit, deoarece restanța înscrisă nu avea o întârziere la plată mai mare de 30 de zile, însă banca a refuzat.

În urma investigației efectuate, s-a constatat că banca a raportat date negative la biroul de credit cu încălcarea dispozițiilor art. 5 alin. (1) din Decizia nr. 105/2007, restanța acumulată de petent nefiind mai mare de 30 de zile de la scadență.

Față de această situație, operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, constând în încălcarea prevederilor acestei legi și a Deciziei nr. 105/2007.

În urma demersurilor efectuate de Autoritatea de supraveghere, datele negative raportate la biroul de credit de către bancă pe numele petentului, cu încălcarea prevederilor legale, au fost șterse.

FIȘĂ DE CAZ

Un petent a sesizat faptul că o bancă a raportat datele sale cu caracter personal la biroul de credit, în condițiile în care nu a încheiat un contract de credit cu această instituție bancară.

În cadrul investigației efectuate, banca nu a putut face dovada existenței unui contract de credit încheiat cu petentul, transmiterea datelor către biroul de credit realizându-se așadar fără niciun temei.

Față de această situație, operatorul a fost sancționat pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, respectiv pentru prelucrarea nelegală a datelor cu caracter personal.

În urma demersurilor efectuate de Autoritatea națională de supraveghere, datele raportate la biroul de credit de către bancă pe numele petentului au fost șterse.

FIȘĂ DE CAZ

Un petent a reclamat faptul că o bancă nu i-a actualizat datele referitoare la restructurarea unui credit, transmise la biroul de credit, motiv pentru care i s-a refuzat cererea de acordare a unui credit de către o altă instituție bancară.

Banca și-a exprimat punctul de vedere față de cazul petentului prin mai multe adrese, transmise atât acestuia, cât și Autorității Naționale pentru Protecția Consumatorilor, considerând că raportările transmise la biroul de credit sunt corect efectuate și nu pot fi radiate.

În urma investigației efectuate, a rezultat că banca nu l-a informat pe petent în nicio modalitate cu privire la consecințele acceptării restructurării cardului său de credit, respectiv cu privire la transmiterea acestor date la biroul de credit.

Față de această situație, operatorul a fost sancționat pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, pentru nerespectarea dreptului de informare corespunzătoare a petentului.

Autoritatea de supraveghere a dispus prin decizie ca banca să ia măsuri pentru ștergerea datelor referitoare la restructurarea cardului de credit, menționate la rubrica "Observații" din

cadrul raportului de credit, pe care le-a transmis în mod eronat la biroul de credit pe numele petentului.

Operatorul în cauză a pus în aplicare decizia instituției noastre.

2. Prelucrarea datelor prin mijloace de supraveghere video

Referitor la prelucrarea datelor personale prin mijloace de supraveghere video, numărul petițiilor transmise Autorității naționale de supraveghere a înregistrat o creștere față de anii anteriori ca urmare a montării de sisteme de supraveghere video de către tot mai multe persoane juridice sau fizice, precum și a conștientizării de către persoanele fizice a drepturilor de care beneficiază și a rolului Autorității naționale de supraveghere în apărarea acestora.

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de supraveghere video se supune atât prevederilor Legii nr. 677/2001, modificată și completată, ale Deciziei nr. 52/2012, cât și ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată.

În urma investigațiilor efectuate la mai multe categorii de operatori, în special persoane juridice și asociații de proprietari, s-a constatat că aceștia fie nu cunosc, fie nu respectă prevederile Legii nr. 677/2001 și ale Deciziei nr. 52/2012.

De asemenea, Autoritatea națională de supraveghere a efectuat o serie de investigații cu privire la prelucrările de date efectuate prin intermediul sistemelor de supraveghere video instalate la nivelul unor unități școlare, ca urmare a plângerilor și sesizărilor primite, în special din partea unora dintre cadrele didactice ce își desfășoară activitatea în respectivele unități.

În cadrul investigațiilor efectuate la unitățile de învățământ, s-a constatat faptul că, inițial, camerele video au fost montate în sălile de curs în scopul exclusiv al desfășurării examenelor naționale și de bacalaureat, în baza reglementărilor emise de Ministerul Educației Naționale în această materie, însă în unele unități de învățământ s-a decis menținerea acestora în funcțiune și după încheierea examenelor. Mai mult decât atât, în unele situații, s-a constatat faptul că au fost montate camere de supraveghere video și în alte spații, de genul laboratoarelor, birourilor, cancelariilor, unde își desfășoară activitatea curentă elevii, cadrele didactice sau personalul auxiliar.

Autoritatea națională de supraveghere a sesizat Ministerul Educației Naționale cu privire la necesitatea modificării procedurilor operaționale ce vizează acest subiect, în vederea asigurării respectării dispozițiilor Legii nr. 677/2001 în mod unitar, astfel încât:

- prelucrarea datelor efectuată prin montarea unor camere de supraveghere video în sălile de curs pentru desfășurarea examenelor naționale să fie realizată strict pe perioada desfășurării acestora;
- prelucrarea datelor prin montarea unor camere de supraveghere video în sălile de curs pentru desfășurarea examenelor naționale să fie efectuată pe baza unor instrucțiuni care să reglementeze activitățile pe care trebuie să le desfășoare persoanele împuternicite;
- responsabilitățile ce revin fiecărei structuri implicate (inspectorate școlare, unități școlare/instituțiile de învățământ preuniversitar de stat, comisiile județene de examen/comisia de examen a municipiului București, comisiile din centrele de examen, comisiile din centrele zonale de evaluare, comisiile de contestații, utilizatori) în cadrul prelucrării datelor personale prin montarea unor camere de supraveghere video în sălile de curs pentru desfășurarea examenelor naționale să fie stabilite în mod distinct, inclusiv sub aspectul verificării de către operatori a respectării instrucțiunilor mai sus amintite;
- perioada de menținere în funcțiune a camerelor video, precum și modalitatea de încetare a funcționării acestora să fie stabilite în mod expres;
- menținerea în funcțiune a camerelor de supraveghere video în sălile de curs în afara perioadelor de desfășurare a examenelor naționale nu se poate realiza decât pe baza avizului Autorității naționale de supraveghere, în conformitate cu art. 8 alin. (3) din Decizia nr. 52/2012, de către unitățile școlare care întrunesc în acest caz calitatea de operator de date cu caracter personal.

Cu privire la acest ultim aspect, instituția noastră precizează că acordarea avizului se poate face numai în situații temeinic justificate și dovedite, cu îndeplinirea cumulativă a mai multor condiții, după cum urmează:

Unitățile de învățământ solicitante ale avizelor trebuie să prezinte argumente privind interesul legitim al instalării unui asemenea sistem de supraveghere, astfel încât acesta să prevaleze asupra drepturilor și libertăților fundamentale sau intereselor persoanelor supravegheate prin utilizarea acestui sistem.

În același timp, trebuie făcută dovada faptului că a fost efectuată consultarea sindicatului sau a reprezentanților angajaților și a obținerii consimțământului expres și neechivoc al tuturor angajaților, precum și al reprezentanților legali ai minorilor.

De asemenea, trebuie indicat explicit scopul și argumentată necesitatea prelucrării datelor cu caracter personal ale persoanelor care își desfășoară activitatea în sălile de clasă, în birouri sau cancelarii, prin intermediul sistemelor de supraveghere video.

Totodată, precizăm că Autoritatea națională de supraveghere a obținut, în instanță, hotărâri definitive și irevocabile prin care se statuează faptul că prelucrarea datelor personale (imaginilor) ale angajaților în birouri s-a realizat în condiții de nelegalitate, întrucât nu a fost efectuată anterior implementării dispozitivelor de videosupraveghere o analiză temeinică asupra necesității și proporționalității unei astfel de măsuri, precum și identificarea de soluții alternative care să aibă un impact mai redus asupra vieții private a salariaților.

De asemenea, instanțele au stabilit faptul că prin instalarea camerelor de supraveghere video a fost încălcat dreptul la viață privată al salariaților și s-a creat în rândul celor vizualizați o stare de disconfort.

În ceea ce privește instalarea unor camere de supraveghere video de către persoane fizice pentru uzul lor personal (de exemplu, protejarea vieții sau a proprietății private), în urma controalelor efectuate a reieșit că situațiile în care este incidentă legislația privind protecția datelor personale diferă, în funcție de condițiile în care sunt realizate operațiunile de prelucrare.

Astfel, regula generală prevăzută de art. 2 alin. (6) din Legea nr. 677/2001 constă în inaplicabilitatea dispozițiilor legislației privind protecția datelor personale în cazul prelucrărilor de date efectuate de persoane fizice exclusiv pentru uzul lor personal, dacă datele în cauză nu sunt destinate a fi dezvăluite. Aceste prevederi sunt reluate de art. 17 alin. (2) din Decizia nr. 52/2012.

Pe de altă parte, conform Hotărârii Curții de Justiție a Uniunii Europene din 11 decembrie 2014, pronunțată în cauza František Ryneš împotriva Úřad pro ochranu osobních údajů (C-212/2013), s-a considerat că legislația privind protecția datelor personale se poate aplica și în situațiile în care persoanele fizice operează un sistem de supraveghere instalat pe proprietatea personală pentru uzul personal, dar care surprinde și stochează imagini din spațiul public.

Prin urmare, în vederea respectării jurisprudenței CJUE, după data pronunțării hotărârii anterior menționate, Autoritatea națională de supraveghere a considerat admisibile acele

plângeri și sesizări prin care se reclamă instalarea de către persoanele fizice a unui sistem de supraveghere video prin care se colectează și stochează inclusiv imagini din spațiul public.

FIȘĂ DE CAZ (supraveghere video la locul de muncă)

Printr-o plângere, Autoritatea națională de supraveghere a fost sesizată în legătură cu prelucrarea datelor cu caracter personal prin intermediul unui sistem de supraveghere video instalat de către primăria unei comune, cu nerespectarea Legii nr. 677/2001 și a Deciziei nr. 52/2012.

Astfel, s-a reclamat faptul că era montată o cameră de supraveghere video în incinta unui birou din cadrul primăriei, în care își desfășurau activitatea funcționari publici, iar imaginile captate și stocate erau vizualizate pe un terminal instalat în biroul primarului comunei.

La data efectuării investigației, s-au confirmat aspectele sesizate, motiv pentru care s-a dispus încetarea prelucrării datelor cu caracter personal (imaginea) captate prin intermediul camerelor de supraveghere video montate în birouri, măsură implementată de către primar, conform celor solicitate de instituția noastră.

Având în vedere faptul că primăria nu a notificat Autorității naționale de supraveghere prelucrările de date cu caracter personal realizate prin sistemul de supraveghere video, așa cum prevede art. 22 din Legea nr. 677/2001, nu a realizat o informare completă a persoanelor vizate, așa cum prevede art. 12 din Legea nr. 677/2001 și nici nu a implementat o politică de securitate a datelor prelucrate prin intermediul sistemului de supraveghere video, care să cuprindă cerințele minime de securitate a prelucrărilor de date cu caracter personal, operatorul a fost sancționat contravențional în baza prevederilor art. 31, art. 32, respectiv art. 33 din Legea nr. 677/2001.

FIȘĂ DE CAZ (asociații de proprietari)

Prin plângerea adresată Autorității naționale de supraveghere, un petent a sesizat faptul că asociația de proprietari din blocul în care locuiește a instalat un sistem de supraveghere

video fără a exista o hotărâre a adunării generale a proprietarilor și prin încălcarea actelor normative care reglementează prelucrarea datelor cu caracter personal.

De asemenea, s-a mai reclamat faptul că au fost instalate camere la etajul unde locuiește, în ciuda opoziției manifestate în scris de către proprietarii de pe acel palier. În aceeași petiție, se mai sesiza faptul că asociația de proprietari nu este înscrisă în registrul de evidență a prelucrărilor de date cu caracter personal pentru această prelucrare.

În urma investigației, asociația de proprietari a fost sancționată contravențional cu amendă pentru săvârșirea faptelor prevăzute de art. 31 (omisiunea de a notifica prelucrarea efectuată prin intermediul sistemului de supraveghere video instalat), art. 32 (lipsa informării persoanelor vizate, potrivit legii) și art. 33 (absența unei proceduri privind securitatea prelucrării datelor cu caracter personal) din Legea nr. 677/2001.

În urma investigației, s-a dispus prin decizie încetarea prelucrării și ștergerea datelor cu caracter personal colectate prin intermediul camerelor de supraveghere video instalate la etajul unde locatarii nu și-au dat consimțământul pentru această prelucrare.

Decizia a fost adusă la îndeplinire de către asociația respectivă.

FIȘĂ DE CAZ (unități de învățământ)

Prin petiția transmisă, petentul a sesizat că s-a dispus de conducerea unui liceu instalarea unei camere de supraveghere audio-video în secretariatul liceului, fără acordul petentei care își desfășura activitatea în biroul respectiv.

În cadrul investigației efectuate, s-a reținut faptul că, prin invocarea unor ordine emise de Ministerul Educației Naționale privind desfășurarea examenelor naționale și de bacalaureat, liceul a decis instalarea unui sistem de supraveghere video pe holuri, la intrarea în liceu, în curtea exterioară, în sala de consiliu, în cabinetele de informatică, în cancelarie, în sălile de clasă și pe holul de la cămin (reglementările emise de Ministerul Educației Naționale se refereau însă la instalarea camerelor de supraveghere în clase numai pe perioada examenelor naționale și de bacalaureat).

În urma investigației, liceul a fost sancționat contravențional pentru săvârșirea faptelor prevăzute de art. 31, întrucât a omis să notifice în calitate de operator prelucrarea efectuată prin intermediul camerelor de supraveghere și respectiv, de art. 32, pentru inexistența unei

informări corespunzătoare a persoanelor vizate și lipsa unui temei legal adecvat pentru instalarea camerelor de supraveghere în anumite spații.

De asemenea, în urma investigației, s-a dispus prin decizie încetarea prelucrării datelor cu caracter personal efectuate prin intermediul camerelor de supraveghere video montate în secretariat, cancelarie, săli de curs (în afara examenelor naționale), sala de consiliu.

Măsura dispusă de Autoritatea națională de supraveghere a fost respectată de către liceul în cauză.

3. Dezvăluirea datelor personale către diverse entități

Prin mai multe plângeri adresate Autorității naționale de supraveghere, au fost semnalate aspecte referitoare la încălcarea dispozițiilor legale privind condițiile în care date personale au fost dezvăluite către terți (instituții medicale, entități de drept public și privat), fără să fi fost obținut în prealabil acordul persoanelor vizate ori fără să se fi acordat suficientă importanță dreptului la informare al acestora.

De asemenea, în anumite cazuri, s-a constatat în urma investigațiilor întreprinse că dezvăluirea datelor personale s-a efectuat fără să existe un temei legal sau în mod disproporționat față de scopul urmărit.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către angajatorul său, o societate bancară, în sensul că ar fi colectat și, respectiv, ar fi dezvăluit ilegal datele sale cu caracter personal către mai multe entități. Petentul și-a exercitat dreptul de acces către angajatorul prezumat a-i fi dezvăluit datele cu caracter personal, solicitând comunicarea tuturor documentelor care aveau legătură cu incidentul semnalat.

În vederea soluționării cazului sesizat, Autoritatea națională de supraveghere a extins controlul la toate entitățile implicate.

În cadrul acestor investigații, s-a constatat faptul că, în cursul procedurii disciplinare deschise de angajator (societatea bancară), ca urmare a numeroaselor convocări realizate în cursul cercetării disciplinare, în urma cărora petentul a depus o serie de documente justificative,

angajatorul a solicitat instituției medicale la serviciile căreia apelase petentul, o copie de pe declarația pe propria răspundere completată la momentul eliberării certificatului medical. Cu această ocazie, dând curs solicitării, instituția medicală a remis angajatorului mai multe copii de pe actele medicale ce conțineau date sensibile (date privind starea de sănătate) și care nu erau necesar a fi dezvăluite.

De asemenea, în cadrul aceleiași proceduri disciplinare, o secție de poliție a transmis către societatea bancară, la solicitarea acesteia, informații privind săvârșirea unei contravenții și aplicarea de sancțiuni contravenționale în sarcina petentului, pentru fapte produse în afara obligațiilor sale de serviciu.

Ca atare, la finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a aplicat sancțiuni contravenționale în baza art. 32 din Legea nr. 677/2001, tuturor entităților implicate în acest caz, pentru prelucrarea excesivă a unor date personale prin raportare la scopul prelucrării și la tipurile de date personale colectate sau respectiv, dezvăluite.

FIȘĂ DE CAZ

Un petent a reclamat faptul că i-a fost încălcat dreptul la confidențialitate de către o instituție a prefectului, întrucât aceasta a transmis date cu caracter personal ale petentului către mai multe primării împotriva cărora petentul formulase numeroase reclamații. Astfel, instituția prefectului reclamată a divulgat numele și prenumele petentului, adresa de e-mail și adresa sa de domiciliu, fără acordul acestuia, prin adrese transmise către primării din zona sa teritorială, către unele fiind înaintate chiar integral petiția petentului.

Ca urmare a investigației efectuate, s-a constatat faptul că, în cazul petițiilor adresate de petent instituției prefectului, competența de a verifica aspectele sesizate și de a aplica sancțiuni, după caz, revenea persoanelor împuternicite de ministrul afacerilor interne sau de prefect, fiind prin urmare nejustificată transmiterea datelor sale personale sau redirectionarea petițiilor către chiar primăriile împotriva cărora au fost formulate aceste reclamații.

În apărarea sa, instituția prefectului a invocat prevederile O.G. nr. 27/2002 privind activitatea de soluționare a petițiilor, cu modificările și completările ulterioare, în sensul că petițiile sunt redirectionate către alte instituții în cazul în care acestea au atribuții în rezolvarea

situației sesizate. De asemenea, s-a mai susținut faptul că au fost dezvăluite datele de contact ale petentului, întrucât pe niciuna dintre reclamațiile transmise de acesta, nu fuseseră înscrise mențiunile "secret" sau "strict secret". Totodată, s-a mai precizat faptul că petentul își consemnează datele cu caracter personal în documentele publicate în format electronic pe blogul său.

Argumentele invocate de operator nu au fost acceptate ca fiind argumente legale valabile în procesul de dezvăluire a datelor în cazul semnalat. Potrivit art. 5 din Legea nr. 677/2001, orice prelucrare de date cu caracter personal poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare sau în alte cazuri de excepție prevăzute la art. 5 alin. (2) din Legea nr. 677/2001, neaplicabile în această speță.

Ca atare, Autoritatea națională de supraveghere a dispus sancționarea operatorului în baza art. 32 din Legea nr. 677/2001.

FIȘĂ DE CAZ

O petentă a sesizat Autoritatea națională de supraveghere cu o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către fostul său angajator, o societate de telefonie mobilă, în sensul că acesta i-ar fi dezvăluit ilegal datele sale cu caracter personal prelucrate prin contractul individual de muncă către o societate de selecție și plasare a forței de muncă, fără acordul său. În urma acestei dezvăluiri, această din urmă societate a încheiat un contract de muncă în numele petentei, fără consimțământul acesteia, petenta aflând despre această situație cu ocazia depunerii documentației necesare la autoritățile competente în vederea obținerii indemnizației de șomaj.

Autoritatea națională de supraveghere a efectuat investigații atât la fostul angajator, cât și la societatea căreia i se dezvăluiseră datele petentei, pentru a elucida circumstanțele în care au fost dezvăluite datele către societatea de selecție și plasare a forței de muncă.

Ca urmare a controlului efectuat la fostul angajator, acesta a motivat necesitatea transmiterii informațiilor aferente contractului de muncă al petentei pentru evitarea restructurării postului acesteia. Cu toate acestea, neexistând acordul petentei pentru

dezvăluirea acestor informații, s-a dispus sancționarea contravențională în temeiul art. 32 din Legea nr. 677/2001.

În urma declarațiilor obținute de la reprezentanții societății de selecție și plasare a forței de muncă, s-a constatat că, deși petenta se prezentase la un interviu prealabil cu această societate, nu semnase niciun contract de muncă, astfel că înscrierea datelor sale în REVISAL s-a făcut fără consimțământul său, motiv pentru care și acest operator a fost sancționat contravențional în baza art. 32 din Legea nr. 677/2001.

4. Dezvăluirea datelor personale pe Internet

În anul 2014, Autoritatea națională de supraveghere a înregistrat un număr considerabil de plângeri având ca obiect dezvăluirea datelor personale pe Internet, fie în legătură cu derularea unor proceduri judiciare, fie pe diverse pagini indexate de Google, de către persoane fizice sau entități private.

În cazul plângerilor considerate admisibile au fost efectuate investigații pentru soluționarea aspectelor reclamate.

a) Dezvăluirea datelor personale în legătură cu derularea unor proceduri judiciare

Dezvăluirea pe Internet a unor date cu caracter personal din dosare aflate sau care s-au aflat pe rolul instanțelor judecătorești a făcut obiectul mai multor investigații, ca urmare a plângerilor înregistrate la Autoritatea națională de supraveghere. Persoanele vizate reclamau dezvăluirea datelor personale fie pe portal.just.ro (portalul instanțelor de judecată din România, administrat de Ministerul Justiției), fie pe diverse platforme legislative administrate de societăți comerciale, care preluau informațiile în mod automat de pe portal.just.ro.

În cazurile care au privit portalul instanțelor de judecată (portal.just.ro), petenții au reclamat, în principal, dezvăluirea mai multor categorii de date, inclusiv a CNP-ului și afișarea dosarului cuprinzând datele personale ale părților inclusiv după arhivarea și scoaterea acestuia de pe rolul instanțelor de judecată. Deși petenții s-au adresat instanțelor de judecată responsabile de publicarea datelor în ECRIS (aplicația internă de gestiune a dosarului în

instanță) și care au fost preluate automat pe portal.just.ro, aspectele sesizate nu au fost soluționate, motiv pentru care s-au adresat Autorității naționale de supraveghere. În urma investigațiilor efectuate, datele personale publicate excesiv au fost șterse, iar cele afișate după soluționarea și arhivarea dosarului au fost anonimizate.

Totodată, Autoritatea națională de supraveghere s-a adresat Ministerului Justiției, în vederea verificării implementării Recomandării nr. 69/2012 prin care instituția noastră solicita Ministerului Justiției și Consiliului Superior al Magistraturii luarea măsurilor pentru stabilirea unei durate limitate de stocare a datelor cu caracter personal conținute în aplicația ECRIS, disponibile pe portalul instanțelor de judecată, raportat la principiul proporționalității scopului prelucrării efectuate și în concordanță cu dispozițiile legale ale Codului de procedură civilă, Codului de procedură penală și ale Legii Arhivelor Naționale.

În cadrul unora dintre investigațiile desfășurate, s-a constatat că pe portalul instanțelor de judecată erau disponibile informații (inclusiv numele părților) din dosare care ar fi trebuit să fie arhivate electronic automat după doi ani de la ultima intervenție, precum și dosare în care erau dezvăluite excesiv date personale precum codul numeric personal.

În urma corespondenței purtate cu Ministerul Justiției, Autoritatea națională de supraveghere a fost informată cu privire la adoptarea mai multor măsuri la nivelul acestui minister, dar și al instanțelor judecătorești, prin care se urmărește respectarea Legii nr. 677/2001, astfel încât să nu fie dezvăluite mai multe date personale decât cele strict necesare pentru asigurarea publicității pe portal, iar informațiile aferente dosarelor să fie șterse la împlinirea termenului de arhivare electronică de doi ani.

De asemenea, în cadrul demersurilor de soluționare a unor plângeri, instituția noastră s-a adresat Înaltei Curți de Casație și Justiție, care, în consecință, a luat măsura de a elimina indexările din motoarele de căutare pe Internet a datelor personale aferente dosarelor aflate pe rolul instanței supreme, în mod similar cu portalul celorlalte instanțe judecătorești din România.

Cazurile referitoare la prelucrarea datelor personale pe anumite platforme legislative, date din dosare aflate sau care s-au aflat pe rolul instanțelor judecătorești, au fost asemănătoare ca și problematică cu cele care au privit portal.just.ro, o diferență importantă constând în faptul că pe portalul instanțelor de judecată informațiile nu sunt indexate pe motoarele de căutare tip Google, așa cum se întâmplă în cazul platformelor legislative.

În alte situații, petenții au reclamat faptul că hotărârile judecătorești în care au avut calitatea de părți se află pe diferite site-uri administrate de societăți comerciale. În urma investigațiilor efectuate a rezultat că scopul publicării hotărârilor judecătorești pe anumite site-uri este acela de a pune la dispoziția publicului jurisprudența în mod gratuit și de a furniza informații persoanelor interesate de probleme juridice pe domenii specifice. Spre exemplu, raportat la aspecte rezultate din procesele de divorț, operatorii în cauză au înțeles să dea curs recomandării Autorității de supraveghere de a nu mai fi publicate în acest caz datele personale ale părților din dosare.

Petenții s-au adresat Autorității naționale de supraveghere în legătură cu prelucrarea datelor personale pe Internet, întrucât nu au obținut soluționarea cererilor lor direct de la operatori (instanțe judecătorești sau societăți comerciale), ceea ce a impus intervenția Autorității de supraveghere pentru respectarea drepturilor acestora de către operatori. În urma investigațiilor efectuate, operatorii au fost sancționați; de asemenea, li s-a recomandat, după caz, de a notifica prelucrările de date cu caracter personal realizate și de a respecta drepturile persoanelor vizate prevăzute de Legea nr. 677/2001, inclusiv a drepturilor de informare, intervenție și opoziție.

În situațiile în care s-a impus, președintele Autorității naționale de supraveghere a emis decizii administrative de ștergere a datelor cu caracter personal publicate ilegal pe Internet.

FIȘĂ DE CAZ

O petentă a reclamat că pe un anumit site, administrat de o societate comercială care colectează automat date din dosarele publicate pe portalul instanțelor judecătorești, au fost publicate datele sale cu caracter personal (nume și prenume) și anumite informații rezultând din calitatea de parte în dosare ale instanțelor de judecată, fără acordul său.

În urma unei căutări simple (pe baza numelui și a prenumelui) realizate atât pe site-ul reclamat, cât și pe motorul de căutare Google, au rezultat informații cu privire la petentă: nume, prenume, obiectul dosarului în care este parte, instanța, secția, ședința, completul, părțile implicate, soluția.

Petenta s-a adresat cu o plângere operatorului, exercitându-și dreptul de opoziție și solicitând ștergerea datelor sale personale de pe site-ul respectiv. Operatorul nu a șters datele

petentei și i-a comunicat acesteia că, în măsura în care datele sale vor fi eliminate din cadrul portalului instanțelor de judecată, acestea nu se vor mai regăsi nici în site-ul reclamat.

Față de constatări, operatorului reclamat i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001, întrucât operatorul nu a șters de pe site datele petentei, în urma exercitării de către aceasta a dreptului de opoziție și nu a asigurat informarea petentei conform art. 12 din Legea nr. 677/2001.

Totodată, președintele Autorității naționale de supraveghere a emis o decizie de ștergere a datelor personale ale petentei de pe site-ul reclamat, decizie respectată de operator.

b) "Dreptul de a fi uitat"

Urmare a Hotărârii Curții de Justiție a Uniunii Europene (CJUE) din 13 mai 2014, pronunțată în cauza Google Spain SL, Google Inc. împotriva Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12), decizie „reper” în domeniul protecției datelor personale, mai mulți petenți au sesizat Autoritatea națională de supraveghere în legătură cu ștergerea datelor lor cu caracter personal de pe site-uri indexate pe motorul de căutare Google, întrucât cererile adresate Google Inc. nu au fost soluționate favorabil. În cazurile cărora le erau aplicabile prevederile Legii nr. 677/2001 în sensul în care au fost interpretate dispozițiile Directivei 95/46/CE de către CJUE în această cauză, la solicitarea Autorității naționale de supraveghere, Google Inc. a eliminat din lista de căutări adresele URL menționate de către petenți. În situațiile sesizate de petenți în care informațiile publicate pe Internet și indexate de Google erau legate de rolul pe care aceștia îl aveau în viața publică, petițiile nu au fost considerate admisibile, motiv pentru care nu s-au efectuat investigații.

Decizia CJUE menționată mai sus a fost pronunțată ca urmare a unei trimeri preliminare adresate de o instanță națională din Spania în cadrul unei dispute între Google și autoritatea de protecție a datelor din Spania (Agencia Espanola de Proteccion de Datos, AEPD).

Decizia CJUE stabilește faptul că este necesar, în principiu, ca motoarele de căutare să elimine conexiunile dintre rezultatele unei căutări și o pagină web dacă aceasta din urmă conține informații despre care persoana vizată consideră că ar trebui să „fie uitate”. Astfel, potrivit Deciziei CJUE:

- activitatea unui motor de căutare (care constă în găsirea informațiilor publicate sau introduse pe Internet de către terți, indexarea acestora în mod automat și stocarea lor temporară și, în cele din urmă, punerea acestora la dispoziția utilizatorilor de Internet într-o anumită ordine de preferință) trebuie calificată drept prelucrare a datelor cu caracter personal, în temeiul prevederilor art. 2 lit. (b) din Directiva 95/46/CE;

- operatorul acestui motor de căutare trebuie considerat „operator”, în sensul art. 2 lit. (d) din Directiva 95/46/CE;

- în cazul în care operatorul unui motor de căutare înființează într-un stat membru o sucursală sau o filială destinată promovării și vânzării spațiului publicitar de pe pagina acestui motor, a cărei activitate este orientată către locuitorii aceluși stat membru, atunci se consideră că prelucrarea datelor cu caracter personal este efectuată în cadrul activităților unui operator cu sediul pe teritoriul respectivului stat membru, în sensul prevederilor art. 4 alin. (1) lit. (a) din Directiva 95/46/CE;

- pentru respectarea drepturilor prevăzute de art. 12 lit. (b) și art. 14 primul paragraf lit. (a) din Directiva 95/46/CE (dreptul de intervenție și de ștergere), operatorul unui motor de căutare este obligat să elimine de pe lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele unei persoane, link-urile către paginile web publicate de terți și care conțin informații referitoare la respectiva persoană;

- art. 12 lit. (b) și art. 14 primul paragraf lit. (a) din Directiva 95/46/CE trebuie interpretate în sensul că operatorul unui motor de căutare trebuie să examineze în special dacă persoana vizată are dreptul ca informația respectivă referitoare la persoana sa să nu mai fie, în stadiul actual, asociată cu numele său de o listă de rezultate, afișată în urma unei căutări efectuate plecând de la numele său. Întrucât persoana vizată poate, având în vedere drepturile sale fundamentale prevăzute la articolele 7 și 8 din Carta Drepturilor Fundamentale a UE (dreptul la viață privată, dreptul la protecția datelor cu caracter personal), să solicite ca informația în cauză să nu mai fie pusă la dispoziția marelui public prin intermediul includerii sale într-o asemenea listă de rezultate, aceste drepturi prevalează în principiu nu numai asupra interesului economic al operatorului motorului de căutare, ci și asupra interesului publicului de a avea acces la informația respectivă cu ocazia unei căutări referitoare la numele acestei persoane. Nu aceasta ar fi însă situația dacă ar reieși că, din motive speciale, precum rolul jucat de persoana

respectivă în viața publică, ingerința în drepturile sale fundamentale este justificată de interesul preponderent al publicului menționat de a avea acces, prin intermediul acestei includeri, la informația în cauză.

Raportat la această situație, pe 26 noiembrie 2014, Grupul de Lucru Art. 29, din care face parte și Autoritatea națională de supraveghere, a adoptat „Ghidul pentru aplicarea Hotărârii Curții de Justiție a Uniunii Europene privind ”Google Spania și INC v. Agencia Española de Protección de Datos (AEPD) Mario Costeja Gonzales” C-131/12”. Conform acestui document, autoritățile de supraveghere nu sunt competente să intervină în cazul în care informațiile referitoare la petiționar, rezultate în urma utilizării unui motor de căutare, reprezintă fapte de competența poliției sau instanțelor de judecată. Autoritățile de supraveghere vor putea interveni însă în cazul pronunțării unei hotărâri judecătorești prin care respectiva faptă a fost considerată ca fiind infracțiune, spre exemplu calomnie sau insultă. De asemenea, autoritățile de supraveghere nu pot interveni dacă informațiile referitoare la petiționar reprezintă opinii personale ale persoanei care le-a postat pe Internet, fapt care intră sub incidența libertății de exprimare.

Decizia CJUE din 13 mai 2014 afirmă, de fapt, existența „dreptului de a fi uitat”, utilizând o interpretare a prevederilor actuale ale Directivei 95/46/CE.

Dreptul de a fi uitat este prevăzut în mod expres de propunerea de regulament înaintată de Comisia Europeană în anul 2012 și care va înlocui actuala Directivă 95/46/CE.

FIȘĂ DE CAZ

O petentă a sesizat faptul că imaginea sa a fost colectată de pe propriul blog și prelucrată ilegal pe o pagină de Internet de unde nu poate fi ștearsă.

Petenta s-a adresat Google Inc. cu solicitarea de eliminare din lista de căutări a respectivei adrese URL, însă nu s-a dat curs solicitării sale pe motiv că materialul de la adresa indicată de petentă a fost plasat în mod deliberat de către aceasta în sfera publică, recomandându-i să se adreseze autorității naționale pentru protecția datelor, în cazul în care este nemulțumită de răspunsul primit, cu menționarea numărului de referință primit.

Având în vedere Decizia CJUE din cauza Costeja din 13 mai 2014, s-a efectuat o investigație prin transmiterea unei solicitări către Google Inc. de a da curs cererii petentei, considerată a fi întemeiată.

În urma demersurilor întreprinse de Autoritatea de supraveghere la Google Inc., adresa URL menționată de petentă a fost eliminată din lista de căutări.

c) Alte cazuri de dezvăluire a datelor personale pe Internet

Alte cazuri sesizate Autorității naționale de supraveghere, având obiect similar, au privit dezvăluirea datelor cu caracter personal fie pe pagini web aparținând unor societăți comerciale sau alte entități de drept privat, fie de către persoane fizice pe bloguri personale.

FIȘĂ DE CAZ

Un petent a reclamat faptul că pe un blog aparținând unui sindicat sunt publicate în continuare datele sale cu caracter personal (nume, prenume, adresă și număr de telefon personale), deși a solicitat ștergerea acestora.

Petentul s-a adresat sindicatului cu o solicitare de ștergere a datelor sale de pe respectivul blog, exercitându-și dreptul de intervenție, însă operatorul a refuzat să dea curs cererii pe motiv că datele respective sunt date de identificare publice ale unui agent economic (persoană fizică autorizată) și se regăsesc pe pagina web a Ministerului Finanțelor Publice.

O simplă căutare cu ajutorul motorului Google (pe baza numelui și prenumelui petentului) a condus la articolul publicat pe site-ul reclamat și respectiv la datele indicate de petent.

În urma investigației, față de scopul jurnalistic urmărit de sindicat prin publicarea pe blog a articolului care cuprinde date cu caracter personal ale petentului, s-a considerat excesivă prelucrarea datelor acestuia referitoare la adresa de domiciliu și numărul său de telefon.

De asemenea, s-a considerat că operatorul a încălcat dreptul de intervenție al petentului, întrucât nu a luat măsuri de ștergere a datelor personale ale acestuia, în urma solicitării scrise.

În urma constatărilor, operatorului i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001.

Totodată, președintele Autorității naționale de supraveghere a emis o decizie de ștergere a datelor personale ale petentului de pe blogul reclamat, decizie respectată de către operator.

5. Nerespectarea drepturilor de acces, intervenție și opoziție

Față de anii anteriori, s-a înregistrat o creștere semnificativă a plângerilor și sesizărilor având ca obiect prelucrarea datelor personale în contextul nerespectării drepturilor persoanelor vizate (în special, a drepturilor de acces, intervenție și opoziție), ca urmare a exercitării acestora, fie ca urmare a constatării faptului că unii operatorii nu cunosc și nu respectă dispozițiile legale aplicabile, fie întrucât aceștia le ignoră cu bună-știință.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o bancă, reclamând că aceasta i-a încălcat dreptul de acces, deoarece nu i-a furnizat toate informațiile solicitate prin cererea adresată. Astfel, petentul solicitase să i se precizeze dacă datele sale personale au fost accesate într-o perioadă anume de către angajații unei sucursale a băncii, care erau persoanele care au accesat aceste date, precum și scopul accesării.

Banca a precizat printr-un răspuns evaziv că datele personale ar fi putut fi vizualizate de toți angajații agenției respective, sub rezerva păstrării secretului profesional, prelucrarea acestora fiind și în scopul optimizării produselor bancare.

Autoritatea națională de supraveghere a constatat că răspunsul formulat era lacunar, în contradicție cu prevederile art. 13 din Legea nr. 677/2001, care prevede faptul că operatorul este obligat ca, în situația în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia o serie de informații, printre altele referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele.

La finalul controlului, operatorul a fost sancționat contravențional pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, punându-i-se în vedere să reformuleze un răspuns complet către petent.

FIȘĂ DE CAZ

Un petent a sesizat faptul că un spital privat i-a încălcat dreptul de acces la datele sale cu caracter personal, deoarece nu i-a furnizat, potrivit art. 13 din Legea nr. 677/2001, informațiile cu caracter personal privind starea de sănătate și documentele ce conțineau aceste informații din dosarul medical, pe care operatorul le-a prelucrat pe perioada spitalizării, cât și informații referitoare la prelucrarea imaginii în blocul operator, ca urmare a unei intervenții chirurgicale avute de acesta în cadrul spitalului.

În acest context, operatorul a comunicat un răspuns care preciza că datele cu caracter personal sunt arhivate și clasificate conform legii, eliberându-se numai la solicitarea organelor de drept și nu sunt supuse accesului public.

Petentul făcuse o solicitare relativ similară în urmă cu doi ani, pentru care s-a adresat cu plângere la Autoritatea națională de supraveghere care a amendat la data respectivă operatorul.

Ca atare, în anul 2014 petentul s-a adresat din nou cu plângere, invocând încălcarea dreptului de acces. Având în vedere că la data efectuării controlului, spitalul nu a putut face, din nou, dovada transmiterii unui răspuns în sensul prevederilor art. 13 din Legea nr. 677/2001, fiind la a două abatere în acest caz, Autoritatea națională de supraveghere a aplicat o sancțiune contravențională pentru fapta prevăzută de art. 32 din Legea 677/2001, într-un quantum crescut.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001, de către o societate civilă profesională de executori judecătorești, în sensul că nerespectării dreptului de intervenție prevăzut de art. 14 și dreptului de opoziție prevăzut de art. 15 din Legea nr. 677/2001, ca urmare a dezvăluirii datelor sale, inclusiv a CNP-ului, pe site-ul acestei societăți. Printr-o cerere scrisă, petentul a solicitat ca, în termen de 15 zile, să i se șteargă și/sau să i se

blocheze și/sau să i se transforme în date anonime datele sale cu caracter personal: nume actual, nume în

Cu ocazia efectuării controlului, operatorul a pus la dispoziție două documente susținând că, odată cu un „proces-verbal de înmânare” legat de dosarul de executare, s-a depus în cutia poștală de la adresa de domiciliu, o adresă de răspuns cu privire la exercitarea dreptului de intervenție.

Un fapt semnalat în cursul efectuării controlului a fost acela că adresa prin care operatorul a răspuns la solicitarea petentului, prin care aceasta își exercita dreptul de intervenție, avea același număr de înregistrare ca și cel al dosarului de executare și nu un număr de înregistrare distinct, în contextul în care cererea petentului avea alt obiect decât cel privind dosarul de executare și un temei legal distinct în baza căreia a fost depusă.

Astfel, adresa de răspuns invocată conținea precizări despre utilizarea CNP-ului acesteia în actele de executare, precum și faptul că publicația de vânzare a fost publicată pe pagina web a Uniunii Naționale a Executorilor Judecătorești din România, conform prevederilor Legii nr. 188/2000 și pe site-ul societății de executori, conform art. 838 din Codul de procedură civilă, însă răspunsul nu conținea toate informațiile solicitate de petent.

Autoritatea națională de supraveghere a reținut că dispozițiile din Codul de procedură civilă privind publicitatea vânzării nu prevăd și publicarea CNP-ului. Totodată, s-a arătat că datele personale având funcție de identificare, precum CNP și seria și numărul actului de identitate, se prelucrează numai cu respectarea dispozițiilor art. 8 din Legea nr. 677/2001. În aplicarea dispozițiilor privind prelucrarea codului numeric personal din Legea nr. 677/2001, instituția noastră a emis Decizia nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală. Astfel, prelucrarea acestor date poate fi efectuată numai dacă persoana vizată și-a dat în mod expres consimțământul sau prelucrarea este prevăzută în mod expres de o dispoziție legală, ori, în alte cazuri, cu avizul Autorității naționale de supraveghere și numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

La finalul controlului, operatorul a fost sancționat contravențional pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, pentru încălcarea prevederilor legale referitoare la dreptul de intervenție și prelucrarea excesivă, respectiv, fără temei legal, a datelor personale.

6. Nerespectarea măsurilor de securitate și confidențialitate a prelucrării datelor personale

În cursul anului 2014, Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că au fost încălcate măsurile de securitate și confidențialitate a datelor cu caracter personal colectate de unii operatori prin intermediul actelor și contractelor încheiate (regii autonome, societăți de recuperare creanțe, furnizori de servicii, operatori de telefonie, instituții publice), ca urmare a neglijenței manifestate în manipularea unor documente sau a neadoptării cerințelor minime de securitate care să prevină dezvăluirea neautorizată a datelor personale.

În urma investigațiilor efectuate, s-a constatat că unii operatori nu au aplicat măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, date colectate prin diverse documente întocmite în derularea activității curente a operatorilor.

FIȘĂ DE CAZ

Prin plângerile înregistrate la Autoritatea națională de supraveghere, trei petenți au sesizat faptul că o regie autonomă le-a dezvăluit datele cu caracter personal fără consimțământul lor. Petenții au susținut că au depus la regia autonomă respectivă petiții on-line în care au menționat numele și prenumele, codul numeric personal, domiciliul, numărul de telefon, adresa de e-mail și locul de muncă prin intermediul formularului electronic, în care semnalau o serie de probleme existente la o altă regie autonomă unde erau angajați. Aceste petiții au intrat în posesia colegilor lor de muncă, având menționate pe ele inclusiv numărul de înregistrare de la regia autonomă la care s-au făcut reclamațiile, care ulterior, le-au postat pe un grup de socializare pe Internet (Facebook). Divulgarea datelor personale și a informațiilor legate de reclamațiile petenților le-au produs prejudicii de imagine, unul dintre ei fiind nevoit să ceară demisia de la locul de muncă.

În urma investigației efectuate la regia autonomă la care s-au depus petițiile, operatorul a fost sancționat pentru contravenția prevăzută de art. 33 din Legea nr. 677/2001, întrucât nu a prezentat suficiente dovezi din care să rezulte că a aplicat, până la data efectuării investigației, măsuri tehnice și organizatorice adecvate, inclusiv sub aspectul instrucțiunilor date

propriilor angajați, care să prevină dezvăluirea sau accesul neautorizat la dosarele personale ale petiționarilor din reclamațiile gestionate în activitatea de inspecție și control.

Demersurile au continuat ulterior la angajatorul petenților, care a fost sancționat contravențional pentru contravenția prevăzută de art. 33 din Legea nr. 677/2001, întrucât operatorul nu a prezentat suficiente dovezi din care să rezulte că a aplicat, până la data efectuării investigației, măsuri tehnice și organizatorice adecvate, inclusiv sub aspectul instrucțiunilor date persoanelor ce acționează sub autoritatea sa, prin care să prevină dezvăluirea datelor angajaților, în speță, diseminarea datelor petenților conținute în sesizările adresate către un terț și care au ajuns în posesia angajaților operatorului sancționat.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o societate de recuperare creanțe, susținând că i-a fost încălcat dreptul de opoziție, întrucât societatea nu a încetat prelucrarea datelor sale personale, respectiv numărul său de telefon, deși nu a dat acceptul societății pentru a-i utiliza datele personale, cu toate că s-a adresat acesteia în scris.

În cadrul investigației efectuate în acest caz, reprezentantul operatorului a declarat faptul că nesoluționarea cererii petentului se datorează faptului că, după primirea ei la secretariatul societății, cererea a fost pierdută și nu a mai fost înregistrată în registrul intern.

Față de această situație, operatorul a fost sancționat contravențional pentru săvârșirea contravenției prevăzute de art. 33 din Legea nr. 677/2001, deoarece nu a aplicat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva pierderii cererii petentului, care conținea datele sale personale, astfel cum ar fi avut obligația potrivit art. 20 din Legea 677/2001.

În același timp, societatea a luat măsuri pentru a nu mai fi utilizat numărul de telefon al petentului, acesta nemaifiind prezent în baza sa de date.

FIȘĂ DE CAZ

Petentul a semnalat că s-a prezentat la un magazin de desfacere aparținând unui operator de servicii de telefonie mobilă cu un telefon personal achiziționat, pe care l-a lăsat în service, deoarece necesita reparații. În schimbul telefonului său, petentul a primit provizoriu un alt telefon, pe care să îl folosească pe perioada în care telefonul său era supus intervenției tehnice.

Potentul a constatat faptul că în memoria telefonului primit provizoriu se află date cu caracter personal de la utilizatori precedenți: logare automată pe Facebook, numere de telefon și mesaje personale, inclusiv balanța conturilor bancare. Urmare a acestei situații, petentul a sesizat operatorul de telefonie, însă a precizat că sesizarea sa nu a fost luată în considerare.

În urma investigației efectuate de Autoritatea națională de supraveghere în acest caz, operatorul a fost sancționat pentru săvârșirea contravenției prevăzute de art. 33 din Legea nr. 677/2001, respectiv pentru neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, care ar fi putut să prevină astfel de incidente ce conduc la dezvăluirii neautorizate de date personale.

7. Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

În cursul anului 2014, s-a menținut numărul mare al plângerilor și sesizărilor având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (SMS) sau prin poșta electronică. Majoritatea acestora au privit aspecte legate de protecția vieții private în sectorul comunicațiilor electronice prin primirea de mesaje comerciale nesolicitate prin poșta electronică, fără consimțământul expres și neechivoc al destinatarului în acest sens.

Pentru soluționarea plângerilor considerate admisibile, Autoritatea națională de supraveghere a efectuat o serie de investigații pentru a verifica existența consimțământului persoanei vizate de a primi mesaje comerciale pe adresa sa de poșta electronică sau prin SMS. În unele cazuri investigate, s-a constatat că expeditorii mesajelor comerciale nu au respectat prevederile legale sub aspectul obținerii consimțământului prealabil și al respectării opțiunii persoanelor vizate de a nu mai primi mesaje comerciale nesolicitate. Astfel, în multe situații, s-a

constatat faptul că operatorii au continuat să trimită mesaje cu caracter comercial chiar și după ce persoanele vizate și-au exercitat dreptul de opoziție.

FIȘĂ DE CAZ

O petentă a reclamat faptul că a primit un mesaj comercial nesolicitat pe adresa personală de e-mail din partea unei bănci, în conținutul căruia era promovat un produs al acelei bănci.

Petenta s-a adresat în prealabil băncii, solicitând informații privind sursa de unde a fost obținută adresa sa de e-mail, scopul prelucrării și destinatarii acestei date personale, însă a fost nemulțumită de răspunsul primit.

Banca a transmis un răspuns pe e-mail petentei prin care îi comunica că, în urma celor semnalate de aceasta, au fost luate toate măsurile care se impuneau în ceea ce privește transmiterea materialelor publicitare prin e-mail și că pe viitor nu va mai primi mesaje publicitare prin e-mail. Petentei nu i s-a răspuns însă și la celelalte solicitări cu privire la sursa de colectare a adresei de e-mail și destinatarii acestei date cu caracter personal.

În urma investigației efectuate, s-a constatat faptul că nu s-a obținut consimțământul expres al petentei pentru transmiterea de mesaje comerciale, deoarece banca a apreciat că mesajul transmis nu avea caracter comercial, ci informațional, prin care i-au adus la cunoștință acesteia avantajele cu privire la funcționarea produselor băncii. De asemenea, din verificări, a reieșit și faptul că petentei nu i-au fost comunicate toate informațiile solicitate, respectiv sursa de unde a fost obținută adresa sa de e-mail, scopul prelucrării și destinatarii acestei date personale.

Față de constatări, operatorului reclamat i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001 și a Legii nr. 506/2004, întrucât i-a transmis petentei, pe adresa sa de e-mail, o comunicare comercială fără a avea consimțământul său expres prealabil și nu i-a comunicat toate informațiile solicitate.

În baza constatărilor, a mai rezultat faptul că banca nu a inclus în contractul încheiat cu societatea împuternicită pentru trimiterea de mesaje comerciale prin poșta electronică clauzele prevăzute de art. 20 alin. (5) din Legea nr. 677/2001 (stabilirea de instrucțiuni privind prelucrarea datelor personale și aplicarea măsurilor de securitate de către persoana

împuternicită), fapt pentru care s-a aplicat o sancțiune contravențională cu amendă și în temeiul art. 33 din Legea nr. 677/2001.

FIȘĂ DE CAZ

Un petent a reclamat faptul că a primit mai multe mesaje comerciale nesolicitate de tip SMS de la un operator de telefonie mobilă, deși și-a exercitat anterior dreptul de opoziție cu privire la prelucrarea numărului său de telefon în scop de marketing printr-o cerere înaintată operatorului. Ulterior acestei cereri, petentul a primit un răspuns prin care era informat că operatorul va lua măsurile necesare astfel încât acesta să nu mai primească mesaje promoționale pe numărul său de telefon mobil.

Ulterior acestui răspuns, societatea i-a mai transmis petentului un mesaj comercial de tip SMS, motivând prin faptul că actualizarea datelor în sistemul informatic cu menționarea modificărilor apărute în contul unui client poate dura până la 14 zile. Câteva luni mai târziu, operatorul a mai trimis un mesaj cu caracter comercial de tip SMS petentului, de această dată invocând faptul că acest mesaj a fost trimis de o societate parteneră care nu are acces la baza de date a operatorului, motiv pentru care nu are actualizate informațiile referitoare la solicitarea petentului de a nu mai primi mesaje comerciale.

Față de constatări, operatorului reclamat i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001 și a Legii nr. 506/2004, întrucât i-a transmis petentului, prin SMS, mai multe comunicări comerciale, fără a avea consimțământul expres prealabil al acestuia (conform opțiunii negative exprimate printr-o cerere adresată societății), încălcând astfel prevederile art. 32 coroborat cu art. 15 din Legea nr. 677/2001 și ale art. 12 din Legea nr. 506/2004.

FIȘĂ DE CAZ

O petentă a reclamat faptul că a primit pe adresa sa de e-mail două mesaje comerciale nesolicitate de la o societate comercială, deși nu s-a abonat niciodată pentru primirea de newsletter-e din partea societății. Ca urmare a mesajului comercial nesolicitat primit pe adresa sa de e-mail, petenta s-a adresat operatorului prin intermediul poștei electronice, conform informațiilor existente la secțiunea „Termeni și condiții” de pe site-ul acestuia, cu solicitarea de

a i se comunica sursa adresei sale de e-mail și de a i se șterge respectiva adresă din baza de date. Operatorul i-a transmis un e-mail petentei prin care i-a comunicat sursa adresei sale de e-mail.

Ulterior, petenta s-a adresat din nou operatorului, prin poșta electronică, solicitând să i se confirme ștergerea adresei sale de e-mail din baza de date a operatorului, însă nu a primit niciun răspuns la cererea sa și, în plus, a primit un nou mesaj comercial nesolicitat de la același operator.

În timpul investigației efectuate la societatea reclamată, s-a constatat faptul că pe site-ul acesteia exista o rubrică (abonare la newsletter) care oferea posibilitatea persoanelor fizice să furnizeze adresa de e-mail pentru a primi ulterior diverse oferte. Adresa de e-mail a petentei a fost preluată în baza de date destinată transmiterii de newsletter-e în urma solicitării acesteia de a primi o ofertă concretă de achiziționare a unor produse.

La cererea petentei de a i se șterge adresa de e-mail din baza de date, societatea a făcut demersuri pentru eliminarea acesteia din sistemul de evidență propriu, dar nu i-a transmis și un răspuns în acest sens. Ulterior solicitării, petenta a primit mai multe comunicări comerciale nesolicitate prin e-mail. Reprezentanții societății au declarat în timpul investigației că acest fapt s-a datorat unei erori umane, un angajat preluând adresa de e-mail a petentei din inbox-ul căsuței de e-mail a societății, de unde nu fusese ștersă.

Față de constatări, operatorului reclamat i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001 și a Legii nr. 506/2004, întrucât i-a transmis petentei prin poșta electronică mai multe comunicări comerciale, fără a avea consimțământul expres prealabil al acesteia.

CAPITOLUL AL V-LEA

ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE

Una dintre atribuțiile Autorității naționale de supraveghere este de a asigura o cooperare activă la nivel internațional, reglementată prin art. 21 alin. (3) litera k) din Legea nr. 677/2001, care prevede că instituția noastră „cooperează cu autoritățile similare de peste hotare în vederea asistenței mutuale, precum și cu persoanele cu domiciliul sau cu sediul în străinătate, în scopul apărării drepturilor și libertăților fundamentale ce pot fi afectate prin prelucrarea datelor cu caracter personal”.

Cooperarea la nivel internațional în domeniul protecției datelor reprezintă unul din obiectivele Autorității naționale de supraveghere, în special în ceea ce privește schimbul de experiență și stabilirea unor bune practici. Colaborarea pe plan extern se realizează prin participarea la grupuri de lucru, conferințe și seminarii și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei, în domeniul protecției datelor cu caracter personal, precum și prin implicarea în activitatea desfășurată în cadrul acestora.

Grupul de Lucru Articolul 29

Aspectele dezbătute în cadrul reuniunilor Grupului de Lucru Articolul 29 și a subgrupurilor sale sunt esențiale pentru a stabili bune practici și mecanisme, respectiv de asigurare a unor instrumente adecvate în ceea ce privește aplicarea legislației în domeniul protecției datelor. Activitatea în Grupului de Lucru Articolul 29 și a subgrupurilor sale pe anul 2014 s-a finalizat prin adoptarea de opinii privind:

- aplicarea principiului proporționalității și principiului necesității în sectorul polițienesc. Opinia are drept scop clarificarea noțiunilor de necesitate și de proporționalitate și aplicarea acestora în cazul măsurilor existente sau propuse în vederea soluționării unor probleme în contextul asigurării respectării legii la mai multe niveluri – local/regional, național sau european;
- privind cerințele pentru regulile corporatiste obligatorii prezentate autorităților naționale de protecție a datelor din Uniunea Europeană și pentru regulile transfrontaliere

privind protecția vieții private prezentate agențiilor APEC cu responsabilități în materie de CBPR. Acest document identifică cerințele comune sau similare pentru regulile corporatiste obligatorii, astfel cum sunt autorizate de obicei de către autoritățile naționale de protecție a datelor din Uniunea Europeană pentru transferurile de date cu caracter personal în afara Uniunii Europene, însă în cadrul unui grup multinațional, precum și pentru sistemul de reguli transfrontaliere privind protecția vieții private al Organizației de Cooperare Economică Asia-Pacific;

- notificarea încălcărilor securității datelor cu caracter personal. În timp ce notificarea autorității competente este necesară pentru toate cazurile de încălcare a securității datelor în conformitate cu Directiva 2002/58/CE. Această opinie analizează cazurile de încălcare a securității datelor cu caracter personal care necesită notificarea persoanelor vizate și prezintă măsurile pe care operatorii ar fi putut să le adopte în cadrul punerii în aplicare a sistemului lor pentru a evita încălcarea securității datelor cu caracter personal sau, cel puțin, măsurile care ar fi putut să fie puse în aplicare de la început pentru a scuti operatorul de la notificarea persoanelor vizate.

- supravegherea comunicațiilor electronice în scopul colectării de date operative și al asigurării securității naționale;

- tehnicile de anonimizare. Anonimizarea este descrisă ca o tehnică aplicată datelor cu caracter personal în vederea eliminării ireversibile a posibilității de identificare. În acest context, Grupul de Lucru Articolul 29 a concluzionat, prin adoptarea avizului, că „datele anonimizate ar trebui, în consecință, să fie date anonime care s-au referit anterior la o persoană identificabilă pentru care identificarea nu mai este însă posibilă”;

- noțiunea de interes legitim al operatorului potrivit art. 7 din Directiva 95/46/CE. Documentul analizează criteriile stabilite prin art. 7 din Directiva 95/46/CE astfel încât respectiva prelucrare de date să fie legală și oferă îndrumări cu privire la modalitatea de aplicare a art. 7 (f) potrivit cadrului legal actual. Art. 7 (f) reprezintă ultimul temei legal pentru prelucrare legală de date personale. În fapt, necesită un echilibru între interesul legitim al operatorului sau al terților către care vor fi dezvăluite datele și interesul sau drepturile fundamentale ale persoanei vizate.

- evoluțiile recente privind Internetul lucrurilor. Internetul Lucrurilor reprezintă un sistem interoperabil care implică sisteme de conexiune la internet, aplicațiile de la nivelul telefoanelor inteligente, sisteme de frecvență. Astfel, respectivul aviz a încercat să definească

aria de aplicabilitate a sistemelor ce utilizează o conexiune la Internet, modul de folosire a datelor cu caracter personal, precum și respectarea principiului de privacy by design;

- aplicarea Directivei 2002/58/CE în ceea ce privește dispozitivele de amprentare.

Comitetul Consultativ al Consiliului Europei T-PD

La nivelul Comitetul Consultativ T-PD al Consiliului Europei au continuat discuțiile privind revizuirea Convenției Consiliului Europei pentru protecția persoanelor cu privire la procesarea automată a datelor personale, adoptată la Strasbourg, la 28 ianuarie 1981, inclusiv Protocolul Adițional la Convenție privind autoritățile de supraveghere și transferul datelor personale în state terțe.

În acest sens, în conformitate cu art. 17 din Statutul Consiliului Europei și în conformitate cu Rezoluția CM/Res (2011) 24 privind comitetele interguvernamentale și organismele subordonate, Comitetul de Miniștri a înființat comitetul ad hoc CAHDATA. Comitetul de Miniștri a mandatat comitetul CAHDATA să finalizeze și să transmită Comitetului de Miniștri propunerile pentru modernizarea Convenției 108, ținând cont de propunerile elaborate de Comitetul Consultativ al Convenției 108.

Grupul de Supraveghere Comună VIS, SIS II, Eurodac

În cadrul reuniunilor Grupului de Supraveghere Comună în domeniul VIS, SIS II și Eurodac sunt analizate implicațiile Regulamentului (CE) nr. 767/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 privind Sistemul de informații privind vizele (VIS) și schimbul de date între statele membre cu privire la vizele de scurtă ședere, ale Deciziei 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II), precum și ale Regulamentului Consiliului nr. 2725/2000 din 11 decembrie 2000, privind instituirea sistemului „Eurodac” pentru compararea amprentelor în scopul aplicării eficiente a Convenției de la Dublin (ce va fi înlocuit, începând cu data de 20 iulie 2015, de Regulamentul nr. 603/2013) asupra domeniului protecției datelor și politicilor de supraveghere, precum și stabilirea pe termen lung a planului de acțiune la nivelul grupului.

Membrii grupului împărtășesc informații relevante cu privire la investigațiile efectuate la nivel național în legătură cu sistemul VIS, SIS II și Eurodac în diferite state membre, subiectele

abordate împreună cu reprezentanții Comisiei Europene și cei ai noii Agenției IT a Uniunii Europene - LISA (EU Agency for large-scale IT systems) vizând, în special, situația actuală a VIS, dar și evoluții recente care includ, printre altele, calitatea datelor alfanumerice și biometrice.

Totodată, în cadrul Grupurilor au loc discuții cu privire la necesitatea de a dezvolta un cadru normativ comun pentru inspecții, posibilitatea de a efectua investigații comune pentru statele care eliberează vize împreună în mai multe state terțe, precum și cu privire la fezabilitatea unui format similar de investigații care să fie efectuate în scopul auditării altor sisteme informatice de mari dimensiuni (Eurodac și SIS II).

Organismul comun de control în domeniul Europol și Vămi

Modificarea cadrului legislativ în domeniul cooperării polițienești a reprezentat și în 2014 unul din subiectele aflate pe agenda de lucru a reuniunilor Organismului comun de control Europol (Europol Joint Supervisory Body – JSB Europol). În acest sens, menționăm ca în octombrie 2014 a fost adoptată cea de-a treia opinie privind propunerea de regulament Europol. Acest document abordează trei aspecte majore:

- prelucrarea datelor cu caracter speciale și diferitele categorii de persoane vizate
- dreptul de acces al persoanei vizate
- cooperarea dintre autoritățile pe protecția datelor și Autoritatea Europeană pentru Protecția Datelor (European Data Protection Supervisor - EDPS).

Cea de-a treia analiză confirmă încă o dată concluzia primului aviz și a celui de-al doilea, respectiv faptul că nivelul de protecție a datelor cu caracter personal oferit prin regulament este mai scăzut decât cel garantat în prezent prin Decizia Europol.

Seminar TAIEX privind dezvoltarea unei politici de securitate în contextul protejării datelor cu caracter personal – Chișinău, Republica Moldova

La invitația Comisiei Europene, reprezentanții Autorității naționale de supraveghere au participat la seminarul TAIEX privind elaborarea unei politici de securitatea în contextul protejării datelor cu caracter personal, care a avut loc la Chișinău, Republica Moldova.

Obiectivul acestei reuniuni a fost acela de a asigura un schimb de informații și bune practici privind responsabilitățile operatorilor, luând în considerare ultimele tehnologii și riscurile pe care le prezintă acestea în ceea ce privește prelucrările de date personale.

Seminarul a abordat subiecte cum sunt, spre exemplu, dezvoltarea de politici de securitate, tipuri de riscuri cu care se confruntă operatorii de date, metode de evaluare a costurilor de implementare a politicii de securitate a datelor personale, responsabilitatea operatorului de a asigura securitatea și confidențialitatea datelor personale prelucrate, inclusiv aplicarea de soluții practice pentru asigurarea identificării și autentificării utilizatorilor, soluționarea incidentelor de securitate.

Seminar de cazuistică – Skopje, Macedonia

Seminariile de cazuistică reprezintă o serie de evenimente organizate de autoritățile naționale pe protecția datelor și sunt organizate ca subgrup al Conferinței de primăvară a autorităților pe protecția datelor.

Aceste reuniuni au drept obiectiv schimbul de informații privind aspectele practice la nivel operațional și promovează cooperarea în general la nivel european. Seminarul organizat de Autoritatea pe protecția datelor din Macedonia (Directorate for Personal Data Protection) a abordat teme precum protecția datelor în sistemul judiciar, colectarea excesivă a datelor personale și echilibrul dintre dreptul la protecția datelor și dreptul de acces la informațiile publice, datele biometrice, marketingul și protecția datelor, profilare și protecția datelor, în cadrul cărora reprezentanții autorității de supraveghere au susținut prezentarea privind dezvăluirea datelor cu caracter personal pe portalul instanțelor judecătorești.

Proiectul „Sprijinirea procesului de liberalizare a vizelor în Georgia, prin acordarea de asistență în domeniul protecției datelor cu caracter personal și anti-discriminării”

La invitația adresată de Centrul Român pentru Politici Europene (CRPE), Autoritatea națională de supraveghere a participat la evenimentul de lansare a proiectului „Sprijinirea procesului de liberalizare a vizelor în Georgia prin acordarea de asistență în domeniul protecției datelor cu caracter personal și anti-discriminării”. Acest proiect a fost derulat la inițiativa CRPE, în parteneriat cu Open Society Georgia, fiind susținut de Ministerul Afacerilor Externe (MAE) din

România, în cadrul Politicii de Asistență Oficială pentru Dezvoltare, având ca obiectiv sprijinirea reformei administrative și legislative din Georgia, în conformitate cu standardele europene, prin furnizarea de expertiză și asistență românească în domeniul anti-discriminării și protecției datelor personale.

La acest eveniment au participat din partea României reprezentanți ai CRPE, un expert independent, reprezentanți ai Ministerului Afacerilor Externe, ai Consiliului Național pentru Combaterea Discriminării, precum și ambasadorul României în Georgia. De asemenea, au mai participat reprezentanți ai instituțiilor omoloage din Georgia, precum și reprezentanți ai unor ONG-uri și ai mass-media locale, evenimentul fiind reflectat și în emisiunile televiziunilor din Georgia.

Evenimentul de lansare a fost structurat în două părți principale, respectiv prezentări și discursuri din partea invitaților români și georgieni și workshop-uri dedicate celor două axe de interes: protecția datelor personale și anti-discriminarea în vederea identificării nevoilor și stabilirii cadrului de efectuare a schimbului de experiență în cele două domenii: cadrul instituțional și legal în domeniul protecției datelor personale, principalele obstacole în implementarea cadrului legal și cadrul instituțional și legal în domeniul antidiscriminării, principalele obstacole în implementarea cadrului legal.

Cooperarea cu alte autorități pe protecția datelor

În anul 2014, ca urmare a unor plângeri ale unor cetățeni canadieni privind un operator situat pe teritoriul României, primite de autoritatea pe protecția datelor din Canada, a fost încheiat Memorandumul de înțelegere între Comisarul Pentru Protecția Vieții Private din Canada și instituția noastră, referitor la asistența mutuală în cadrul procesului de aplicare a cadrului normativ privind protecția vieții private în cadrul sectorului privat. Acest protocol de colaborare are drept obiectiv asistența privind aspecte procedurale, investigative sau alte aspecte referitoare la aplicarea trans-frontalieră a cadrului normativ privind protecția vieții private, inclusiv în ceea ce privește aspecte care pot ajuta în cadrul investigațiilor aflate în curs de desfășurare.

Pachetul Frontiere Inteligente

În anul 2013, Comisia a prezentat propuneri pentru un sistem de intrare/ieșire (EES) și pentru un program de înregistrare a călătorilor (RTP) pentru spațiul Schengen, cunoscute în mod generic drept „frontiere inteligente”, respectiv:

- i) Propunere de Regulament al Parlamentului European și al Consiliului de instituire a sistemului de intrare/ieșire (EES) pentru înregistrarea datelor referitoare la intrarea și ieșirea resortisanților țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene,
- ii) Propunere de Regulament al Parlamentului European și al Consiliului de instituire a programului de înregistrare a călătorilor

Cele două propuneri legislative regândesc sistemul de control al frontierelor Schengen pentru perioada 2014-2020, prin dezvoltarea la frontierele externe a unor sisteme de intrare/ieșire (EES) și a unor programe de înregistrare a călătorilor (RTP). Prin aceste propuneri legislative se urmărește atât monitorizarea și centralizarea situației imigranților, cât și identificarea persoanelor care au depășit perioada legală de ședere în Uniunea Europeană.

În acest sens, Autoritatea națională de supraveghere consideră că implementarea unor astfel de sisteme de colectare și prelucrare a datelor prin intermediul sistemului european de intrări/ieșiri (EES) și programul pentru înregistrarea călătorilor (RTP) presupune o prelucrare automatizată pe scară largă a datelor cu caracter personal și poate reprezenta o nouă situație de risc pentru protecția datelor cu caracter personal ale persoanelor fizice și, implicit, respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață privată.

Datele personale ale pasagerilor (PNR)

Autoritatea națională de supraveghere a primit spre avizare proiectul de lege privind utilizarea datelor despre pasageri pentru prevenirea și investigarea actelor de terorism sau asimilate acestora, a infracțiunilor contra securității naționale sau a amenințărilor la adresa securității naționale.

Implementarea unui asemenea sistem implică riscuri în ceea ce privește protecția datelor cu caracter personal ale persoanelor fizice, precum și în legătură cu respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață privată, cu privire la prelucrarea datelor cu caracter personal.

Legalitatea unui asemenea sistem trebuie evaluată având în vedere principiile statuate în Carta drepturilor fundamentale ale UE, în special în art. 7 privind dreptul la viață privată și familială și art. 8 privind protecția datelor personale, două drepturi diferite și complementare, garantate de Cartă, precum și cele ale art. 8 din Convenția pentru apărarea drepturilor și libertăților fundamentale.

Astfel, în concordanță cu jurisprudența Curții Europene a Drepturilor Omului rezultată din încălcarea art. 8 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale, nivelul de protecție oferit de prevederile articolului menționat anterior ar fi diminuat în mod inacceptabil dacă folosirea de tehnici științifice moderne ar fi permisă cu orice preț și fără realizarea unui echilibru între beneficiile folosirii extensive a acestor tehnici și interesele importante legate de viața privată, iar orice stat care pretinde să aibă un rol de pionier în dezvoltarea noilor tehnologii poartă responsabilitatea obținerii unui echilibru corect în această problemă.

În același timp, atragem atenția asupra faptului că principiul necesității și cel al proporționalității respectivului sistem pot fi demonstrate doar după evaluarea funcționalității și utilității sistemelor informatice deja existente la scară largă în cadrul cărora se prelucrează o multitudine de informații.

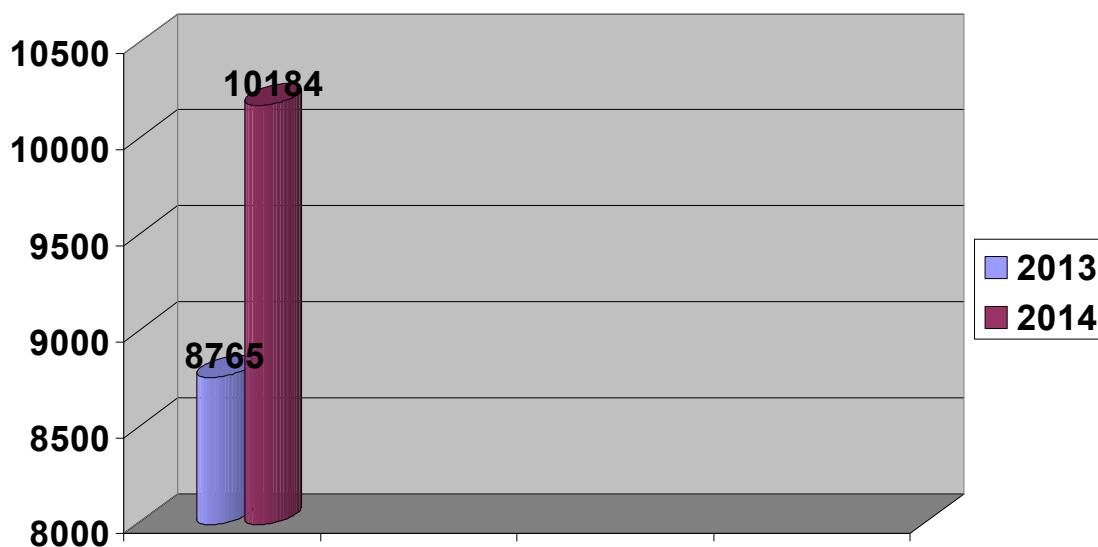
CAPITOLUL AL VI-LEA

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRIILOR DE DATE CU CARACTER PERSONAL

În anul 2014, Autoritatea națională de supraveghere a soluționat **10.184** de solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări și cereri prin care se solicită punctul de vedere sau clarificarea unor aspecte ce țin de prelucrările de date cu caracter personal efectuate de aceștia.

Față de anul anterior, numărul solicitărilor a fost mai mare și cu un grad de complexitate crescut. Astfel, comparativ cu anul 2013, numărul de solicitări înregistrate în anul 2014 a crescut cu aproximativ 15%.

Notificări și cereri



Astfel, în anul 2014, au fost soluționate 8.590 de notificări privind prelucrări de date cu caracter personal, dintre care 7961 efectuate atât pe teritoriul României și 629 transferuri de date către state din Uniunea Europeană, Zona Economică Europeană și state terțe.

Din cele 629 de notificări cu transferuri de date către entități din străinătate, în 537 au fost declarate transferuri către state din Uniunea Europeană, Zona Economică Europeană și din state terțe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entități care au aderat în baza principiilor Safe Harbor), precum și transferuri către state terțe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată și completată.

Totodată, au fost notificate 72 de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, pe baza contractelor cu clauze standard și 20 de transferuri în baza regulilor corporatiste obligatorii (Binding Corporate Rules).

În urma analizării transferurilor de date în străinătate către state terțe, a fost emis un număr de 16 autorizații de transfer, din care 11 pentru transferuri în baza regulilor corporatiste obligatorii (Binding Corporate Rules).

În același timp, au fost analizate 1382 de alte solicitări ale operatorilor privind aspecte referitoare la dispozițiile Legii nr. 677/2001, modificată și completată, rapoarte anuale ale autorităților publice, și au fost emise 212 de puncte vedere.

Secțiunea 1 – Activitatea de înregistrare a prelucrărilor de date

Referitor la prelucrările de date notificate de operatori, în anul 2014, s-a constatat o creștere a numărului operatorilor din domeniul monitorizării/securității persoanelor, spațiilor și/sau bunurilor publice/private, a reclamei, marketingului și publicității și a comerțului on-line.

În funcție de activitatea ce a făcut obiectul prelucrărilor de date notificate, Autoritatea națională de supraveghere a îndrumat operatorii de date, în special cu privire la respectarea prevederilor art. 4, 12, 19 și 20 din Legea nr. 677/2001, modificată și completată. Spre exemplu, s-a recomandat acestora să colecteze de la persoanele vizate doar acele date cu caracter special strict necesare realizării unui scop bine determinat, explicit și legitim, să obțină consimțământului expres al persoanei vizate, dacă nu există prevederi legale care reglementează prelucrarea, precum și să o informeze cu privire la toate drepturile ce îi sunt garantate de Legea nr. 677/2001 și modalitatea concretă prin care acestea pot fi exercitate (care trebuie să fie adecvată mijloacelor de prelucrare a datelor).

Ca și anul precedent, o serie de instituții publice și entități din domeniul privat au notificat, în principal, prelucrările de date efectuate ca urmare a derulării unor proiecte

finanțate din fonduri europene nerambursabile, în cadrul Programului Operațional Sectorial Dezvoltarea Resurselor Umane, Programul Operațional Sectorial Creșterea Competitivității și Programul Operațional Regional.

De asemenea, entități din domeniul privat au notificat Autoritatea națională de supraveghere pentru prelucrările efectuate în scopul comercializării produselor on-line.

În activitatea de monitorizare/securitate a persoanelor, spațiilor și/sau bunurilor publice/private, s-a constatat creșterea numărului asociațiilor de proprietari/locatari care au instalat echipamente de supraveghere video pe căile de acces în imobile.

În plus, ca urmare a intrării în vigoare a Legii nr. 51/2013 pentru modificarea și completarea Ordonanței Guvernului nr. 82/2000 privind autorizarea operatorilor economici care desfășoară activități de reparații și de reconstrucție a vehiculelor rutiere, precum și de dezmembrare a vehiculelor scoase din uz, operatorii economici asigură posibilitatea ca beneficiarul să asiste vizual, prin intermediul unui sistem video, la modul în care sunt executate lucrările de mai sus.

Tot referitor la prelucrarea efectuată prin intermediul echipamentelor de supraveghere video, de subliniat este și aceea realizată de școlile de conducători auto care, pentru examinarea în vederea obținerii permisului de conducere, au obligația de a dota vehiculele utilizate la pregătirea practică cu sistem tehnic de monitorizare video și audio precum și cu un sistem de poziționare globală. Această obligație a fost reglementată prin Ordinul nr. 733/2013 emis de ministrul transporturilor pentru aprobarea Normelor privind autorizarea școlilor de conducători auto și a instructorilor auto, a Normelor privind atestarea profesorilor de legislație rutieră și a instructorilor de conducere auto, a Metodologiei de organizare și desfășurare a cursurilor de pregătire teoretică și practică a persoanelor în vederea obținerii permisului de conducere, a Programei de școlarizare, precum și privind condițiile și obligațiile pentru pregătirea teoretică și practică a persoanelor în vederea obținerii permisului de conducere

Operatorilor de mai sus li s-a solicitat să respecte reglementările legale în vigoare, în special cu privire la îndeplinirea obligației legale prevăzută de art. 12 alin. (1) din Legea nr. 677/2001, modificată și completată, în condițiile reglementate de art. 11 din Decizia nr. 52/2012. De asemenea, aceștia au fost atenționați că trebuie să aibă în vedere faptul că printre măsurile de securitate adoptate trebuie să se regăsească și prevederi din care să rezulte cu claritate faptul că accesarea/utilizarea înregistrărilor video să fie efectuată numai de către

persoane abilitate în acest sens, exclusiv în momentul producerii de incidente ce necesită implicarea organelor competente în domeniu.

Pe de altă parte, în anul 2014, entități din domeniul privat au notificat prelucrarea datelor cu caracter personal ale clienților, acționarilor și administratorilor de companii (nume/prenume, sex, data și locul nașterii, cetățenie, telefon/fax, adresă, e-mail și codul numeric personal) în scopurile rapoarte de credit și rapoarte de analiză financiară.

Este de subliniat faptul că operatorii în speță colectau codul numeric personal din surse publice, de la Registrul Comerțului, respectiv Monitorul Oficial, pe bază de contract cu plată online. Față de această situație, Autoritatea națională de supraveghe a precizat operatorului care sunt condițiile de prelucrare a codului numeric personal al unei persoane vizate în conformitate cu prevederile art. 8 din Legea nr. 677/2001, coroborate cu cele ale Deciziei nr. 132/2011. În plus, s-a adus la cunoștința operatorului faptul că, în cazul în care datele nu sunt obținute direct de la persoana vizată, acesta are obligația de a furniza persoanelor fizice ale căror date le utilizează în momentul colectării datelor sau dacă se intenționează dezvăluirea datelor către terți, cel mai târziu până în momentul primei dezvăluiri, toate informațiile prevăzute la art. 12 alin. (2) din Legea nr. 677/2001, modificată și completată, raportat la circumstanțelor specifice de prelucrare (respectiv modalității de prelucrare a datelor, suportului pe care datele sunt colectate, etc.).

În urma analizării formularelor de notificare, s-a propus efectuarea unor investigații din oficiu pentru verificarea anumitor aspecte referitoare la prelucrarea datelor cu caracter personal, și anume:

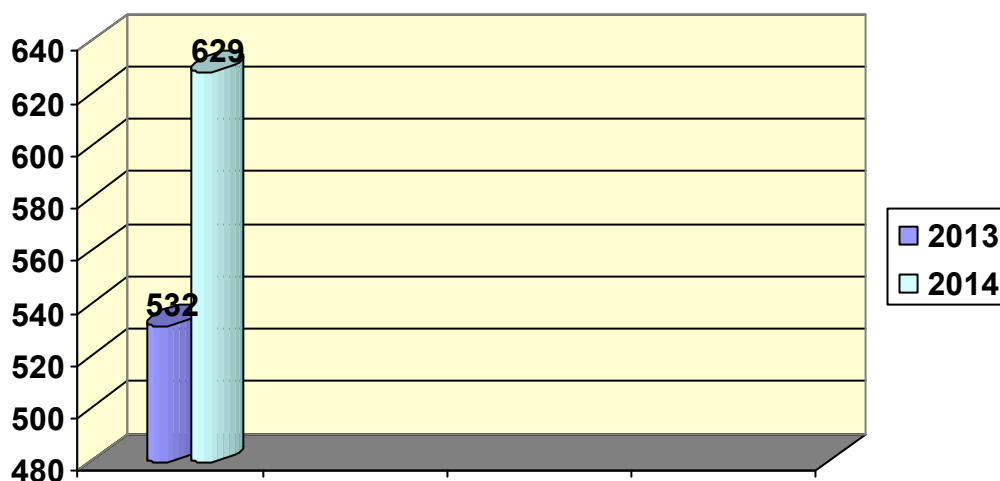
- clarificarea condițiilor de prelucrare a codului numeric personal în scop de reclamă, marketing și publicitate, inclusiv pe pagina de Facebook a operatorului;
- verificarea modalității în care se efectuează prelucrarea datelor cu caracter personal prin utilizarea mijloacelor cloud computing;
- verificarea condițiilor în care se efectuează prelucrarea datelor cu caracter personal având ca scop monitorizarea timpului de utilizare a internetului pe calculatoarele societății folosite de salariați;
- verificarea condițiilor în care se efectuează prelucrarea datelor cu caracter personal, în special codul numeric personal și seria și numărul actului de identitate de către o casă de licitații;

- verificarea condițiilor în care se efectuează prelucrarea și transferul în străinătate al datelor cu caracter personal de către entități de drept privat;
- clarificarea condițiilor în care se realizează prelucrarea datelor biometrice ale angajaților în scopul pontării acestora;
- clarificarea condițiilor în care se realizează prelucrarea datelor cu caracter personal, în special a codului numeric personal în scop de „reclamă, marketing și publicitate, respectiv emiterea cardului de fidelitate.

Secțiunea a 2-a – Transferul datelor cu caracter personal în străinătate

Din cele 629 de notificări cu transferuri de date către entități din străinătate, în 537 au fost declarate transferuri către state din Uniunea Europeană, Zona Economică Europeană și din state terțe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entități care au aderat în baza principiilor Safe Harbor), precum și transferuri către state terțe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată și completată.

Totodată, au fost notificate 72 de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, pe baza contractelor cu clauze standard și 20 de transferuri în baza regulilor corporatiste obligatorii (Binding Corporate Rules). Sub acest aspect, comparativ cu anul anterior se constată o creștere a notificărilor cu transferuri de date către entități din străinătate.



Referitor la transferurile de date către state terțe, în baza prevederilor art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, conform contractelor încheiate între părțile între care are loc transferul de date, raportat la deciziile Comisiei Europene privind clauzele contractuale tip pentru transferul de date cu caracter personal către operatori sau persoanele împuternicite de către operator, stabilite în țări terțe, în temeiul Directivei 95/46/CE, acestea au vizat activități din următoarele domenii:

- contactarea furnizorilor și clienților în vederea furnizării ori solicitării de informații comerciale, procesarea plăților/facturilor în legătură cu furnizorii/clientții;
- efectuarea plăților către angajații operatorului, în special pentru cheltuielile suportate de aceștia, contactarea angajaților cu privire la chestiuni legate de facturile clienților, facturile vânzătorilor și registrele contabile;
- activități de suport tehnic;
- managementul resurselor umane, realizarea unui sistem de evidență la nivel de grup;
- gestiune economico-financiară și administrativ;
- studii clinice și cercetare medicală, monitorizarea securității medicamentelor, evidența raportărilor privind efecte adverse.

Pentru clarificarea condițiilor în care se realizează transferul de date personale către statele terțe s-a propus efectuarea unor investigații la sediul operatorilor ce le-au notificat și s-a solicitat operatorilor, după caz, remedierea deficiențelor constatate. Ulterior, Autoritatea națională de supraveghere a emis un număr de 5 autorizații de transfer în baza contractelor cu clauze standard.

În considerarea dispozițiilor art. 25 alin. (2) din Directiva 95/46/CE, referitoare la caracterul adecvat al nivelului de protecție oferit de o țară terță, ce se evaluează având în vedere toate circumstanțele referitoare la un transfer sau la o categorie de transferuri de date, președintele Autorității naționale de supraveghere a emis, în anul 2014, Decizia nr. 41 privind stabilirea unui model de autorizație pentru transferul în străinătate al datelor cu caracter personal în baza regulilor corporatiste obligatorii (Binding Corporate Rules — BCR).

În situația în care transferul datelor cu caracter personal se realizează în baza normelor corporatiste obligatorii (binding corporate rules) operatorul trebuie să transmită Autorității naționale de supraveghere următoarele documente:

- normele corporatiste obligatorii în forma aprobată de către autoritatea coordonatoare (lead authority);

- autorizația emisă de către autoritatea coordonatoare sau adresa prin care operatorul a fost înștiințat despre aprobarea normele corporatiste obligatorii de către autoritatea coordonatoare;

- formularul de solicitare a aprobării normelor corporatiste obligatorii pentru transferul datelor cu caracter personal prevăzut în WP 133 al Grupului de lucru art. 29;

- documentul ce conține lista entităților care fac parte din grupul operatorului, în măsura în care este posibil.

Aceste documente se vor transmite atât în limba engleză, cât și în limba română.

Transferurile de date în străinătate efectuate, în baza prevederilor art. 29 alin. 4 din Legea nr. 677/2001, modificată și completată, conform baza normelor corporatiste obligatorii (binding corporate rules) au vizat activități din următoarele domenii:

- resurse umane, respectiv recrutare și politica de recrutare, inclusiv planificarea succesiunii și managementul talentelor, administrarea beneficiilor (inclusiv pensii, înregistrarea și prelucrarea eligibilității dependenților), administrarea salariilor și plata cheltuielilor, evaluările de performanță, planificarea carierei, monitorizarea abilităților, mutări ale posturilor, promovări și restructurări de personal, administrarea detașărilor internaționale, gestionarea cursurilor de instruire, raportarea și monitorizarea învățării și instruirii, monitorizarea șanselor egale;
- standardizarea procesului privind relațiile contractuale cu clienții, contabilitatea financiară globală în legătură cu furnizorii, contractorii și clienții, evaluarea și urmărirea relației de afaceri pentru a asigura că firmele membre respectă politica de independență a societății și politicile locale proprii de independență, monitorizarea calității serviciilor.

În urma analizării transferurilor de date în străinătate către state terțe, a fost emis un număr de **16** autorizații de transfer, din care **11** pentru transferuri în baza regulilor corporatiste obligatorii (Binding Corporate Rules).

Secțiunea a 3-a Puncte de vedere privind diverse chestiuni de protecția datelor

În anul 2014, atât persoanele vizate, cât și operatorii au solicitat opinii cu privire la condițiile legale de prelucrare a datelor cu caracter personal.

În continuare, prezentăm unele dintre cele mai semnificative cazuri :

1. Două societăți de administrare a fondurilor de pensii private, ambele înscrise în registrul de evidență a prelucrărilor de date cu caracter personal, au fuzionat, societatea absorbantă devenind administratorul fondurilor de pensii. Operatorul a solicitat informații cu privire la obligațiile societăților care au fuzionat, în special în ceea ce privește activitatea de reclamă, marketing și publicitate, prin intermediul adresei de poștă electronică și numerelor de telefon.

În acest context, s-au comunicat operatorului informații referitoare la obligația de a furniza persoanelor vizate, în cazul în care datele nu sunt obținute direct de la acestea, datele prevăzute la art. 12 alin. (2) din Legea nr. 677/2001, modificată și completată (identitatea operatorului, scopul prelucrării, etc.).

Totodată, operatorul a fost informat cu privire la regula instituită de Legea nr. 677/2001, modificată și completată, respectiv aceea că prelucrarea datelor personale ale unei persoane fizice, de către o altă persoană fizică sau juridică, în calitatea sa de operator de date cu caracter personal, se efectuează numai cu consimțământul persoanei în cauză, dat în mod expres și neechivoc.

În plus, potrivit prevederilor art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, este interzisă efectuarea de comunicări comerciale prin utilizarea unor sisteme automate de apelare și comunicare care nu necesită intervenția unui operator uman, prin fax ori prin poștă electronică sau prin orice altă metodă care folosește serviciile de comunicații electronice destinate publicului, cu excepția cazului în care abonatul sau utilizatorul vizat și-a exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări.

Totodată, s-a subliniat că persoanelor vizate trebuie să le fie oferită posibilitatea de a-și exercita, în orice moment dreptul de opoziție.

2. O asociație cu activitate la nivel național a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la obligația de a notifica, în contextul noii legi a voluntariatului, prelucrările de date efectuate pentru încheierea contractelor și pentru gestionarea registrului intern de voluntari, precum și în scopul organizării de evenimente în cadrul Programului European de Voluntariat. Prin acesta organizații din România recrutează și plasează voluntari la organizații din Europa, unde aceștia desfășoară activități de voluntariat pe baza unui contract de colaborare specific.

Raportat la aceste aspecte, s-a comunicat că nu este necesară efectuarea notificării (spre exemplu, notificarea prelucrării datelor cu caracter personal nu este necesară când prelucrarea datelor cu caracter personal referitoare la proprii angajați și la colaboratorii externi este efectuată de entitățile de drept public și de drept privat, în vederea îndeplinirii unor obligații legale).

Se va completa formularul de notificare în cazul prelucrărilor/transferurilor de date cu caracter personal care nu se realizează pentru îndeplinirea unei obligații legale.

3. O societate comercială a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la aplicabilitatea Legii nr. 677/2001, în cadrul furnizării serviciilor de telefonie prin internet.

S-a precizat că, potrivit art. 3 lit. a și d) din Legea nr. 677/2001, pentru ca o prelucrare de date să intre în sfera de aplicare a acestei legi, este necesar ca informațiile colectate să aibă calitatea de date cu caracter personal și să fie organizate într-un sistem de evidență, accesibil potrivit unor criterii determinate, indiferent dacă acest sistem este organizat în mod centralizat ori descentralizat sau este repartizat după criterii funcționale ori geografice.

De asemenea, s-a menționat că în sensul dispozițiilor art. 3 lit. e) din Legea nr. 677/2001, operator este orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal.

Având în vedere informațiile furnizate, s-a apreciat că societatea are calitatea de operator și este necesar să notifice Autorității naționale de supraveghere prelucrarea efectuată, în vederea înscrierii acesteia în Registrul de evidență a prelucrărilor de date cu caracter personal.

Totodată, au fost prezentate etapele necesare pentru obținerea înregistrării în Registrul electronic de evidență a prelucrărilor de date cu caracter personal.

4. O instituție publică a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la obligația de notificare a prelucrărilor de date efectuate în activitatea sa curentă, și anume aceea de a ține registrul deschis spre consultare publicului.

Legat de aspectele puse în discuție, Autoritatea națională de supraveghere a precizat că, potrivit prevederilor art. 22 alin. (2) din Legea nr. 677/2001, modificată și completată, „notificarea nu este necesară în cazul în care prelucrarea are ca unic scop ținerea unui registru destinat prin lege informării publicului și deschis spre consultare publicului în general sau oricărei persoane care probează un interes legitim, cu condiția ca prelucrarea să se limiteze la datele strict necesare ținerii registrului menționat.”

În același timp, acestei instituții i s-au adus la cunoștință obligațiile care îi revin potrivit dispozițiilor legale aplicabile în domeniul protecției datelor cu caracter personal (informarea persoanelor vizate, dreptul de acces, intervenție, opoziție, confidențialitatea și securitatea prelucrărilor).

5. O societate comercială a solicitat punctul de vedere cu privire la condițiile necesare pentru derularea activității de localizare a bunurilor, prin intermediul datelor de geolocalizare.

Față de aspectele relatate de operator, Autoritatea de supraveghere a precizat faptul că utilizarea sistemului de geolocalizare GPS reprezintă o modalitate de prelucrare de date cu caracter personal, întrucât permite angajatorului identificarea unui angajat, în mod indirect, prin localizarea bunului utilizat de către salariatul său, chiar dacă scopul prelucrării, așa cum se precizează, este cel al protecției bunurilor societății.

Prin urmare, raportat la dispozițiile Legii nr. 677/2001, entitatea care dorește să recurgă la astfel de sisteme de localizare geografică intră sub incidența acestora, precum și ale Deciziei nr. 11/2009 privind stabilirea categoriilor de operațiuni de prelucrare a datelor cu caracter personal, susceptibile de a prezenta riscuri speciale pentru drepturile și libertățile persoanelor.

În sensul celor de mai sus, întrucât astfel de dispozitive de geolocalizare comportă anumite riscuri în privința drepturilor și libertăților persoanei care utilizează bunul respectiv (angajatul), înainte de instalarea unor astfel de sisteme de supraveghere, angajatorul trebuie

să facă în prealabil o evaluare a riscurilor la care se supune activitatea sa pentru a stabili necesitatea implementării lor, precum și existența altor posibilități de îndeplinire a scopului propus.

Această evaluare este necesară în vederea argumentării și dovedirii unui interes legitim al operatorului care ar trebui să prevaleze față de interesul, drepturile și libertățile persoanei fizice în cauză, pentru a se justifica incidența situației de excepție prevăzute de art. 5 alin. (2) lit. e) din Legea nr. 677/2001.

În măsura în care nu sunt îndeplinite condițiile de excepție ale dispozițiilor legale sus-menționate, este necesar consimțământul angajatului respectiv. De asemenea, este necesară respectarea dreptului la informare a salariaților, potrivit art. 12 din aceeași lege.

Totodată, întrucât pot fi afectate drepturile salariaților, este necesară și consultarea prealabilă a organismelor reprezentative ale acestora.

6. O asociație de proprietari a cerut punctul de vedere al Autorității naționale de supraveghere cu privire la necesitatea notificării în situația colectării de la membrii proprietari ai asociației de copii ale actelor de proprietate în baza cărora să fie stabilită cota parte indiviză ce revine fiecăruia

Legat de aspectele puse în discuție, Autoritatea națională de supraveghere a precizat că, pentru prelucrarea datelor proprietarilor și chiriașilor, efectuată de către asociație, exclusiv în scopul administrării imobilului, nu se impune depunerea notificării, potrivit prevederilor art. 1 lit. c) din Decizia nr. 90/2006.

Totodată, s-a comunicat faptul că, deși în cazul sus-menționat nu este necesară depunerea notificării, asociația de proprietari are calitate de operator de date și trebuie să respecte prevederile Legii nr. 677/2001, modificată și completată. În acest context, chiar art. 38 alin. (3) din Ordonanța de Urgență nr. 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, republicată, stabilește că „păstrarea, actualizarea și utilizarea datelor din cartea de imobil (...) se fac cu respectarea dispozițiilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare”.

CAPITOLUL AL VII-LEA MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, în anul 2014, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal i s-a alocat prin Legea bugetului de stat nr. 356/2013, un buget în sumă de 3.273.000 lei cu următoarea structură:

lei

Denumire indicator	Cod	Buget inițial 2014	Buget actualizat la 31.12.2014	Sume cheltuite pana la 31.12.2014	Execuție (%)
Total cheltuieli	51.01	3273000	2945000	2885260	97.97
Cheltuieli de personal	10	2326000	2283000	2279780	99.86
Bunuri și servicii	20	927000	642000	597116	93.01
Cheltuieli de capital	71	20000	20000	18489	92.45
Plăți efectuate în ani precedenți				-10125	

Pentru că pe parcursul exercițiului bugetar au avut loc retrageri de fonduri și rectificări bugetare, s-a urmărit permanent actualizarea priorităților pentru realizarea celor mai importante proiecte cu fondurile existente.

Creditele definitive aprobate au asigurat realizarea în condiții de performanță a obiectivelor propuse.

În ceea ce privește utilizarea fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorității de Supraveghere a constituit un procent de 78% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 2.279.780 lei, (prin ocuparea unor posturi temporar prin detașare de la alte instituții)

Înregistrându-se în continuare un deficit major de personal (11 posturi neocupate). Majoritatea cheltuielilor de personal au fost aferente plăților făcute pentru munca salariată a angajaților din departamentele de specialitate.

Cheltuielile cu deplasările au reprezentat 4.44% din totalul cheltuielilor pe anul 2014 datorită unui număr crescut de plângeri și controale la operatorii de date din teritoriu.

Trebuie menționat faptul că Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal își realizează obiectul principal de activitate prin investigații și controale la operatorii situați pe teritoriul României, precum și la consulatele României.

La nivelul Uniunii Europene, Autoritatea de Supraveghere are obligația de a participa la lucrările Grupului de lucru Art. 29 și la grupurile de lucru pe domeniul protecției datelor constituite la acest nivel și ale autorităților comune de control (Schengen, Europol, Eurodac) și la lucrările Consiliului Europei în domeniu. Sumele alocate pentru deplasări cuprind și aceste cheltuieli.

În anul 2014, cheltuielile cu bunuri și servicii au crescut cu 14% față de anul 2013, avându-se permanent în vedere mai mulți factori – oportunitatea cheltuielilor, criteriul prețului cel mai scăzut aplicat în procedurile de achiziții alături de cerințe tehnice atent stabilite.

Politicile contabile utilizate la întocmirea situațiilor financiare anuale sunt în conformitate cu reglementările contabile în vigoare.

Situațiile financiare anuale oferă o imagine fidelă a realității poziției financiare a instituției, încadrarea în creditele bugetare alocate pe grupe, titluri, articole și alineate de cheltuieli așa cum sunt prevăzute în bugetul autorității.

Cheltuielile bugetare s-au făcut cu respectarea principiilor privind legalitatea, oportunitatea, continuitatea și eficiența.

Toate documentele ce intră sub incidența controlului financiar preventiv propriu sunt verificate și vizate.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, putem preciza că acestea au fost utilizate cu maximă eficiență și printr-o atentă administrare de către instituția noastră.

CAPITOLUL VIII

PROPUNERI DE LEGE FERENDA

1. Propunere de completare a legii fundamentale în contextul reformei constituționale

Propunem adăugarea în categoria drepturilor fundamentale a dreptului la protecția datelor cu caracter personal, ca drept distinct, alături de art. 26 din Constituție privind dreptul la viață intimă, familială și privată, în concordanță cu prevederile art. 16 din Tratatul de Funcționare a Uniunii Europene.

Propunem adăugarea unui articol privind Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, competențele și rolul acesteia de apărător al dreptului la viață privată și al dreptului la protecția datelor cu caracter personal ale persoanelor fizice, după articolul referitor la instituția Avocatului Poporului.

2. Modificarea art. 1 al Legii nr. 554/2004 a contenciosului administrativ

Raportat la rolul Autorității naționale de supraveghere de a intenta acțiuni în justiție, propunem modificarea art. 1 al Legii nr. 554/2004, astfel încât persoanele vizate să dobândească de drept calitatea de reclamant, în cadrul acțiunilor în justiție intentate de Autoritatea Națională de Supraveghere pentru apărarea drepturilor acestora, într-o manieră similară acțiunilor introduse de Avocatul Poporului.

3. Propunere de modificare a art. 9 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare

Autoritatea națională de supraveghere propune modificarea art. 9 alin. (3) din Legea nr. 506/2004, astfel încât să fie stabilite prin lege condițiile de soluționare a plângerilor privind apelurile abuzive, într-o manieră similară celei deja existente în majoritatea statelor membre ale Uniunii Europene.

4. *Propunere de modificare a Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal*

Propunem următoarele modificări:

Alineatul (3) al articolului 1 se modifică și va avea următorul cuprins:

„(3) Atribuțiile Autorității naționale de supraveghere sunt, în principal, reglementate prin Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.”

Alineatul (5) al articolului 3 se modifică și va avea următorul cuprins:

„(5) În exercitarea atribuțiilor sale, președintele Autorității naționale de supraveghere emite decizii și instrucțiuni obligatorii pentru entitățile la a căror activitate se referă.”

Alineatul (1) al art. 13 se modifică și va avea următorul cuprins:

„(1) Autoritatea națională de supraveghere are dreptul să facă investigații și controale prealabile, iar în exercitarea atribuțiilor de control, precum și în cadrul procedurii de soluționare a plângerilor și sesizărilor, are dreptul să ceară autorităților administrației publice orice informații sau documente necesare îndeplinirii acestor atribuții, să verifice, la sediul entității sau al autorității de supraveghere, orice suport de stocare a datelor cu caracter personal, să audieze și să ia declarații de la conducătorii autorităților administrației publice și de la orice funcționar public sau personal contractual care poate da informațiile necesare soluționării unei cereri adresate Autorității naționale de supraveghere în legătură cu prelucrarea datelor cu caracter personal și libera circulație a acestor date.”

Alineatul (2) al articolului 15 se modifică și va avea următorul cuprins:

„(2) Numărul maxim de posturi, exclusiv demnitarii, este de 85.”

Alineatul (1) al articolului 16 se modifică și va avea următorul cuprins:

„(1) Personalul Autorității naționale de supraveghere are același statut cu personalul din aparatul celor două Camere ale Parlamentului, este format din funcționari publici parlamentari sau, după caz, personal contractual, și beneficiază de aceleași drepturi, potrivit reglementărilor legale aplicabile funcționarului public parlamentar ori, după caz, personalului contractual din aparatul celor două Camere ale Parlamentului.”

5. Propunere de completare și modificare a Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările ulterioare

Propunem următoarele completări și modificări:

La articolul 21 alineatul (3), lit. d¹ se abrogă.

Alineatul (3) al articolului 23 se modifică și va avea următorul cuprins:

„(3) Operatorii care nu au fost anunțați în termen de 15 zile de la data notificării despre efectuarea unui control prealabil pot începe prelucrarea.”

După alineatul (3) al articolului 25 se introduce un nou alineat, alin. (3¹), cu următorul cuprins:

„(3¹) Termenul de înaintare a plângerii către autoritatea de supraveghere este de cel mult un an de la data la care a avut loc încălcarea drepturilor persoanei vizate sau de la data la care aceasta a luat la cunoștință de producerea unei încălcări.”

Alineatul (6) al articolului 25 se modifică și va avea următorul cuprins:

„(6) Decizia trebuie motivată și se comunică părților interesate în termen de 30 de zile de la data emiterii acesteia.”

După articolul 27, se introduce un nou articol, art. 27¹, cu următorul cuprins:

„ Art. 27¹ Operatorul este obligat să transmită informațiile solicitate de autoritatea de supraveghere în exercitarea atribuțiilor sale de investigare, în termenul indicat de aceasta, sub sancțiunea prevăzută de art. 34.”

Alineatul (8) al articolului 25 se modifică și va avea următorul cuprins:

„(8) Autoritatea de supraveghere se poate adresa justiției pentru apărarea oricăror drepturi garantate de prezenta lege persoanelor vizate. În acest caz, persoanele vizate dobândesc, de drept, calitatea de reclamant, urmând a fi citate în această calitate. Instanța competentă este Tribunalul Municipiului București. Cererea de chemare în judecată este scutită de taxa de timbru.”

Alineatul (4) teza a doua al articolului 29 se modifică și va avea următorul cuprins:

„(4) (...) Aceste garanții pot fi stabilite, în special, prin clauze contractuale adecvate.”

Articolul 31 se modifică și va avea următorul cuprins:

„Omisiunea de a efectua notificarea în condițiile art. 22 sau ale art. 29 alin. (3) în situațiile în care această notificare este obligatorie, precum și notificarea incompletă sau care conține informații false constituie contravenții, dacă nu sunt săvârșite în astfel de condiții încât să constituie infracțiuni, și se sancționează cu amendă de la 3.500 la 15.000 lei.”

Articolul 32 se modifică și va avea următorul cuprins:

„Prelucrarea datelor cu caracter personal de către un operator sau de o persoană împuternicită de acesta, cu încălcarea prevederilor art. 4-10 sau cu nesocotirea drepturilor prevăzute la art. 12-15 sau la art. 17, constituie contravenție, dacă nu este săvârșită în astfel de condiții încât să constituie infracțiune, și se sancționează cu amendă de la 4.000 la 75.000 lei.”

Articolul 33 se modifică și va avea următorul cuprins:

„Neîndeplinirea obligațiilor privind aplicarea măsurilor de securitate și de păstrare a confidențialității prelucrărilor, prevăzute la art. 19 și art. 20, constituie contravenție, dacă nu este săvârșită în astfel de condiții încât să constituie infracțiune, și se sancționează cu amendă de la 7.500 la 150.000 lei, iar pentru societățile comerciale cu o cifră de afaceri de peste 5.000.000 lei, prin derogare de la dispozițiile O.G. nr. 2/2001 privind regimul contravențiilor, cu modificările ulterioare, cu o amendă de până la 1,5% din cifra de afaceri pe anul precedent.”

Articolul 34 se modifică și va avea următorul cuprins:

„Refuzul de a furniza autorității de supraveghere informațiile sau documentele cerute de aceasta în exercitarea atribuțiilor de investigare prevăzute la art. 27 constituie contravenție dacă nu este săvârșită în astfel de condiții încât să constituie infracțiune, și se sancționează cu amendă de la 7.500 la 75.000 lei.”

După articolul 34 se introduce un nou articol, articolul 34¹, intitulat „Nerespectarea deciziilor autorității de supraveghere”, cu următorul cuprins:

„Nerespectarea deciziilor prin care autoritatea de supraveghere a dispus interzicerea prelucrării, suspendarea provizorie sau încetarea prelucrării datelor, ștergerea parțială ori integrală a datelor prelucrate și care nu au fost contestate în termenul legal, constituie contravenție, dacă nu este săvârșită în astfel de condiții încât să constituie infracțiune, și se sancționează cu amendă de la 7.500 la 75.000 lei.”

După articolul 34 se introduce un nou articol, articolul 34², intitulat „Informarea publicului cu privire la sancțiuni”, cu următorul cuprins:

„În funcție de gravitatea și circumstanțele faptelor constatate, autoritatea de supraveghere poate obliga operatorul să aducă la cunoștința publicului, prin orice modalitate, sancțiunea contravențională dispusă. Măsura se ia prin decizie motivată și se comunică părților interesate.”