

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

R A P O R T A N U A L

2015

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 2015.

În cursul acestui an, activitatea instituției noastre s-a subsumat dezideratului respectării regulilor aplicabile în domeniul protecției datelor cu caracter personal în mediul public și privat.

Direcțiile de acțiune ale Autorității naționale de supraveghere s-au concentrat pe intensificarea măsurilor 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 operatori.

Investigațiile efectuate din oficiu au urmărit, cu precădere, verificarea respectării regulilor de protecție a datelor personale în activitatea desfășurată de instituții publice, de entități deținătoare de website-uri și de unități de turism. În vederea soluționării plângerilor și a sesizărilor primite, 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 supraveghere video și de activitatea on-line a unor operatori.

Ca rezultat al activității de control desfășurate în anul 2015, s-a constatat o creștere semnificativă a cuantumului amenziilor aplicate prin comparație cu anul anterior.

Sub aspectul acțiunilor de informare, remarcăm că, pe lângă organizarea de evenimente specifice dedicate sărbătoririi Zilei Europene a Protecției Datelor, instituția noastră a participat activ la numeroase reuniuni la care a fost invitată, desfășurate cu largă implicare a reprezentanților din mediul public și privat. De asemenea, Autoritatea a celebrat 10 ani de la înființare printr-o dezbatere publică, ce a avut loc pe data de 10 iunie 2015, la Palatul Parlamentului, cu participarea reprezentativă a autorităților publice centrale și a mediului de afaceri.

Anul 2015 a fost marcat de o decizie importantă pronunțată, pe data de 6 octombrie, de Curtea de Justiție a Uniunii Europene, prin care a fost invalidată Decizia 2000/520/CE a Comisiei Europene, adoptată în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, decizie care reglementa transferul de date cu caracter personal din state membre ale Uniunii Europene către entități din Statele Unite ale Americii, în baza principiilor Safe Harbour.

Aceasta a implicat o schimbare a practicii în activitatea de monitorizare a transferurilor de date personale către Statele Unite ale Americii, în concordanță cu abordarea comună a tuturor autorităților de protecția datelor din Uniunea Europeană, stabilită în cadrul Grupului de Lucru Art. 29, de pe lângă Comisia Europeană.

În același timp, subliniem că, în anul 2016, este preconizată adoptarea noilor reglementări europene privind protecția datelor personale, de către Parlamentul European și Consiliu, ce constau într-un Regulament privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, de directă aplicabilitate în toate statele membre ale Uniunii Europene, precum și o Directivă privind protecția datelor prelucrate în scopul prevenirii, detectării, investigării și punerii sub urmărire a infracțiunilor și a altor activități judiciare.

În perspectiva adoptării acestui pachet legislativ, instituția noastră își propune asigurarea tranziției către aplicarea reglementărilor europene preconizate să devină efective din anul 2018. Aceasta implică o evaluare complexă a instrumentelor specifice asigurării protecției datelor personale în vederea identificării soluțiilor optime de sistematizare a activității și de cooperare eficientă cu celelalte autorități de protecția datelor personale din Uniunea Europeană.

În acest context, consolidarea capacității administrative a Autorității reprezintă o prioritate și necesită alocarea unor resurse materiale, financiare și umane adecvate exercitării atribuțiilor sale specifice, în vederea armonizării din punct de vedere legislativ și instituțional cu noul cadru prevăzut de pachetul legislativ de reformă la nivel european.

În final, permiteți-mi să îmi exprim speranța că Autoritatea va beneficia și pe viitor de întregul dumneavoastră sprijin pentru edificarea unei adevărate culturi a protecției datelor personale în România.

Ancuța Gianina OPRE,
Președinte

CUPRINS

CAPITOLUL I

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

CAPITOLUL II

INIȚIATIVE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

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
---	---

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Acte administrative cu caracter normativ	10
Secțiunea a 2-a Avizarea actelor normative.....	13
Secțiunea a 3-a Puncte de vedere privind diverse chestiuni de protecția datelor.....	32
Secțiunea a 4-a Activitatea de reprezentare în fața instanțelor de judecată.....	42
Secțiunea a 5-a Informare publică	53

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.....	61

CAPITOLUL V

ACTIVITATEA ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE	86
--	----

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

Secțiunea 1	Activitatea de înregistrare a prelucrărilor de date.....	95
Secțiunea a 2-a	Transferul datelor cu caracter personal în străinătate.....	97
Secțiunea a 3-a	Puncte de vedere referitoare la activitatea operatorilor	100

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII.....	103
--	------------

CAPITOLUL VIII

PROPUNERI DE LEGE FERENDA.....	105
---------------------------------------	------------

CAPITOLUL I PREZENTARE GENERALĂ

Raportul de activitate pe anul 2015 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 activități.

În cuprinsul **Capitolului al II-lea** sunt prezentate 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 la 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 avizelor asupra proiectelor de acte normative, deciziilor 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 privind incidența legislației în domeniul protecției datelor asupra activității desfășurate de operatori, condițiile prelucrării datelor cu caracter special, legalitatea dezvoltării unor date și la transferul acestora în străinătate.

În secțiunea privind 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 2015.

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 implică verificarea modului de aplicare a dispozițiilor legale în materie. În cadrul investigațiilor efectuate în anul 2015, au fost aplicate sancțiuni contravenționale constând în avertismente și amenzi în cuantum total de 679.700 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, ce a implicat participarea activă la grupurile de lucru de la nivel european și internațional, destinate stabilirii unei practici armonizate între autoritățile naționale de protecție a datelor personale.

Capitolul al VI-lea privind activitatea de supraveghere a prelucrărilor de date cu caracter personal cuprinde principalele concluzii 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 10.819 de notificări privind prelucrări 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 privind creditele bugetare puse la dispoziția Autorității naționale de supraveghere și sumele cheltuite pe fiecare articol al clasificăției bugetare.

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

CAPITOLUL II

INIȚIATIVE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

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.

Pe parcursul anului 2015, au continuat lucrările Grupului de Lucru DAPIX în contextul negocierii, de către Statele membre, a proiectului Regulamentului general privind protecția datelor și a celui privind Directiva privind protecția datelor în cadrul activităților autorităților de aplicare a legii. În acest sens, Autoritatea națională de supraveghere a continuat să participe, la solicitarea Ministerului Afacerilor Externe și Ministerului Afacerilor Interne, la formularea elementelor de mandat referitoare la diferite aspecte privind textele celor două proiecte de acte ale Uniunii Europene.

În acest context, la unele dintre reuniunile DAPIX s-au pus în discuție aspecte privind domeniul de aplicare al Directivei privind protecția datelor în cadrul activităților autorităților de aplicare a legii, în raport cu cel al Regulamentului general privind protecția datelor.

Referitor la câmpul de aplicare al Directivei, respectiv extinderea domeniilor reglementate de această directivă și la cel privind ordinea publică și siguranța publică (propunerea Ministerului Afacerilor Interne), Autoritatea națională de supraveghere a subliniat faptul că, în jurisprudența Curții Europene a Uniunii Europene (CJUE), conceptele de ordine

publică și siguranță publică au fost analizate în Hotărârea din 10 iulie 2008 emisă în Cauza Jipa (C-33/07).

În această privință, CJUE a subliniat întotdeauna că, deși, în general, statele membre sunt libere să stabilească cerințele de ordine publică și de siguranță publică în conformitate cu nevoile lor naționale, care pot varia de la un stat membru la altul și de la o perioadă la alta, nu este mai puțin adevărat că, în contextul comunitar și în special ca justificare a unei derogări de la principiul fundamental al liberei circulații a persoanelor, aceste cerințe trebuie interpretate în mod strict, astfel încât sfera lor să nu poată fi stabilită unilateral de fiecare stat membru fără exercitarea unui control din partea instituțiilor Comunității Europene.

Jurisprudența CJUE a precizat astfel că noțiunea de ordine publică presupune, în orice caz, pe lângă tulburarea ordinii sociale pe care o reprezintă orice încălcare a legii, existența unei amenințări reale, prezente și suficient de grave la adresa unui interes fundamental al societății.

De asemenea, instanța europeană a statuat faptul că "măsurile luate din motive de ordine publică sau de siguranță publică trebuie să se întemeieze exclusiv pe conduita persoanei în cauză, neputând fi acceptate motivări care nu sunt direct legate de cazul respectiv sau care sunt legate de considerații de prevenție generală."

Raportat la jurisprudența CJUE și prevederile Cartei, precum și ale Legii fundamentale, Autoritatea națională de supraveghere a apreciat că includerea sferei ordinii publice și a siguranței publice în câmpul de aplicare al Directivei, fără respectarea jurisprudenței CJUE în materie și a dispozițiilor constituționale, poate conduce la riscul apariției unor încălcări ale drepturilor fundamentale ale persoanelor fizice.

În consecință, pentru a fi respectate cerințele de predictibilitate și previzibilitate ale actelor normative, se impune stabilirea cu foarte mare claritate a activităților care intră în sfera ordinii publice și a siguranței publice și care ar putea fi incluse în textul Directivei, astfel încât să fie îndeplinite exigențele CJUE statuate în jurisprudența sa.

Prin urmare, Autoritatea națională de supraveghere și-a menținut rezerva în mod constant asupra faptului că nu este posibilă exceptarea în totalitate a sferei ordinii publice de la aria de aplicare a Regulamentului și includerea acesteia în textul Directivei.

În consens cu cele de mai sus și-a exprimat opinia și Serviciul Juridic al Consiliului, care a susținut faptul că sintagma „public security”, ar urma să fie acoperită de domeniul de aplicare al acestui proiect de Directivă, ceea ce ar conduce la scăderea nivelului de protecție asigurat.

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Acte administrative cu caracter normativ

Decizia nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum și pentru modificarea și abrogarea unor decizii

Această decizie a fost emisă în aplicarea prevederilor art. 22 alin. (9) din Legea nr. 677/2001, conform căroră Autoritatea națională de supraveghere poate stabili și cazuri în care notificarea nu este necesară, în baza referatului de aprobare nr. 18/2.06.2015 și luând în considerare necesitatea asigurării unei protecții eficiente a drepturilor persoanelor ale căror date cu caracter personal sunt supuse prelucrării, în special în cazul anumitor operațiuni de prelucrare a datelor cu caracter personal care prezintă riscuri pentru drepturile și libertățile persoanelor, precum și pentru a evita formalitățile administrative.

Decizia nr. 200/2015 a fost publicată în Monitorul Oficial nr. 969 din 28 decembrie 2015, cu următorul conținut:

Art. 1

(1) Notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nu este necesară, cu excepția următoarelor cazuri privind:

- a) prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice ori de natură similară, de apartenența sindicală, precum și a datelor privind starea de sănătate și viața sexuală;
- b) prelucrarea datelor genetice și biometrice;
- c) prelucrarea datelor care permit, direct sau indirect, localizarea geografică a persoanelor fizice prin mijloace de comunicații electronice;
- d) prelucrarea datelor cu caracter personal referitoare la săvârșirea de infracțiuni de către persoana vizată ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale aplicate persoanei vizate, efectuată de către entități de drept privat;

e) prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea și/sau evaluarea unor aspecte de personalitate, precum competența profesională, credibilitatea, comportamentul sau alte asemenea aspecte;

f) prelucrarea datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidență având ca scop adoptarea unor decizii automate individuale în legătură cu analizarea solvabilității, a situației economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravențională sau penală a persoanelor fizice, de către entități de drept privat;

g) prelucrarea datelor cu caracter personal ale minorilor efectuate în cadrul activităților de marketing direct;

h) prelucrarea datelor cu caracter personal ale minorilor, efectuate prin intermediul internetului sau a mesageriei electronice;

i) prelucrarea datelor cu caracter personal prevăzute la lit. a), referitoare la propriii membri, efectuate de asociații, fundații sau orice alte organizații fără scop patrimonial, exclusiv în vederea realizării specificului activității organizației, în măsura în care datele sunt dezvăluite unor terți fără consimțământul persoanei vizate;

(2) În situațiile de la alin. (1) lit. a) - i) notificarea nu este necesară atunci când prelucrarea este prevăzută de lege.

Art. 2

(1) Cu excepția cazurilor prevăzute la art. 29 alin. (5) și (6) din Legea nr. 677/2001, cu modificările și completările ulterioare, în toate situațiile, inclusiv în cele prevăzute la art. 1 din prezenta decizie, transferul datelor cu caracter personal către statele situate în afara Uniunii Europene, a Zonei Economice Europene, precum și către statele cărora Comisia Europeană nu le-a recunoscut, prin decizie, un nivel de protecție adecvat, va face obiectul notificării Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

(2) Transferurile prevăzute la alin. (1), efectuate în baza art. 29 alin. (4) din Legea nr. 677/2001, cu modificările și completările ulterioare, sunt supuse autorizării de către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Art. 3

(1) Operatorii sunt obligați să notifice Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal prelucrările datelor cu caracter personal stabilite la art. 1 alin. (1) și art. 2, înainte de începerea prelucrării.

(2) Dacă pe baza notificării, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal constată că prelucrarea se încadrează în una dintre situațiile prevăzute la art. 1 alin. (1) lit. a), b), d), g) sau h), dispune efectuarea unui control prealabil, în condițiile prevăzute de art. 23 din Legea nr. 677/2001, cu modificările și completările ulterioare.

(3) 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, cu precădere a celor privind asigurarea drepturilor persoanelor vizate, precum și a confidențialității și securității datelor.

Art. 4

Formularul tipizat al notificărilor din anexa la Decizia președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 95/2008 privind stabilirea formularului tipizat al notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în Monitorul Oficial al României, Partea I, nr. 876 din 24 decembrie 2008, se modifică prin înlocuirea coordonatelor de contact ale Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal cu actualele coordonate, astfel: "Bd. Gheorghe Magheru nr. 28-30, sectorul 1, București, telefon 031.805.9211".

Art. 5

La data intrării în vigoare a prezentei decizii, art. 15 din Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, publicată în Monitorul Oficial al României, Partea I, nr. 389 din 11 iunie 2012, se modifică după cum urmează:

"Art. 15

(1) Prelucrarea datelor personale prin sisteme de supraveghere video, inclusiv transferul acestora într-un stat terț, trebuie notificată Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, anterior începerii prelucrării.

(2) Face excepție de la alin. (1) prelucrarea datelor cu caracter personal efectuată de o persoană fizică, pentru uz personal, printr-un sistem de supraveghere video care captează imagini inclusiv din spații publice."

Art. 6

Prezenta decizie nu aduce atingere altor dispoziții legale care prevăd obligația de notificare, precum și celorlalte decizii ale președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, în vigoare.

Art. 7

(1) Prezenta decizie intră în vigoare la data publicării în Monitorul Oficial al României, Partea I.

(2) La data intrării în vigoare a prezentei decizii se abrogă Decizia președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 90/2006 privind cazurile în care nu este necesară notificarea prelucrării unor date cu caracter personal, publicată în Monitorul Oficial al României, Partea I, nr. 654 din 28 iulie 2006, Decizia președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 91/2006 privind cazurile în care este permisă notificarea simplificată a prelucrării datelor cu caracter personal, publicată în Monitorul Oficial al României, Partea I, nr. 654 din 28 iulie 2006, Decizia președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 100/2007 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal, publicată în Monitorul Oficial al României, Partea I, nr. 823 din 3 decembrie 2007, Decizia nr. 28/2007 privind transferurile datelor cu caracter personal către alte state, publicată în Monitorul Oficial al României, Partea I, nr. 182 din 16 martie 2007, Decizia 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, publicată în Monitorul Oficial al României, Partea I, nr. 155 din 12 martie 2009, precum și Decizia nr. 23/2012 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal, publicată în Monitorul Oficial al României, Partea I, nr. 216 din 2 aprilie 2012.

Secțiunea a 2-a Avizarea actelor normative

În anul 2015, au fost solicitate Autorității naționale de supraveghere o serie de avize privind proiecte de acte normative inițiate de diverse entități. Asupra majorității acestora, s-au efectuat observații și propuneri, întrucât s-a apreciat că este necesară completarea textelor respective, prin raportare la necesitatea respectării reglementărilor legale referitoare la protecția datelor cu caracter personal.

Unele dintre proiectele de acte normative de mai sus, prin textele propuse, prezentau un grad mare de ingerință în viața privată, aducând atingeri drepturilor fundamentale, motiv pentru care au fost efectuate recomandări pentru reanalizarea acestora și armonizarea lor cu dispozițiile legale privind protecția datelor sau chiar au fost avizate negativ în măsura în care observațiile nu au fost preluate de către inițiatori.

Prezentăm în continuare, pentru exemplificare, cele mai relevante dintre acestea:

- **Guvernul României a transmis *propunerea legislativă pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.***

Au fost efectuate următoarele observații și propuneri:

- referitor la definiția datelor de identificare a echipamentului de la art. 2 alin. (1) lit. b¹) din textul supus analizei, se remarcă faptul că aceasta nu are corespondent în Directiva 2002/58/CE implementată prin Legea nr. 506/2004, iar astfel cum este formulată, creează confuzie cu definițiile datelor de trafic și de localizare menționate în art. 2 alin. (1) lit. b) și c) din Legea nr. 506/2004, motiv pentru care se propune eliminarea art. 2 alin. (1) lit. b¹).

- se observă existența unei neconcordanțe între dispozițiile art. 5 alin. (1) și alin. (2¹) din textul propunerii.

Astfel, alineatul (1) face vorbire despre abonați și utilizatori, în timp ce alineatul (2¹) se referă la abonații cu plata în avans, stabilindu-se scopuri și condiții de prelucrare a datelor de trafic diferite. Cu toate acestea, art. 2 lit. a) din Legea nr. 506/2004 definește utilizatorul, iar art. 4 alin. (1) pct. 3 din Ordonanță de urgență nr. 111/2011 privind comunicațiile electronice, cu modificările și completările ulterioare, definește abonatul.

Conform dispozițiilor legale sus-menționate, abonat înseamnă orice persoană fizică sau juridică care a încheiat un contract pentru furnizarea unor servicii de comunicații electronice destinate publicului oferite de un furnizor de astfel de servicii, indiferent dacă plata se realizează în avans ori ulterior furnizării serviciilor.

- se poate observa că această nouă categorie de persoane (abonați cu plata în avans) nu este definită de lege, dar nici de proiectul transmis, sens în care se propune reanalizarea acestor dispoziții.

- textul de la art. 5 alin. (2¹) din propunerea legislativă (prelucrarea datelor de trafic se efectuează în scopul stabilirii obligațiilor contractuale ce privesc abonații cu plata în avans) este

necorelat cu prevederile art. 5 alin. (2) din Legea nr. 506/2004, mai ales în privința termenului de 3 ani, creând un regim diferit al abonaților, inclusiv din perspectiva scopului prelucrării datelor de trafic.

- raportat la propunerea textului art. 12¹ din proiectul de lege se remarcă faptul că aceasta vine în contradicție cu actualele prevederi ale art. 1 alin. (4) din Legea nr. 506/2004, unde se precizează că această lege nu se aplică în activitatea din domeniul apărării naționale și securității naționale, nici în cadrul activităților de combatere a infracțiunilor și de menținere a ordinii publice, nici în cadrul altor activități în domeniul dreptului penal.

- apreciem că art. 12¹ alin. (1) ar trebui să stabilească sfera infracțiunilor care justifică solicitarea accesului la date, raportat la cele reținute de Curtea Constituțională în paragraful 49 al Deciziei nr. 440/2014, precum și la dispozițiile art. 53 din Constituție care prevăd condițiile restrângerii exercițiului unor drepturi sau al unor libertăți.

- sub acest aspect, s-a subliniat faptul că este necesară stabilirea unor norme clare și previzibile, pentru a se respecta cerințele de necesitate și proporționalitate stabilite de Legea fundamentală și pentru a se evita apariția unor situații de abuz al autorităților.

- la art. 12¹ din propunerea legislativă se remarcă faptul că și în cuprinsul alin. (1) sunt enumerate, alături de alte autorități, organele de stat cu atribuții în domeniul apărării și securității naționale, cărora li se aplică o serie de condiții de acces la date, altele decât cele prevăzute la alin. (2), motiv pentru care s-a apreciat că este necesară reanalizarea acestor dispoziții și corelarea celor două alineate.

- referitor la art. 12¹ alin. (3), se observă că acesta instituie condiții numai în ceea ce privește solicitările și răspunsurile în format electronic, fiind omisă stabilirea condițiilor pe care trebuie să le respecte atunci când sunt pe suport de hârtie. În acest sens, s-a precizat că Legea nr. 677/2001, care completează dispozițiile Legii nr. 506/2004, se aplică atât sistemelor de evidență automatizate, cât și celor constituite pe hârtie.

- de asemenea, propunerea limitează răspunderea pentru integritatea și securitatea datelor numai la persoanele care certifică datele sub semnătură electronică. Or, obligațiile legale privind asigurarea confidențialității și securității datelor furnizate revin tuturor entităților/utilizatorilor care au acces la acestea.

- totodată, mențiunile efectuate numai în ceea ce privește solicitările și răspunsurile determină interpretarea că datele cu caracter personal furnizate ar putea fi excluse de la respectarea condițiilor reglementate de această propunere.

- referitor la termenul de cinci ani instituit la alin. (5) al art. 12¹, s-a semnalat faptul că, în expunerea de motive, este necesară fundamentarea acestei perioade de timp, raportat la principiul proporționalității prelucrării datelor.

- totodată, s-a subliniat faptul că, în propunerea legislativă, este necesar să se prevadă un mecanism autentic de control, care să asigure Autorității naționale de supraveghere și Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM) o verificare permanentă și efectivă a respectării dispozițiilor legale, astfel încât să poată fi sesizate cu ușurință cazurile în care furnizorii de servicii încalcă dispozițiile legale privitoare la tipul de date reținute, durata în care acestea sunt stocate, distrugerea lor în cazurile prevăzute de lege ori organele și instituțiile cărora li se permite accesul la aceste date (a se vedea paragraful 68 al Deciziei nr. 440/2014 a Curții Constituționale).

- în același timp, s-a apreciat că este necesară și reanalizarea actualelor prevederi ale Legii nr. 506/2004 din perspectiva obligațiilor ce revin furnizorilor de servicii de comunicații electronice, inclusiv sub aspectul regimului sancționator aplicabil și al departajării competențelor de sancționare între cele două autorități, respectiv ANCOM și ANSPDCP.

- **Ministerul Societății Informaționale a solicitat punctul de vedere cu privire la *proiectul Legii privind modificarea și completarea OUG nr. 111/2011, în ceea ce privește înregistrarea utilizatorilor de cartele preplătite.***

Referitor la acest proiect de lege, Autoritatea națională de supraveghere a remarcat faptul că propunerea este similară proiectului anterior de lege, declarat neconstituțional prin Decizia nr. 461/2014 a Curții Constituționale, și nu soluționează aspectele de neconstituționalitate semnalate de instanța de contencios constituțional privind: sfera subiectelor cărora li se aplică reținerea în masă a datelor, garanții suficiente împotriva abuzurilor, proporționalitatea măsurii, inclusiv cu privire la instrumentul juridic de modificare a OUG nr 111/2011, raportat la cele statuate de Curtea Constituțională privind faptul că, prin acest act, se completează de fapt cadrul general privind reținerea datelor reprezentat de Legea nr. 82/2012.

De asemenea, Autoritatea națională de supraveghere a formulat următoarele observații:

- la art. 3, prin sintagma "la ordinea publică și prevenirea infracțiunilor" se extinde nejustificat sfera scopului dispozițiilor actuale în vigoare, ceea ce indică nerespectarea celor statuate de CCR cu privire la încălcarea instrumentului juridic de modificare a OUG nr 111/2011;

- la pct. 55 este necesară reanalizarea categoriilor de date stabilite și reducerea acestora la cele strict necesare, în vederea respectării principiului caracterului adecvat, pertinent și neexcesiv stabilit de Legea nr. 677/2001;
- art. 51 alin. (12) conține o eroare de redactare pe fond, întrucât furnizorii sunt cei care au calitatea de operatori de date cu caracter personal, nefiind vorba de două noțiuni distincte;
- la art. 51 alin. (13) se impune reanalizarea formulării, întrucât norma este vagă și lasă să se înțeleagă posibilitatea de includere în formular și a altor date decât cele de la pct. 55;
- la art. 51 alin. (14) este necesară reformularea, deoarece există o confuzie de termeni, împuternicitul neavând calitatea de operator, potrivit Legii nr. 677/2001, în cadrul acestei activități; pe de altă parte, această trimitere la Legea nr. 677/2001 a existat și în forma anterioară a legii, nefiind însă suficientă, ca garanție, doar prevederea privind obligația de respectare a Legii nr. 677/2001.
- la art. 51 alin. (16), prin formularea referitoare la toate datele prevăzute la alin. (11), se creează confuzie față de termenul de 3 ani stabilit de Legea nr. 506/2004 pentru datele de trafic, precum și o inegalitate de tratament între persoanele vizate, pe de o parte, în calitatea lor de abonați, astfel cum prevede Legea nr. 506/2004, iar pe de altă parte în calitate de utilizatori de cartele preplătite;
- la art. 73² alin. (2) obligația stabilită este disproporționată în raport de scopul prelucrării și nu este în concordanță cu termenele prevăzute de Legea nr. 506/2004, creându-se o inegalitate între persoanele vizate care utilizează serviciile de comunicații electronice puse la dispoziția acestora de către furnizori, numai pentru faptul că se conectează prin puncte de acces la internet puse la dispoziția publicului de către persoanele juridice.

- **Ministerul Finanțelor Publice a solicitat punctul de vedere asupra proiectului de Ordonanță de urgență a Guvernului pentru modificarea și completarea unor acte normative în domeniul procedural fiscal, precum și pentru reglementarea unor măsuri fiscale.**

În ceea ce privește proiectul supus analizei, Autoritatea națională de supraveghere a formulat următoarele observații:

Activitățile prevăzute prin completarea art. 54 din Ordonanța Guvernului nr. 92/2003 cu alin. (4) și (5) din proiectul supus analizei 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), precum și date financiare, respectiv "informații în legătură cu operațiunile și soldurile aferente conturilor".

Realizarea, de către instituțiile de credit, "zilnic, în mod automat" de raportări (dezvăluiri de date) obligatorii către organe fiscale ale Agenției Naționale de Administrare Fiscală, este de natură să aducă o gravă atingere dreptului la viață privată prin instaurarea unor măsuri de supraveghere fiscală, efectuate în masă, fără nicio distincție cu privire la categoriile de persoane, cu încălcarea dreptului constituțional la viață privată și a principiului proporționalității. Această măsură constituie o restrângere a exercițiului drepturilor și libertăților persoanelor, în sensul art. 52 din Carta Drepturilor Fundamentale a Uniunii Europene.

Astfel, raportat la modificarea legislativă în discuție, s-a considerat că datele tuturor persoanelor vizate ce dețin conturi la instituțiile financiare sau care utilizează serviciile puse la dispoziție de aceste instituții ar urma să fie prelucrate de Agenția Națională de Administrare Fiscală, cu încălcarea principiilor de protecție a datelor, statuate de art. 4 din Legea nr. 677/2001, și fără să se stabilească anumite garanții adecvate pentru respectarea drepturilor persoanelor vizate.

În sensul celor de mai sus, s-a subliniat că trebuie respectate principiile de prelucrare a datelor cu caracter personal, instituite de art. 4 alin. (1) din Legea nr. 677/2001.

De altfel, conform Curții de Justiție a Uniunii Europene, o reglementare privind protecția datelor cu caracter personal, așa cum aceasta este prevăzută în art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene, trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime, astfel încât persoanele să dispună de garanții suficiente, care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date.

S-a arătat că, prin completările aduse Ordonanței Guvernului nr. 92/2003 de alin. (4) și (5) din art. 54 în proiectul supus analizei, ar urma să se legifereze efectuarea de transmisii (comunicări) electronice de date personale între diverse entități, instituții de credit și organe fiscale ale Agenției Naționale de Administrare Fiscală.

S-a menționat că măsurile dispuse de proiect, printre care și acelea de raportare, zilnică și în mod automat, de informații în legătură cu operațiunile și soldurile aferente conturilor și de date cu caracter personal, reprezintă o ingerință în drepturile garantate prin art. 7 și art. 8 din

Carta Europeană a Drepturilor Omului, întrucât nu se respectă principiul proporționalității între măsurile luate și interesul public ocrotit (respectiv combaterea fraudei și evaziunii fiscale).

Măsurile dispuse de proiect privesc ansamblul persoanelor care utilizează serviciile instituțiilor de credit, fără distincție, chiar în lipsa unor indicii cu privire la săvârșirea unor fapte de evaziune fiscală, ceea ce poate conduce la abuzuri și la utilizarea nelegală a datelor.

S-a subliniat faptul că proiectul supus analizei nu prevede niciun criteriu obiectiv care să permită delimitarea accesului organelor fiscale din cadrul Agenției Naționale de Administrare Fiscală la date și utilizarea acestora ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracțiuni de tipul fraudei sau evaziunii fiscale, infracțiuni care, având în vedere amploarea și gravitatea ingerinței în drepturile fundamentale consacrate la art. 7 și art. 8 din Carta Europeană a Drepturilor Omului, pot fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerință.

Corelat cu aspectul sus-menționat, s-a precizat că proiectul nu prevede în mod expres că accesul organelor fiscale din cadrul Agenției Naționale de Administrare Fiscală la datele prelucrate și utilizarea ulterioară a acestora trebuie să se facă în mod strict în scopul prevenirii și al descoperirii unor infracțiuni precis delimitate sau al desfășurării urmăririi penale în cazul lor, ci prevede doar că "informațiile obținute conform alin. (4) și (5) se utilizează doar în scopul îndeplinirii atribuțiilor specifice Agenției Naționale de Administrare Fiscală".

În consecință, Autoritatea națională de supraveghere a considerat că proiectul transmis este de natură să aducă atingere dreptului la viață privată și la protecția datelor cu caracter personal.

➤ **Ministerul Finanțelor Publice a solicitat propuneri și observații în ceea ce privește *proiectul de Lege privind Codul de procedură fiscală*.**

În acest sens, Autoritatea națională de supraveghere a transmis următoarele observații:

Întrucât în cuprinsul proiectului de act normativ se utilizează sintagma "date de identificare" cu referire la contribuabil/plătitor sau debitor, s-a apreciat că este necesară definirea acestor date în art. 1, precum și o eventuală enumerare a celor ce urmează a fi utilizate, în funcție de categoria de contribuabil/plătitor sau debitor (persoane fizice, persoane juridice ori alte entități fără personalitate juridică ce datorează, conform legii, impozite, taxe și contribuții sociale).

Referitor la art. 11 alin. (7) din proiect, s-a apreciat că este necesară completarea textului prin adăugarea unei referiri la entități fără personalitate juridică ce datorează, conform legii, impozite, taxe și contribuții sociale.

Cu privire la definirea, stabilirea, respectiv înregistrarea/modificarea domiciliului fiscal al persoanelor fizice (art. 31 și art. 32 din proiectul de Cod de procedură fiscală) s-a recomandat luarea în considerare a prevederilor legale privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români.

Referitor la prevederile art. 47 – "Comunicarea actului administrativ fiscal" în contextul publicării prin afișare la sediul organului fiscal emitent și pe pagina de internet a autorității administrației publice a unui anunț cu privire la emiterea actului menționat, s-a apreciat că trebuie enumerate, limitativ, informațiile (inclusiv cele constând în date cu caracter personal referitoare la contribuabilul/plătitorul persoană fizică) ce urmează a fi făcute publice, pentru a se evita o eventuală ingerință în viața privată a persoanelor fizice.

În ceea ce privește conținutul art. 61 "Obligația instituțiilor de credit de a furniza informații", respectiv al art. 62 "Obligația altor entități de a raporta tranzacții" din proiectul de Cod de procedură fiscală, s-au subliniat următoarele:

Realizarea, inclusiv zilnică, de raportări nediferențiate ale tuturor persoanelor fizice ce intră în raporturi cu instituțiile de credit (ce presupun și dezvăluiri de date cu caracter personal), obligatorii către organele fiscale centrale, astfel cum prevăd art. 61 alin. (1) și (2) și art. 62 din proiect, este de natură să aducă o gravă atingere dreptului la viață privată prin instaurarea unor măsuri de supraveghere fiscală, efectuate în masă, fără nicio distincție cu privire la categoriile de persoane, ceea ce ridică problema afectării dreptului constituțional la viață privată și a principiului proporționalității prelucrării datelor personale, prevăzut de art. 4 din Legea nr. 677/2001, raportat la interesul public ocrotit (combaterea fraudei și evaziunii fiscale). Această măsură poate constitui o restrângere a exercițiului drepturilor și libertăților persoanelor, în alte condiții decât cele prevăzute de art. 53 din Constituție.

Astfel, raportat la prevederile art. 61 alin. (2) și art. 62 din proiect, s-a arătat că datele tuturor persoanelor vizate ce dețin conturi la instituțiile financiare sau care utilizează serviciile puse la dispoziție de aceste instituții ar urma să fie prelucrate de organele fiscale centrale cu încălcarea principiilor de protecție a datelor, statuate de art. 4 din Legea nr. 677/2001, fără stabilirea anumitor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

De altfel, conform Curții de Justiție a Uniunii Europene, o reglementare privind protecția datelor cu caracter personal, așa cum aceasta este prevăzută în art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene, trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele să dispună de garanții suficiente, care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date.

Totodată, s-a subliniat că, prin proiectul supus analizei, ar urma să se legisfeze efectuarea de transmisii (comunicări) electronice de date, inclusiv date personale, între diverse entități, instituții de credit și organe fiscale centrale sau locale. O comunicare de tipul celor menționate anterior se poate expune la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor, că măsurile dispuse privesc ansamblul persoanelor care utilizează serviciile instituțiilor de credit, fără distincție, chiar în lipsa unor indicii cu privire la săvârșirea unor fapte de evaziune fiscală, de spălare a banilor ori finanțare a terorismului, ceea ce poate conduce la abuzuri și la utilizarea nelegală a datelor.

S-a arătat că proiectul supus analizei nu prevede niciun criteriu obiectiv care să permită delimitarea accesului organelor fiscale la date și utilizarea acestora ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracțiuni de tipul fraudei, evaziunii fiscale, spălării banilor ori finanțării terorismului, infracțiuni care, având în vedere amploarea și gravitatea ingerinței în drepturile fundamentale ar putea fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerință.

Corelat cu aspectul sus menționat, s-a precizat că proiectul nu prevede în mod expres că accesul organelor fiscale la datele prelucrate și utilizarea ulterioară a acestora trebuie să se facă în mod strict în scopul prevenirii și al descoperirii unor infracțiuni precis delimitate sau al desfășurării urmăririi penale în cazul lor. Raportat la prevederile art. 61 alin. (3) din proiect, s-a subliniat că ingerința în respectarea vieții private este accentuată semnificativ prin dezvăluirile prevăzute către toate autoritățile publice centrale și locale.

Cu privire la dispozițiile art. 68 alin. (1) și (2) din proiect, s-a apreciat că impunerea unei obligații generale de furnizare de informații în sarcina autorităților publice și instituțiilor publice și de interes public, centrale și locale, precum și a serviciilor deconcentrate ale autorităților publice centrale, fără să se precizeze că se realizează doar în baza unor solicitări punctuale ale

autorităților fiscale, strict în scopul exercitării atribuțiilor legale, este excesivă și poate conduce la încălcări ale drepturilor persoanelor fizice.

Cât privește dispozițiile art. 68 alin. (3) din proiect, s-a precizat că accesul organelor fiscale on-line la baza de date a autorităților publice, instituțiilor publice și de interes public, centrale și locale, precum și a serviciilor deconcentrate ale autorităților publice centrale, este de natură a crea premisa unor prelucrări excesive de date cu caracter personal, efectuate de organele fiscale în alt scop decât cel pentru care au fost prelucrate datele inițial, de către autoritățile și instituțiile menționate.

Raportat la prevederile art. 82 alin. (1) din proiect s-a subliniat că, așa cum "pentru persoanele fizice care nu dețin cod numeric personal" se atribuie de organul fiscal "un număr de identificare fiscală", din considerente de nediscriminare și egalitate de tratament, precum și pentru evitarea utilizării CNP-ului (dată personală cu caracter special), ar putea să i se atribuie un cod de identificare fiscală unic oricărei persoane fizice, subiect într-un raport juridic fiscal, (altul decât codul numeric personal) având funcție de identificare cu aplicabilitate în materie fiscală.

În ceea ce privește dispozițiile Titlului X "Aspecte internaționale" din proiectul Codului de procedură fiscală, s-a menționat că trebuie să fie clar delimitate condițiile și modalitățile realizării schimburilor de informații, în contextul existenței mai multor tipuri: la cererea unei autorități din alt stat membru, schimb automat obligatoriu de informații, schimb spontan de informații, schimb de informații bazat pe diverse forme de cooperare administrativă ori schimb de informații în baza unor acte și tratate internaționale la care România este parte.

S-a apreciat că este necesară introducerea în text, la acest titlu, a unor dispoziții care să privească în principal:

- respectarea principiului limitării scopului, respectiv obligația de prelucrare a datelor numai în scopul pentru care au fost furnizate;
- transmiterea datelor, inclusiv altor entități numai în anumite condiții, prin canale care să asigure securitatea acestora;
- caracterul exact, adecvat, pertinent și neexcesiv al datelor;
- modalitatea de transmitere a datelor;
- termenul de păstrare a datelor, modalitatea de ștergere, distrugere;
- corectarea, ștergerea, distrugerea datelor în situația în care se constată că au fost transmise date incorecte ori în privința cărora există interdicție de transmitere;

- faptul că autoritățile competente care transmit și primesc date sunt obligate să țină o evidență a acestor activități;

- asigurarea dreptului de informare al persoanei vizate, prin precizarea că, la cerere, acesteia 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, în condițiile legii;

- 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;

- obligația de informare reciprocă în cazul unei încălcări a securității.

În ceea ce privește schimburile de tip FATCA, s-a subliniat că Autoritatea națională de supraveghere își menține recomandările formulate cu privire la conținutul Acordului, precum și punctul de vedere deja exprimat, în sensul necesității ca textul Acordului să prevadă garanții privind protejarea drepturilor și libertăților persoanelor în legătură cu prelucrarea datelor personale, având în vedere natura datelor colectate și prelucrate, precum și transmiterea acestora pe teritoriul SUA.

În consecință, având în vedere toate aspectele sus menționate, Autoritatea națională de supraveghere a propus reanalizarea proiectului de Cod de procedură fiscală supus analizei, luând în considerare aspectele anterior menționate.

- **Ministerul Justiției a transmis spre avizare *proiectul de Lege privind instituirea unui mecanism de prevenire a conflictului de interese în procedura de atribuire a contractelor de achiziție publică și de modificare și completare a unor acte normative.***

Au fost formulate următoarele observații:

Având în vedere faptul că activitățile ce urmează a fi desfășurate de Agenția Națională de Integritate, prin intermediul unui sistem informatic integrat pentru prevenirea și identificarea potențialelor conflicte de interese (Sistemul Prevenție), dar și de autoritățile contractante care ar urma să utilizeze acest sistem, presupun prelucrări de date cu caracter personal (inclusiv date cu caracter special – cum este CNP-ul) ale persoanelor fizice implicate în proceduri de

atribuire a contractelor de achiziție publică, s-a precizat că este necesară luarea în considerație a principiilor de protecție a datelor, stabilite de art. 4 alin. (1) din Legea nr. 677/2001, stabilirea garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate și identificarea modalităților de acces la date al altor entități, raportat la competențele legale ale acestora, raportat la situațiile de excepție stabilite expres de art. 5 alin. (2) din Legea nr. 677/2001.

➤ **Guvernul României a transmis *propunerea legislativă privind exercitarea prin corespondență a dreptului de vot de către alegătorii români cu domiciliul sau reședința în străinătate (Bp. 203/2015***

Față de prevederile propunerii transmise, în scopul asigurării respectării cerințelor legislației din domeniul protecției datelor cu caracter personal, cu privire la prelucrarea datelor cu caracter personal având funcție de identificare, a unor categorii speciale de date și, în mod particular, cu privire la confidențialitatea și securitatea datelor, Autoritatea națională de supraveghere a formulat următoarele observații și propuneri:

În considerarea naturii datelor prelucrate și a faptului că sistemul de "vot prin corespondență" este un sistem bazat pe colectarea și prelucrarea, între altele, a unor date cu caracter special, prevăzute de art. 6 alin. (1) din propunere (codul numeric personal, datele actului care atestă cetățenia română) și de art. 18 alin. (1) din propunere (convingerile politice exprimate prin votul acordat), s-a subliniat că acest sistem trebuie să respecte drepturile și libertățile fundamentale, în special dreptul la viață privată. Astfel, datele menționate anterior se pot prelucra numai în condițiile restrictive stabilite prin art. 7 și art. 8 din Legea nr. 677/2001. Referitor la prelucrarea datelor privind convingerile politice, regula instituită de Legea nr. 677/2001 este că aceste categorii de date sunt interzise de la prelucrare, excepțiile fiind de strictă interpretare și aplicare.

Operatorii implicați în procesul de implementare a sistemului de vot prin corespondență au obligația informării persoanelor vizate (alegători) cu privire la prelucrarea datelor cu caracter personal, în condițiile art. 12 alin. (1) din Legea nr. 677/2001, prealabil obținerii consimțământului acestora, prevăzut de art. 6 alin. (1) din propunere.

Referitor la entitățile implicate în gestionarea Registrului alegătorilor români cu domiciliul sau reședința în străinătate, așa cum sunt prevăzute în art. 4, respectiv în art. 7 din propunere, s-a arătat că este necesară stabilirea responsabilităților și clarificarea calității acestora, respectiv de operatori sau împuterniciți, în sensul definițiilor date de Legea nr. 677/2001.

S-a apreciat că sistemul de "vot prin corespondență" va întâmpina dificultăți în a se asigura că doar persoanele autorizate vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor legale, iar în eventualitatea în care datele vor deveni disponibile unor terți, așa cum este prevăzut în art. 9, art. 11-12 din propunere (Biroul Electoral Central, Ministerul Administrației și Internelor, Compania Națională Imprimeria Națională S.A.), va fi dificilă menținerea standardului de confidențialitate și securitate adecvat pentru protejarea lor și, în consecință, drepturile fundamentale ale alegătorilor în cauză vor fi afectate.

Autoritatea națională de supraveghere a recomandat ca, pentru prelucrările de date din sistemul de vot prin corespondență, să se asigure standarde de securitate și de confidențialitate adecvate pentru protejarea datelor.

În acest context, s-a menționat că modalitatea de comunicare electronică și/sau prin poștă a datelor, mai cu seamă între alegători și entitățile implicate în procesul de implementare a sistemului de vot prin corespondență, poate expune comunicarea la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor.

În ceea ce privește prevederile art. 23 din propunerea legislativă transmisă, s-a propus ca acestea să fie completate, în sensul informării persoanelor vizate (alegătorii români cu domiciliul sau reședința în străinătate) cu privire la drepturile acestora în ceea ce privește prelucrarea datelor cu caracter personal, așa cum sunt prevăzute de art. 12 din Legea nr. 677/2001.

- **Institutul Național de Statistică a transmis spre avizare *proiectul de Hotărâre a Guvernului privind aprobarea Strategiei de dezvoltare a Sistemului Statistic Național și a statisticii oficiale a României în perioada 2015-2020.***

Față de conținutul strategiei sus-menționate, Autoritatea națională de supraveghere a formulat următoarele observații și propuneri:

Raportat la precizările extrem de generale efectuate, s-a apreciat că, pentru respectarea principiilor statuate de art. 4 din Legea nr. 677/2001, se impun mențiuni concrete cu privire la sfera instituțiilor publice din administrația centrală și locală care gestionează codul numeric personal și care vor permite accesul INS la înregistrări, în contextul statisticii privind populația, demografia și migrația internațională.

De asemenea, astfel cum a subliniat în mod constant Autoritatea națională de supraveghere, cu ocazia corespondenței anterioare privind modificarea cadrului legal al

statisticii oficiale, s-a reiterat faptul că implementarea unui astfel de sistem de colectare și prelucrare a datelor, inclusiv a celor speciale, presupune o prelucrare pe scară largă a acestora 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.

Astfel, întrucât în contextul extinderii utilizării surselor de date administrative, în vederea efectuării de statistici în diverse domenii, activitatea de prelucrare a datelor se va realiza prin participarea mai multor actori, trebuie ca viitoarele proiecte de acte normative să stabilească în mod clar rolul și responsabilitățile tuturor entităților implicate în colectarea și prelucrarea datelor personale.

Totodată, se impune luarea în considerare, inclusiv de la crearea sistemului informatic necesar colectării și prelucrării datelor, a tuturor principiilor instituite de art. 4 alin. (1) din Legea nr. 677/2001, modificată și completată, în special a celui privind caracterul adecvat, pertinent și neexcesiv prin raportare la scopul în care datele sunt colectate și ulterior prelucrate.

În același timp, întrucât se vor colecta date prin mijloace electronice, subliniem că, la alegerea modalităților de transmitere a datelor sau a documentelor ce conțin date cu caracter personal, 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.

Având în vedere faptul că pct. 3.2 din textul strategiei prevede necesitatea modificării cadrului juridic al statisticii oficiale, apreciem că viitoarele proiecte de acte normative trebuie să prevadă sau să întărească normele referitoare la protecția drepturilor și libertăților persoanelor, în ceea ce privește prelucrările de date cu caracter personal în acest domeniu.

Față de aspectele prezentate anterior, Autoritatea națională de supraveghere a avizat cu observații proiectul de Hotărâre a Guvernului privind aprobarea Strategiei de dezvoltare a Sistemului Statistic Național și a statisticii oficiale a României în perioada 2015-2020.

- **Ministerul Afacerilor Interne a transmis spre avizare *proiectul de Ordonanță a Guvernului privind utilizarea unor date din registrele cu numele pasagerilor pentru prevenirea și combaterea actelor de terorism, a infracțiunilor conexe acestora și a infracțiunilor contra securității naționale, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale.***

Față de textul proiectului ordonanței Guvernului transmis spre avizare, s-au formulat următoarele observații și propuneri:

Până la momentul actual, propunerea de Directivă privind utilizarea datelor pasagerilor pentru prevenirea, detectarea, cercetarea și reprimarea infracțiunilor de terorism și a infracțiunilor grave (așa-numita Directivă PNR) nu a fost aprobată la nivel european, membrii Parlamentului European respingând această propunere.

În acest context, Grupul de Lucru Articolul 29, prin scrisoarea din 19 martie 2015, adresată Comitetului LIBE din cadrul Parlamentului European cu privire la sistemul UE privind datele pasagerilor, atrage atenția, în principal, asupra următoarelor aspecte: demonstrarea necesității unui sistem PNR la nivel UE, respectiv asigurarea proporționalității prelucrării datelor.

În concordanță cu punctul de vedere sus-menționat, raportat la proiectul de Ordonanță supus analizei, Autoritatea națională de supraveghere a apreciat că implementarea unui astfel de sistem de colectare și prelucrare a datelor despre pasageri presupune o prelucrare 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, pentru respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață intimă, familială și privată.

Aceste riscuri subzistă, cu atât mai mult cu cât, în situația de față, lipsește o reglementare unitară la nivelul Uniunii Europene cu privire la utilizarea datelor pasagerilor, în alt scop decât cel al colectării inițiale.

De asemenea, aceasta implică colectarea unui volum foarte mare de date, motiv pentru care trebuie să se demonstreze clar că acest sistem are un caracter necesar, legitim și proporțional și că obiectivul său nu poate fi atins printr-un sistem mai puțin intruziv raportat la viața privată.

Legalitatea acestui sistem trebuie evaluată având în vedere principiile statuate în Carta drepturilor fundamentale ale Uniunii Europene, 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 (*Cauza S. și M. Marper contra Regatului Unit, 2008*).

De asemenea, principiile necesității și proporționalității acestui 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. Prin urmare, atunci când se propune și se concepe un nou sistem informatic la scară largă, acesta trebuie să respecte principiile necesității, proporționalității, responsabilității ("accountability principle"), evaluării impactului asupra domeniului protecției datelor („data protection impact assessment”), luării în considerare a vieții private începând din momentul conceperii („privacy by design”), stabilirii setărilor de confidențialitate la cel mai înalt nivel încă de la prima utilizare, („privacy by default”), limitării scopului, precum și regulile referitoare la notificarea breșelor de securitate („data breach notification”).

Totodată, s-a apreciat că este necesară analizarea impactului asupra drepturilor fundamentale, precum și a garanțiilor privind protecția datelor stabilite în proiectul de lege, asigurându-se în același timp și respectarea principiului transparenței decizionale.

În acest context s-a precizat că, prin similitudine, aceste aspecte au fost avute în vedere și de CJUE în decizia de invalidare a Directivei 2006/24/CE, precum și de Curtea Constituțională a României, la declararea ca neconstituțională a Legii nr. 82/2012. Ca atare, s-a recomandat ca, la reanalizarea acestui proiect de lege, să se aibă în vedere principiile și garanțiile indicate de forul constituțional suprem în Decizia nr. 440/2014.

În ceea ce privește textul proiectului de ordonanță, raportat la complexitatea reglementării, precum și la termenul scurt de solicitare a avizului, au fost formulate, în principal, următoarele observații:

La art. 2, este necesară definirea UNIP, precum și a datelor PNR, acest din urmă termen fiind necesar a fi pus în concordanță cu prevederile de la art. 1 (1) care reglementează domeniul de aplicare al ordonanței. Este necesară și definirea Sistemului de evidență a datelor PNR în concordanță cu art. 7, precum și a autorităților competente.

De asemenea, s-a solicitat clarificarea entității care are calitatea de operator și menționarea exactă a acesteia, raportat la art. 4 alin. (7) și art. 8 din proiect, precum și la definiția dată de art. 3 lit. e) din Legea nr. 677/2001.

În acest context, legat de categoriile de date despre pasageri ce se regăsesc la art. 5 și care sunt identice cu cele conținute în propunerea de directivă privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave (neadoptată) și raportat la opinia Grupului de Lucru Art. 29 (WP 181/2011), s-a apreciat că lista de elemente ale datelor despre pasageri trebuie redusă.

La art. 9 s-a semnalat, de asemenea, lipsa unei clarități cu privire la procedura de evaluare sub aspectul momentului evaluării (alin. 1), al transmiterii către autoritățile competente (alin. 3), al cazului concret. În acest sens, s-a apreciat că procedura poate fi detaliată numai prin norme metodologice, publicate în Monitorul Oficial.

De asemenea, cu privire la sintagma „anonimizarea prin mascarea lor”, a fost evidențiat faptul că termenul „mascarea” nu este în concordanță cu tehnica de „anonimizare”. Având în vedere aceste aspecte, s-a subliniat că se impun a fi luate toate măsurile necesare pentru protejarea datelor astfel încât elementele de identificare să nu fie divulgate.

În ceea ce privește perioada de stocare a datelor PNR (art. 15), trebuie avute în vedere dispozițiile Legii nr. 677/2001 potrivit cărora stocarea datelor nu trebuie să depășească perioada necesară îndeplinirii scopului, precum și reanalizarea textului în vederea reducerii termenului stabilit. În același timp, s-a propus inserarea unei dispoziții referitoare la responsabilitatea operatorului de a analiza periodic, la o anumită perioadă de timp de la începerea prelucrării, necesitatea stocării datelor cu caracter personal, precum și la obligația de a stoca datele doar pe perioada necesară.

Prin raportare la propunerea de la art. 16 privind interzicerea prelucrării datelor cu caracter special, s-a precizat că deși acesta nu conține în mod expres date cu caracter special, acestea pot fi deduse din anumite categorii de date cum ar fi, spre exemplu, la alin. 2 lit. (a) „situația de călătorie...” sau la lit. (e) „istoricul tuturor modificărilor datelor prevăzute la alin. (1), precum și ale celor prevăzute la lit. (a)-(d)”. Astfel, pot fi obținute informații privind convingerile religioase, informații privind starea de sănătate etc.

La art. 15 alin. (7) lit. a) nu reiese cu claritate modalitatea de calcul a termenului de 5 ani.

Referitor la art. 17 alin. (2), sintagma „orice date suplimentare față de cele prevăzute la art. 5” este neclară, întrucât câmpurile sunt predefinite și, prin urmare, devine imposibilă colectarea altor categorii de date față de cele prestabilite.

La art. 18 alin. (8) și (9), cu privire la exercitarea drepturilor de către persoanele vizate, s-a recomandat să se analizeze necesitatea evidențierii situației în care nu se poate da curs cererilor formulate în exercitarea dreptului de acces, după modelul propus la art. 39 în proiectul de regulament Europol. La art. 21 alin. (5) s-a propus corelarea acestuia cu dispozițiile art. 20, care stabilește competențele Autorității naționale de supraveghere în ceea ce privește constatarea contravențiilor și aplicarea sancțiunilor. De asemenea, s-a propus completarea textului cu obligația de informare a Autorității naționale de supraveghere cu privire la întocmirea rapoartelor anuale și publicarea acestora.

În consecință, față de textul proiectului de ordonanță supus analizei, Autoritatea națională de supraveghere a apreciat că implementarea unui astfel de sistem de evidență poate reprezenta o nouă situație de risc pentru protecția datelor cu caracter personal ale persoanelor fizice și, implicit, pentru respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață intimă, familială și privată cu privire la prelucrarea datelor cu caracter personal.

Având în vedere aspectele de mai sus, s-a precizat că proiectul de ordonanță în forma transmisă necesită reanalizarea acestuia sub aspectul observațiilor menționate anterior, în special în considerarea necesității și proporționalității prelucrărilor de date personale preconizate. Totodată, s-a apreciat că este necesară finalizarea procesului de adoptare la nivelul Uniunii Europene a noului pachet legislativ privind protecția datelor cu caracter personal, anterior adoptării unui astfel de act normativ intern fiind necesare garanții substanțiale de protecție a datelor, raportat la scopul proiectului.

Inițiatorul nu a preluat nicio observație dintre cele efectuate de Autoritatea națională de supraveghere, ordonanța fiind adoptată în ședință de Guvern în forma transmisă de inițiator spre avizare.

- **Autoritatea Națională pentru Turism a transmis spre avizare *proiectul de Hotărâre a Guvernului pentru aprobarea implementării Sistemului Informativ Integrat de Evidență a Turiștilor și a Normelor cu privire la accesul, evidența și protecția turiștilor în structuri de primire turistice cu funcțiuni de cazare.***

Față de prevederile proiectului transmis spre avizare, întrucât acesta nu a parcurs etapa consultării preliminare interinstituționale, potrivit Cap. IV din Regulamentul aprobat prin HG nr.

561/2009, Autoritatea națională de supraveghere a formulat următoarele observații și propuneri:

Activitățile ce urmează a fi desfășurate în cadrul acestui sistem de evidență de către entitățile implicate presupun efectuarea de prelucrări de date cu caracter personal (inclusiv date cu caracter special, cum este seria și nr. cărții de identitate) ale persoanelor fizice.

Ca atare, este necesară luarea în considerare a principiilor de protecție a datelor statuate de art. 4 alin. (1) din Legea nr. 677/2001, stabilirea garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate și identificarea responsabilităților și a modalităților de acces la date al tuturor actorilor implicați, raportat la competențele legale ale acestora, precum și clarificarea calității lor, respectiv de operatori sau împuterniciți, în sensul definițiilor date de Legea nr. 677/2001.

Astfel, raportat la mențiunile de la art. 2 alin. (2) din proiect, privind gestionarea și auditarea sistemului SIET de către Serviciul de Telecomunicații Speciale (STS), aceste activități implică prelucrări de date cu caracter personal în calitate de responsabil al acestei bazei de date naționale. În acest sens, este necesară clarificarea calității STS de operator sau împuternicit, potrivit definițiilor date de art. 3 lit. e) și f) din Legea nr. 677/2001 și raportat la obligațiile de securitate și confidențialitate a datelor stabilite de art. 20 din aceeași lege.

Se impune identificarea atribuțiilor legale potrivit cărora STS are calitatea de a gestiona și audita sistemul SIET, precum și menționarea acestora în nota de fundamentare, ținând cont de faptul că prezentul proiect de act normativ este emis pe baza și în executarea legii, fiind subsecvent acesteia. Aceleași aspecte se impun a fi luate în considerare și cu privire la atribuțiile Ministerului Afacerilor Interne.

De asemenea, trebuie stabilit concret calitatea de operator sau împuternicit a Autorității Naționale de Turism și a operatorilor economici (precum și a structurilor de primire) în cadrul acestui sistem național de evidență, având în vedere faptul că aceste entități sunt calificate drept utilizatori ai sistemului, deși operatorii economici introduc date în SIET și sunt responsabili pentru această activitate.

La art. 2 alin. (3) lit. b) astfel cum este redactat textul, nu se înțelege dacă operatorii economici au acces numai la datele personale introduse de fiecare în parte sau și la cele introduse de alți operatori, sens în care este necesară modificarea formulării, pentru o mai mare claritate. Totodată, remarcăm faptul că nu există dispoziții tranzitorii în textul proiectului de hotărâre care să reglementeze precizările de la pct. 2 din Nota de fundamentare.

În ceea ce privește Normele prevăzute în Anexa nr. 1, la art. 1 alin. (3), este necesară completarea acestui text, pentru eliminarea ambiguității și prevenirea unei practici neunitare, cu trimiteri la dispozițiile art. 2 alin. (3) care enumeră actele de identitate acceptate.

Referitor la enumerarea categoriilor de persoane asupra cărora vor fi anunțate organele de poliție, de la art. 6 alin. (2), precizăm că formularea "precum și a altor persoane cunoscute ca traficanti, turbulenți, prostituate, proxeneți etc." nu este adecvată întrucât denotă ambiguitate, putând conduce în practică la o aplicare neunitară, printr-o apreciere subiectivă și la apariția, în consecință, a unor situații de încălcare a drepturilor fundamentale ale persoanelor fizice. În acest sens, propunem reformularea textului sau eliminarea acestei sintagme.

De asemenea, referitor la prelucrarea datelor cu caracter personal având funcție de identificare, respectiv prelucrarea seriei și numărului cărții de identitate, în considerarea prevederilor art. 8 din Legea nr. 677/2001 și ale Deciziei Autorității naționale de supraveghere nr. 132/2011 (publicată în M. Of. nr. 929 din 28.12.2011), apreciem că este oportună completarea Notei de fundamentare cu justificarea necesității prelucrării acestor informații în Anexa nr. 2 a proiectului.

Autoritatea națională de supraveghere a apreciat că se impune reanalizarea textului proiectului de Hotărâre, ținând cont de observațiile și propunerile de mai sus.

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

Solicitarea de avize pentru instalarea de sisteme de supraveghere video

1. Pe parcursul anului 2015, la nivelul Autorității naționale de supraveghere s-au înregistrat mai multe solicitări din partea unor unități școlare, care privesc acordarea avizului autorității privind instalarea sistemelor de supraveghere video, raportat la dispozițiile art. 8 alin. (3) din Decizia nr. 52/2012, în unele birouri, cancelarii, precum și în sălile de clasă (pe tot parcursul anului școlar).

Față de aceste solicitări, Autoritatea națională de supraveghere nu a acordat avizul în vederea instalării sistemelor de supraveghere video, în considerarea următoarelor aspecte, comunicate în scris unităților de învățământ solicitante:

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilități de înregistrare și stocare a imaginilor și datelor se supune atât prevederilor Legii nr. 677/2001, modificată și completată, ale Deciziei nr. 52/2012 privind

prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, cât și celor ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată.

De asemenea, aceeași lege menționată anterior stabilește în mod expres și anumite situații de excepție de la obligativitatea obținerii consimțământului în cazul prelucrării datelor personale. Printre aceste cazuri de excepție, reglementate de art. 5 alin. (2) din Legea nr. 677/2001, modificată și completată, se numără și cel când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate.

În conformitate cu dispozițiile legale de mai sus, art. 3 coroborat cu art. 6, art. 8 și art. 9 din Decizia nr. 52/2012 prevede că prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video se efectuează cu respectarea regulilor generale prevăzute la art. 4 din Legea nr. 677/2001, cu modificările și completările ulterioare, în special a principiului proporționalității scopului și cu consimțământul persoanei vizate sau în alte condiții de excepție prevăzute de lege.

Prin urmare, se poate recurge la o monitorizare prin supraveghere video, în temeiul dispozițiilor legale de mai sus, numai dacă această măsură este proporțională cu riscurile cu care se confruntă operatorul și determină luarea unei asemenea măsuri intruzive în viața privată. În același timp, trebuie să se țină cont și de interesele, drepturile și libertățile persoanelor vizate (cadrele didactice, elevii etc.).

Astfel, pe de o parte, în ceea ce privește angajații (cadrele didactice), întrucât implementarea unui sistem de supraveghere video poate afecta drepturile lor în calitate de angajați, în plus față de dispozițiile Legii nr. 677/2001, modificată și completată, și ale art. 8 din Decizia nr. 52/2012, trebuie respectate și cele prevăzute de Codul Muncii, precum și Statutul cadrelor didactice.

În acest context, precizăm că art. 8 din Decizia nr. 52/2012 stabilește situațiile în care prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video este permisă, și anume: pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

Alin. (3) al aceluiași articol din Decizia nr. 52/2012 prevede că „nu este permisă prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video în

interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă, cu excepția situațiilor prevăzute expres de lege sau a avizului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal”.

Art. 9 din Decizia nr. 52/2012 stabilește că prelucrarea datelor cu caracter personal ale minorilor prin mijloace de supraveghere video, inclusiv dezvăluirea acestora, este permisă cu acordul expres al reprezentantului legal sau în situațiile prevăzute la art. 5 alin. (2) din Legea nr. 677/2001, cu modificările și completările ulterioare, cu respectarea drepturilor acestora, în special a informării prealabile.

În acest context, dispozițiile art. 27 din Legea nr. 272/2004 privind protecția și promovarea drepturilor copilului, republicată, garantează copilului dreptul la protejarea imaginii sale publice și a vieții sale private, fiind interzisă orice acțiune de natură să afecteze imaginea publică a copilului sau dreptul acestuia la viață privată.

Potrivit aceleiași legi (art. 24), copilul capabil de discernământ are dreptul de a-și exprima liber opinia asupra oricărei probleme care îl privește, precum și de a fi ascultat, consultat și informat asupra consecințelor oricărei decizii care îl privește.

Totodată, Ordinul Ministerului Educației Naționale nr. 4430/2014 privind organizarea și desfășurarea examenului de bacalaureat – 2015 - stabilește la art. 6 alin. (1) următoarele:

“Comisiile de bacalaureat județene/a municipiului București asigură dotarea cu camere de supraveghere video și audio funcționale a sălilor în care se desfășoară probele examenului de bacalaureat național, a sălilor în care se descarcă și se multiplică subiectele, precum și a sălilor în care se preiau, se evaluează și se depozitează lucrările scrise”.

Având în vedere dispozițiile legale de mai sus, prin raportare la conținutul solicitărilor unităților de învățământ, Autoritatea națională de supraveghere a apreciat faptul că există temei legal pentru efectuarea supravegherii video în sălile de clasă numai pe perioada desfășurării examenelor naționale.

În ceea ce privește efectuarea supravegherii video în sălile de clasă, în alte perioade decât cele ale desfășurării examenelor naționale, precum și a supravegherii video în birouri și cancelarii, unitățile de învățământ solicitante ale avizelor nu au prezentat 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, nu s-a făcut dovada faptului că a fost efectuată consultarea sindicatului sau a reprezentanților angajaților și nici dovada obținerii consimțământului expres și neechivoc al tuturor angajaților, precum și al reprezentanților legali ai minorilor.

De asemenea, nu s-a indicat explicit scopul și nu s-a argumentat suficient 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.

În acest context subliniem că, în jurisprudența Curții Europene a Drepturilor Omului referitoare la art. 8 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale (dreptul la respectarea vieții private și de familie), instanța europeană a statuat faptul că „nu este întotdeauna posibil să se facă o diferențiere netă între activitățile individului, care fac parte din viața sa profesională, și acelea care nu intră în această categorie.” (Cauza Niemietz contra Germaniei, 16 decembrie 1992) și că 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 (Cauza S. și M. Marper contra Regatului Unit, 4 decembrie 2008).

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.

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.

Având în vedere cele de mai sus și ținând cont de necesitatea asigurării unei protecții eficiente a dreptului fundamental la viață privată al persoanelor monitorizate prin utilizarea mijloacelor de supraveghere video, Autoritatea națională de supraveghere consideră că avizul solicitat în temeiul art. 8 alin. (3) din Decizia nr. 52/2012 poate fi acordat în mod excepțional, numai cu respectarea tuturor condițiilor mai sus enunțate și numai pentru situații temeinic justificate și dovedite.

Față de solicitările unităților de învățământ referitoare la acordarea avizului Autorității naționale de supraveghere privind instalarea sistemelor de supraveghere video, instituția

noastră a transmis punctul de vedere Ministerului Educației și Cercetării Științifice, cu recomandarea comunicării acestuia către inspectoratele școlare și, implicit, către toate unitățile de învățământ, pentru ca solicitările de avize din partea acestora din urmă să îndeplinească condițiile legale anterior precizate.

2. O societate comercială a solicitat, în temeiul Deciziei nr. 52/2012, acordarea avizului în scopul prelucrării prin mijloace de supraveghere video a datelor cu caracter personal ale propriilor angajați ce își desfășoară „activitatea de vânzări prin telefon (telesales)” în birouri.

Față de solicitarea transmisă s-au făcut următoarele precizări:

Art. 8 din Decizia nr. 52/2012 stabilește situațiile în care prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video este permisă, și anume: pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

De asemenea, în afara situațiilor de mai sus, prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video se poate efectua pe baza consimțământului expres și liber exprimat al acestora, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

În ceea ce privește însă prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video în interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă, s-a subliniat că aceasta nu este permisă decât în situațiile prevăzute expres de lege sau pe baza avizului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (art. 8 alin. (3) din Decizia nr. 52/2012).

Ca atare, supravegherea video în interiorul birourilor nu se poate efectua decât în situațiile expres prevăzute într-un act normativ care obligă neechivoc angajatorul la instituirea sistemelor de supraveghere video sau în situațiile autorizate de Autoritatea națională de supraveghere, potrivit art. 8 alin. (3) din Decizia nr. 52/2012, în situații temeinic justificate.

În ceea ce privește angajații, întrucât implementarea unui astfel de sistem de supraveghere video poate afecta drepturile lor în calitate de salariați, pe lângă dispozițiile Legii nr. 677/2001 și ale art. 8 din Decizia nr. 52/2012, trebuie respectate și cele prevăzute de Codul muncii. În acest sens, anterior implementării unui astfel de sistem se impune o justificare temeinică a luării acestei măsuri concomitent cu consultarea sindicatului sau a reprezentanților salariaților.

De asemenea, în Preambulul Recomandării nr. R (89)2 a Comitetului de Miniștri al Consiliului European, 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 procedurilor tehnologice, dacă nu este reamintit faptul că angajații sunt înaintea 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 tehnicilor de prelucrare a datelor care permit să stabilească profilul angajaților sau luarea deciziilor fondate pe prelucrarea automată".

Având în vedere prevederile normative sus-menționate, precum și situația descrisă de operator, s-a apreciat că, pe de o parte, nu există obligație legală expresă a cărei îndeplinire să conducă la prelucrarea datelor cu caracter personal ale 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 a angajaților și care să prevaleze față de drepturile și libertățile fundamentale sau interesele acestora.

În contextul celor sus-menționate 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 datelor lor cu caracter personal, s-a precizat că situația prezentată de operator nu justifică acordarea avizului Autorității naționale de supraveghere, în temeiul art. 8 alin. (3) din Decizia nr. 52/2012.

Solicitarea de opinii

a) Cu privire la utilizarea de dispozitive de geolocalizare a vehiculelor folosite de angajați

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 vehiculului utilizat de către salariatul său, chiar dacă scopul principal al prelucrării este cel al protecției bunurilor societății de eventuale furturi.

Prin urmare, societatea care dorește să recurgă la astfel de sisteme de localizare geografică a vehiculelor intră sub incidența dispozițiilor Legii nr. 677/2001 și a Deciziei nr. 200/2015.

În sensul celor de mai sus, întrucât astfel de dispozitive de geolocalizare comportă anumite riscuri în privința drepturilor și libertăților persoanei care conduce vehiculul monitorizat (angajatul), înainte de instalarea unor astfel de sisteme de supraveghere, angajatorul trebuie să facă 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. Totodată, întrucât pot fi afectate drepturile salariaților, este necesară și consultarea organismelor reprezentative ale acestora.

Sub aspectul obligației de notificare, s-a precizat că pentru această activitate este necesară completarea și depunerea notificării la Autoritatea națională de supraveghere.

***b) Cu privire la instalarea unui sistem de supraveghere video
în sălile de naștere ale unui spital***

Potrivit Legii nr. 677/2001, regula este aceea că prelucrarea datelor personale ale unei persoane fizice, de către o altă persoană fizică sau juridică, în calitate de operator, se efectuează numai cu consimțământul persoanei în cauză, dat în mod expres și neechivoc. De asemenea, aceeași lege menționată anterior stabilește în mod expres și anumite situații de excepție de la obligativitatea obținerii consimțământului în cazul prelucrării datelor personale, reglementate de art. 5 alin. (2) din Legea nr. 677/2001, modificată și completată.

În același timp, art. 7 din Legea nr. 677/2001 stabilește ca regulă generală interzicerea prelucrării datelor personale privind starea de sănătate, viața sexuală, originea etnică și altele.

În conformitate cu dispozițiile legale de mai sus, art. 3 coroborat cu art. 6 din Decizia nr. 52/2012 stabilește că prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video se efectuează cu respectarea regulilor generale prevăzute la art. 4 din Legea nr. 677/2001, cu modificările și completările ulterioare, în special a principiului proporționalității prelucrărilor efectuate raportat la scopul propus.

Prin urmare, s-a comunicat că nu se poate recurge la o monitorizare prin supraveghere video, decât în temeiul dispozițiilor legale de mai sus și numai dacă această măsură este proporțională cu riscurile cu care se confruntă operatorul, astfel încât să se justifice luarea unei asemenea măsuri intruzive în viața privată. În același timp, trebuie să se țină cont și de interesele, drepturile și libertățile persoanelor vizate (angajații spitalului, pacientele și copiii), raportat la dreptul la viață privată al acestora ocrotit de art. 26 din Constituția României.

În același timp, în ceea ce privește angajații (cadrele medicale și personalul auxiliar), întrucât implementarea unui sistem de supraveghere video poate afecta drepturile lor în calitate de angajați, în plus față de dispozițiile Legii nr. 677/2001 și ale art. 8 din Decizia nr. 52/2012, trebuie respectate și cele prevăzute de Codul Muncii.

Totodată, raportat la situația prezentată referitoare la intenția unei unități medicale de a instala camere video în sălile de naștere, s-a precizat că art. 5 alin. (4) din Decizia nr. 52/2012 prevede că "este interzisă prelucrarea datelor cu caracter personal prin mijloace de supraveghere video în spații în care se impune asigurarea intimității persoanelor", iar camerele individuale de naștere fac parte din această categorie de spații.

Mai mult, art. 9 din Decizia nr. 52/2012 stabilește că prelucrarea datelor cu caracter personal ale minorilor prin mijloace de supraveghere video, inclusiv dezvăluirea acestora, este permisă cu acordul expres al reprezentantului legal sau în situațiile prevăzute la art. 5 alin. (2) din Legea nr. 677/2001, cu respectarea drepturilor acestora, în special a informării prealabile.

Având în vedere textele legale sus menționate, prin raportare la conținutul solicitării, s-a subliniat că nu sunt îndeplinite condițiile de prelucrare a datelor cu caracter personal prevăzute de Legea nr. 677/2001 și de Decizia nr. 52/2012.

***c) Cu privire la legalitatea solicitării, de către o asociație de proprietari,
a copiei cărții de identitate***

Legea nr. 677/2001 stabilește condițiile în care datele cu caracter personal pot fi prelucrate, inclusiv dezvăluite, regula generală ce guvernează prelucrarea datelor personale fiind consimțământul persoanei în cauză, dat în mod expres și neechivoc.

În mod excepțional însă, datele cu caracter personal pot fi prelucrate (inclusiv dezvăluite) fără consimțământul persoanei vizate, în mai multe situații de excepție. Aceste cazuri sunt menționate în mod expres la art. 5 alin. (2) din Legea nr. 677/2001.

Referitor la codul numeric personal, potrivit art. 8 din Legea nr. 677/2001, modificată și completată, prelucrarea (inclusiv dezvăluirea) acestuia și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală 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 cu avizul Autorității naționale de supraveghere.

În acest context, pentru clarificarea și detalierea modalității de prelucrare a codului numeric personal, precum și reținerii copiei cărții de identitate, Autoritatea națională de supraveghere a emis Decizia nr. 132/2011.

În privința copiei cărții de identitate, art. 6 din decizia sus-menționată interzice colectarea acesteia, cu excepția situațiilor de la art. 2 al deciziei: consimțământul persoanei vizate, o prevedere legală expresă sau avizul Autorității naționale de supraveghere.

Precizăm că, în ceea ce privește evidența locatarilor prin cartea de imobil, potrivit Hotărârii Guvernului nr. 1375/2006 privind aprobarea Normelor metodologice din 4 octombrie 2006 de aplicare unitară a dispozițiilor legale privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, responsabilul cărții de imobil are atribuția de a solicita persoanelor care locuiesc în imobil prezentarea actelor de identitate, în termen de 15 zile de la sosire, în vederea înscrierii datelor în cartea de imobil.

Totodată, înscrierea persoanelor în cartea de imobil se face în baza actului de identitate, iar pentru copiii sub 14 ani, în baza certificatului de naștere.

Instruirea responsabililor cărții de imobil se face de către polițistul de ordine publică anume desemnat de șeful unității de poliție pe a cărei rază teritorială este situat imobilul.

În consecință, Autoritatea națională de supraveghere a apreciat că solicitarea copiei cărții de identitate de către asociația de proprietari nu se încadrează în condițiile stabilite de prevederile legale amintite.

d) Cu privire la condițiile prelucrării de date cu caracter personal din surse publice

Față de conținutul acestei solicitări, s-au făcut următoarele precizări:

Art. 5 alin. (1) din Legea nr. 677/2001, modificată și completată, prevede că prelucrarea datelor cu caracter personal poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.

În același timp, la art. 5 alin. (2) sunt prevăzute situațiile în care datele pot fi prelucrate fără consimțământul persoanei vizate (cum este, spre exemplu, cea de la lit. f), respectiv „când prelucrarea privește date obținute din documente accesibile publicului”).

În contextul celor de mai sus, persoana a fost informată că art. 12 alin. (2) din Legea nr. 677/2001 prevede că, în cazul în care datele prelucrate de un operator nu sunt obținute direct de la persoana vizată, acesta este obligat ca, în momentul colectării datelor, dacă se

intenționează dezvăluirea acestora către terți, să furnizeze persoanei vizate, cel mai târziu până în momentul primei dezvăluiri (respectiv înainte de prima postare „pe o altă pagină web”), informațiile referitoare la identitatea operatorului, scopul în care se face prelucrarea datelor, categoriile de date vizate și destinatarii lor, existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care acestea pot fi exercitate.

În consecință, dezvăluirea pe „o altă pagină web”, de date personale colectate din surse publice, trebuie să respecte dispozițiile legale sus-menționate.

e) Cu privire la condițiile legale de dezvăluire a unor date personale către o asociație care apără drepturile persoanelor ce suferă de o anumită afecțiune

Regula instituită de Legea nr. 677/2001, modificată și completată, este aceea că prelucrarea datelor personale ale unei persoane fizice (inclusiv dezvăluirea acestora) de către o altă persoană fizică sau juridică, în calitatea sa de operator, se efectuează numai cu consimțământul persoanei în cauză, dat în mod expres și neechivoc.

În măsura în care se solicită și date privind starea de sănătate, condițiile de prelucrare a informațiilor privind starea de sănătate a unei persoane sunt stabilite în art. 7 și 9 din Legea nr. 677/2001, modificată și completată.

Astfel, regula în privința datelor legate de starea de sănătate este aceea că astfel de informații sunt interzise de la prelucrare (inclusiv de la dezvăluire). În anumite cazuri de excepție, cum ar fi consimțământul persoanei vizate ori alte cazuri expres stabilite de lege, prelucrarea acestor date este permisă.

Unele dintre cazurile de excepție de la consimțământ sunt cele în care prelucrarea datelor (inclusiv dezvăluirea) este necesară pentru protecția vieții, integrității fizice sau sănătății persoanei vizate sau a altei persoane, în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată (asiguratul), pentru protecția sănătății publice, prevenirea unui pericol iminent, prevenirea săvârșirii unor fapte penale etc. (art. 7 alin. (2) coroborat cu art. 9 din Legea nr. 677/2001).

Totodată, legea instituie și condiția ca prelucrarea datelor privind starea de sănătate să fie efectuată de către ori sub supravegherea unui cadru medical supus secretului profesional

sau de către ori sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul (art. 7 alin. (2) lit. g) coroborat cu art. 9 alin. (2) din Legea nr. 677/2001).

În același timp, potrivit art. 7 alin. (3) din aceeași lege menționată mai sus, excepțiile de la regula obținerii consimțământului persoanei vizate cu privire la prelucrarea datelor sale privind starea de sănătate nu aduc atingere dispozițiilor legale care reglementează obligația autorităților publice de a respecta și de a ocroti viața intimă, familială și privată.

În consecință, datele solicitate de către asociație pot fi dezvăluite numai pe baza consimțământului persoanelor fizice în cauză sau în condițiile legale de excepție prezentate mai sus, cu respectarea principiului proporționalității scopului.

✚ **Puncte de vedere privind unele cauze aflate la Curtea de Justiție a Uniunii Europene**

În anul 2015 au fost transmise puncte de vedere ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în mai multe cauze pendinte în fața Curții de Justiție a Uniunii Europene, referitoare la interpretarea anumitor articole din Directiva 95/46/CE, astfel:

- **Cauza C-191/15** privind interpretarea art. 4 alin. (1) lit. a) din Directiva 95/46/CE;
- **Cauza C-192/15** privind interpretarea art. 4 alin. (1) lit. c) precum și art. 28 alin. (3) și alin. (4) din Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- **Cauza C-203/15** privind interpretarea art. 15 alin. (1) din Directiva 2002/58/CE aflată pe rolul Curții de Justiție a Uniunii Europene.

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

Urmare a finalizării unor acțiuni în instanță, promovate de către o serie de operatori sancționați de Autoritatea națională de supraveghere pe parcursul anului 2015, prezentăm mai jos câteva cazuri relevante:

❖ **Hotărâre pronunțată privind refuzul Google Inc. de ștergere a unor link-uri la accesarea cărora sunt furnizate date despre o persoană fizică**

O persoană fizică a sesizat Autoritatea națională de supraveghere asupra faptului că sunt publicate date cu caracter personal (respectiv poze, informații false și defăimătoare) pe mai multe pagini web, de către o persoană necunoscută. Datele se refereau la presupuse acuzații ce

vizau o relație între petent și o persoană de sex feminin din mediul virtual, care a pretins că este studentă și care ar fi solicitat ajutor privind obținerea unei diplome false.

Aceste acuzații, susținea petentul, i-au cauzat grave prejudicii de imagine.

Ulterior, prin Raportul Comisiei de Etică a Universității al cărei cadru didactic este petentul, faptele s-au dovedit a fi nereale, nefondate și neprobate, astfel că persoana vizată s-a adresat Google Inc. din Statele Unite ale Americii cu solicitarea de a șterge datele sale cu caracter personal din motorul de căutare.

Pentru unele dintre link-uri, Google Inc. i-a răspuns petentului că se lucrează la blocarea celor referitoare la numele său, însă pentru alte link-uri cererea a fost respinsă pe motivul că articolele de presă publicate în motorul de căutare au legătură cu chestiuni de interes public legate de viața personală a petentului, iar informațiile sunt de interes public.

Autoritatea națională de supraveghere a analizat plângerea persoanei vizate și documentele doveditoare, a constatat faptul că aceasta este întemeiată și a solicitat Google Inc. să șteargă o serie de link-uri indicate.

Google Inc. a refuzat să dea curs solicitării Autorității naționale de supraveghere și a atacat în instanță actul prin care i se cerea ștergerea link-urilor, susținând că "Societatea nu a fost informată nici cu privire la conținutul concret al petițiilor soluționate, nici cu privire la considerentele avute în vedere de autoritate la emiterea adresei".

De asemenea, Google Inc. a "considerat totuși că nu se impune eliminarea unor rezultate ale căutărilor referitoare la numele petiționarului...", raportat la caracterul informativ, respectiv jurnalistic al rezultatelor căutării, statutul de persoană publică și implicată politic al petiționarului, precum și faptul că acesta prestează o activitate de interes public.

Instanța a respins cererea Google Inc., confirmând astfel argumentele Autorității naționale de supraveghere potrivit cărora plângerea persoanei vizate era întemeiată.

Astfel, instanța a constatat faptul că, "strict teoretic, petentul se încadrează în categoria persoanelor ce au avut un rol în viața publică, dar la acest moment, al judecării prezentei cauze, acest rol nu este dovedit a se fi perpetuat".

De asemenea, instanța a apreciat că, pentru clarificarea problemei, esențiale sunt două aspecte, și anume dacă datele a căror dezindexare se solicită sunt exacte și actuale.

Cu privire la exactitatea datelor, instanța a reținut faptul că, prin hotărârea Comisiei de Etică a Universității al cărei cadru didactic este petentul, "s-au dovedit a fi nereale, nefondate și neprobate acuzațiile aduse persoanei vizate".

Astfel, instanța a statuat faptul că *“raportat la soluția la care a ajuns un for decizional al Universității (...), se impunea ca reclamanta să dea curs cererii petentului de ștergere a linkurilor respective, întrucât persoana vizată s-a dovedit a fi nevinovată. Mai mult, persoana vizată a avut de suferit deja prejudicii de imagine prin faptul că mass-media, înainte de a se pronunța un for decizional asupra vinovăției sau nevinovăției acesteia, a dat publicității, în mediul virtual, unele știri care au condus deja la atingeri aduse vieții intime, familiale și private a petentului. Or, în măsura în care persoana vizată s-a dovedit că nu este vinovată de acuzațiile care i s-au adus, și chiar și mass-media a publicat informații cu privire la Raportul Comisiei de Etică a Universității (...), nu mai există niciun motiv întemeiat ca informațiile în cauză să fie expuse în mediul on-line la infinit, fără să se ia măsura ștergerii lor.”*

Cu privire la caracterul actual al datelor, instanța a reținut că *“(…) dacă la momentul publicării acestor informații, petentul avea calitatea de cadru didactic universitar, precum și pe aceea de candidat la funcția de primar (...), precum și la demnitatea de senator (...), la momentul de față aceste calități nu se mai mențin (...); de la data producerii presupuselor evenimente, anul 2013, au trecut mai bine de 3 ani, astfel că necesitatea informării publicului după acest timp nu mai apare ca fiind la fel de justificată”.*

De asemenea, instanța a arătat că *“aceste informații nu sunt din categoria celor făcute public manifest de persoana vizată cum sunt cele din CV-ul acesteia sau imaginea făcută publică în contextul alegerilor electorale din anul 2012, astfel că nu se mai justifică menținerea lor în sistemul de evidență a motorului de căutare. Prin publicarea pe Internet, datele personale devin accesibile unui număr nedefinit de persoane, iar în aceste condiții persoana vizată nu are cunoștință de entitățile care preiau, ulterior, informațiile cu privire la persoana sa și de modul cum le utilizează mai departe. Impactul potențial al mijlocului de comunicare utilizat are o importanță deosebită, astfel că publicarea unor știri în mediul on-line are un impact mult mai mare decât în presa scrisă, având un efect mai rapid și mai puternic în ceea ce privește difuzarea informațiilor și preluarea ulterioară a acestora de către diverse entități.”*

Totodată, instanța a statuat faptul că *“Interesul persoanei vizate de a obține ștergerea datelor sale personale dezvăluite pe Internet prevalează asupra interesului economic al operatorului de a publica datele, așa cum a reținut și CJUE în Cauza C-131/12.”*, astfel că *“nu se aplică excepția reglementată de art. 5 (2,e) din Legea nr. 677/2001”.*

❖ Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal de către o entitate specializată în producerea și comercializarea produselor din tutun

Autoritatea națională de supraveghere a fost sesizată cu posibile încălcări ale prevederilor Legii nr. 677/2001 prin colectarea excesivă a CNP-ului în cadrul campaniilor promoționale derulate de către o entitate privată specializată în producerea și comercializarea produselor din tutun. În urma investigației efectuate s-a constatat faptul că operatorul controlat prelucrează date în scop de marketing direct, prin împuternicit, pentru promovarea produselor și mărcilor proprii de tutun.

Autoritatea națională de supraveghere a emis un proces-verbal de constatare/sanționare prin care s-a constatat săvârșirea de către operatorul controlat a următoarelor fapte contravenționale:

- omisiunea de a notifica și notificarea cu rea-credință, prevăzută de art. 31 din Legea nr. 677/2001, sub forma notificării incomplete, întrucât operatorul nu și-a completat corespunzător notificarea până la data întocmirii procesului-verbal cu toate informațiile privind categoriile de date personale, pe care le prelucrează în desfășurarea campaniilor promoționale și a activității de marketing, și categoriile de destinatari, conform constatărilor din procesul-verbal, așa cum prevede art. 22 din Legea nr. 677/2001;

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 4 alin. (1) lit. c), d) și e) din Legea nr. 677/2001, întrucât operatorul a colectat și stocat excesiv date personale, inclusiv codul numeric personal, al persoanelor participante la diverse acțiuni promoționale ale produselor sale de tutun, desfășurate până la data întocmirii procesului-verbal, prin raportare la scopul declarat al prelucrării;

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 12 alin. (1) din Legea nr. 677/2001, întrucât operatorul, până la data întocmirii procesului-verbal, nu a asigurat o informare corectă a persoanelor ale căror date personale le-a colectat prin intermediul taloanelor și al aplicațiilor de pe tabletele utilizate de hostesse, prin menționarea necorespunzătoare realității a unei categorii de destinatari – Inspectoratul Național pentru Evidența Persoanelor – cărora nu le sunt, în fapt, dezvăluite datele personale în scopul declarat, cel al probării vârstei majore a persoanelor care au furnizat date personale.

Pentru faptele reținute prin procesul-verbal de constatare/sanționare operatorul a fost sancționat cu trei amenzi contravenționale.

Procesul-verbal de constatare/sanționare a fost contestat în instanță de operatorul sancționat sub aspectul măsurilor recomandate și sub aspectul contravenției de "prelucrarea nelegală a datelor cu caracter personal", prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 4 alin. (1) lit. c), d) și e) din Legea nr. 677/2001, întrucât operatorul a colectat și stocat excesiv date personale, inclusiv codul numeric personal, al persoanelor participante la diverse acțiuni promoționale ale produselor sale de tutun, desfășurate până la data întocmirii procesului-verbal, prin raportare la scopul declarat al prelucrării.

Instanța a respins plângerea, reținând, cu privire la reclamantă că aceasta, în scopul declarat al verificării vârstei participanților la promoții, colectează CNP-ul, nefiind specificată o perioadă limitată de stocare a datelor personale în baza electronică de date, existând înregistrări încă din anul 2008.

În aprecierea excesivității prelucrării raportat la scop, se are în vedere faptul că scopul declarat era reprezentat de verificarea datei de naștere pentru promoțiile produselor din tutun, pentru a nu se încălca principiile Legii nr. 349/2002 pentru prevenirea și combaterea efectelor consumului produselor din tutun, modificată și completată.

Instanța a reținut faptul că, în contextul în care o promoție are o durată limitată în timp iar verificarea vârstei participanților se poate realiza prin comunicarea/stocarea doar a datei nașterii, apare evident că stocarea unor informații suplimentare (CNP-ul și celelalte date solicitate participanților, precum email, număr de telefon) pe o perioadă nedefinită de timp este excesivă și contrară scopului declarat, principiul proporționalității suferind un grav dezechilibru.

De asemenea, instanța a apreciat că susținerile reclamantei referitoare la faptul că prelucrarea CNP-ului este în speță esențială și trebuie să preceadă oricăror activități publicitare, permițând reclamantei să sisteze orice contact cu consumatorii minori care se declară adulți, iar lipsa oricărui mecanism de control al vârstei participanților la promoțiile produselor din tutun ar duce și la încălcarea principiilor Legii nr. 349/2002, sunt vădit neîntemeiate atât timp cât data nașterii este suficientă, iar procesarea datelor era necesară doar pe durata desfășurării promoției respective.

În ceea ce privește prezența recomandărilor făcute de Autoritatea națională de supraveghere prin procesul-verbal de constatare/sanționare, instanța de fond a reținut că acestea nu pot determina anularea sa.

Prin urmare, instanța a respins plângerea reclamantei ca fiind neîntemeiată.

Împotriva sentinței instanței de fond operatorul sancționat a înțeles să nu recurgă la nicio cale de atac, soluția fiind definitivă.

Decizia definitivă a instanței confirmă poziția Autorității naționale de supraveghere de apărare a principiilor prelucrării datelor prevăzute de Legea nr. 677/2001, respectiv de sancționare a operatorilor care prelucrează în mod excesiv datele personale ale persoanelor fizice și fără ca această prelucrare să fie legitimată în baza unor prevederi legale.

❖ Hotărâre pronunțată într-un litigiu privind dezvăluirea datelor cu caracter personal ale unor debitori, de către un executor judecătoresc

Autoritatea națională de supraveghere a fost sesizată de o persoană fizică asupra faptului că, într-un cotidian județean, un birou al unui executor judecătoresc a publicat un anunț privind vânzarea prin licitație publică a patru bunuri imobile, anunț care încalcă prevederile Legii nr. 677/2001. Astfel, la descrierea imobilelor supuse vânzării prin licitație publică, pe lângă alte date, erau menționate numele și prenumele, precum și CNP – urile mai multor debitori.

Instituția noastră a demarat o investigație la entitatea respectivă, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001, a măsurilor de securitate și a modului de colectare și prelucrare a datelor în cadrul activităților derulate de executorii judecătorești.

Potrivit art. 838 alin. (4) „Publicitatea vânzării” din Codul de procedură civilă, publicațiile în extras făcute într-un ziar de circulație națională trebuie să cuprindă numai mențiunile prevăzute la art. 838 alin. (1) lit. a), c) și f) - m) din Codul de procedură civilă, respectiv denumirea și sediul organului de executare, numele executorului judecătoresc, identificarea imobilului cu arătarea numărului cadastral sau topografic și a numărului de carte funciară, precum și descrierea lui sumară, semnătura și ștampila executorului judecătoresc.

În ceea ce privește datele personale având funcție de identificare, precum CNP și seria și numărul CI/BI, acestea se prelucrează numai cu respectarea dispozițiilor art. 8 din Legea nr. 677/2001, coroborate cu cele ale 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, emisă de Autoritatea națională de supraveghere.

Autoritatea națională de supraveghere a emis un proces-verbal de constatare/sancționare prin care s-a constatat săvârșirea de către operatorul controlat a faptei

contravenționale de prelucrare nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 5 și art. 8 din Legea nr. 677/2001, precum și a art. 2 din Decizia nr. 132/2011. Astfel, biroul executorului judecătoresc a dezvăluit într-un cotidian județean, în anunțul privind vânzarea prin licitație publică a patru bunuri imobile, datele cu caracter personal, respectiv CNP - ul a cinci debitori, fără consimțământul expres al persoanelor vizate, în condițiile în care această prelucrare nu este prevăzută în mod expres de o dispoziție legală și nu a obținut avizul Autorității naționale de supraveghere cu privire la această dezvăluire; de asemenea, a dezvăluit numele și prenumele debitorilor în cotidianul susmenționat fără consimțământul acestora, dat în mod expres și neechivoc în acest scop.

Procesul-verbal de constatare/sanționare a fost contestat în instanță de operatorul sancționat, acesta solicitând reducerea la minimum prevăzut de lege al amenzii aplicate.

Instanța a admis plângerea, reținând, cu privire la reclamant, că acesta a recunoscut săvârșirea faptei contravenționale consemnate în procesul-verbal de constatare/sanționare pentru care a fost sancționat de Autoritatea națională de supraveghere și își asumă interpretarea subiectivă a art. 838 din Codul de procedură civilă care reglementează mențiunile cuprinse în publicațiile de vânzare.

Cu toate acestea, instanța de fond a apreciat că reclamantul se află la prima faptă contravențională în materia protecției datelor și, ținând cont de gradul de pericol social al faptei contravenționale săvârșită de acesta, a redus amenda aplicată de Autoritatea națională de supraveghere la minimum prevăzut de lege.

Împotriva sentinței instanței de fond Autoritatea națională de supraveghere a declarat recurs, iar instanța superioară a admis recursul formulat, a casat în tot sentința recurată, în sensul că, rejudecând a respins acțiunea în tot a reclamantului, soluția fiind definitivă.

Decizia definitivă a instanței a confirmat abordarea Autorității naționale de supraveghere de respectare a condițiilor de legitimitate a prelucrării datelor cu caracter personal, așa cum sunt acestea prevăzute de Legea nr. 677/2001.

Atragem atenția asupra faptului că prelucrarea unor date cu caracter personal în cadrul activității derulate de birourile executorilor judecătorești intră sub incidența legislației privind protecția datelor personale, iar aceștia sunt ținuți, în calitate de operatori de date, de respectarea tuturor obligațiilor stabilite de lege în sarcina acestora.

❖ **Hotărâre definitivă pronunțată într-un dosar în care un petent a reclamat o practică incorectă de business de largă adresabilitate**

Investigația efectuată de Autoritatea națională de supraveghere la operatorul în cauză a avut ca obiect soluționarea aspectelor sesizate de un petent care a semnalat o posibilă „practică incorectă de business de largă adresabilitate”.

Astfel, petiționarul a precizat că, în urma cumpărării on-line a unor bilete la cinema de pe un site de profil, 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 specifică deținută de operator, 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”. În aceeași adresă 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.

În procesul-verbal de constatare/sanționare s-a reținut că aplicația specifică, potrivit mențiunilor accesibile la adresa reclamantei, reprezintă un serviciu pus la dispoziție de operator. Acest serviciu oferă persoanelor posibilitatea de a cumpăra on-line fără a mai fi necesară introducerea tuturor datelor cardului de fiecare dată când sunt efectuate cumpărături on-line.

Pentru cumpărarea unui bilet on-line de pe site-ul în discuție (aparținând unui alt operator), conform documentelor puse la dispoziție de operator în cadrul investigației, este necesară parcurgerea mai multor etape diferite.

Pe această din urmă pagină, este selectată implicit “Activează opțiunea plăți rapide” și, prin urmare, persoanelor vizate li se creează fără consimțământul lor și fără o informare prealabilă un cont de utilizator pentru portofelul virtual. Acest cont are atașat un card din care se efectuează plata biletului.

Referitor la relațiile existente între deținătorul site-ului de pe care se cumpăra biletul și operatorul sancționat, cu ocazia investigației s-a reținut că aceste două societăți au încheiat un Contract de acceptare la plată a instrumentelor electronice prin intermediul sistemului de portofel virtual cu un Act adițional.

Prin urmare, în procesul-verbal de constatare/sanționare s-a reținut faptul că operatorul investigat nu a respectat cerințele Legii nr. 677/2001, modificată și completată, prin faptul că:

- de la data implementării sistemului Wallet, respectiv iulie 2012 și până la data efectuării investigației, nu a completat notificarea prelucrării datelor cu caracter personal, motiv pentru

care operatorul a fost sancționat, în temeiul art. 31 din Legea nr. 677/2001 coroborat cu art. 5 și 7 din Ordonanța de Guvern nr. 2/2001, cu modificările și completările ulterioare, pentru săvârșirea contravenției de „omisiunea de a notifica și notificarea cu rea credință”, pentru care s-a aplicat avertisment.

- de la data implementării serviciului de plată on-line pentru site-ul de achiziționare de bilete la evenimente deținut de alt operator și activarea implicită a opțiunii „plăți rapide”, respectiv sfârșitul anului 2012 și până la data investigației, a prelucrat datele cu caracter personal ale persoanelor vizate prin crearea unui cont pentru folosirea serviciului Wallet, fără informarea persoanelor vizate, cu încălcarea art. 12 din Legea nr. 677/2001, motiv pentru care operatorul a fost sancționat, în temeiul art. 32 din Legea nr. 677/2001 coroborat cu art. 5 și 8 din Ordonanța de Guvern nr. 2/2001, cu modificările și completările ulterioare, pentru săvârșirea contravenției de „prelucrare nelegală a datelor cu caracter personal”, pentru care s-a aplicat sancțiunea amenzii.

- de la data implementării serviciului de plată on-line pentru site-ul de achiziționare de bilete la evenimente deținut de alt operator și activarea implicită a opțiunii „plăți rapide”, respectiv sfârșitul anului 2012 și până la data investigației, a prelucrat datele cu caracter personal ale persoanelor vizate prin crearea unui cont pentru folosirea serviciului Wallet, fără ca acestea să-și fi exprimat consimțământul în mod expres și neechivoc pentru această prelucrare, cu încălcarea art. 5 din Legea nr. 677/2001, motiv pentru care operatorul a fost sancționat, în temeiul art. 32 din Legea nr. 677/2001 coroborat cu art. 5 și 8 din Ordonanța de Guvern nr. 2/2001, cu modificările și completările ulterioare, pentru săvârșirea contravenției de „prelucrare nelegală a datelor cu caracter personal”, pentru care s-a aplicat sancțiunea amenzii.

Prin sentința civilă pronunțată în cauză, instanța a respins ca neîntemeiată plângerea formulată de reclamantă. Pentru a hotărî astfel, instanța de fond a reținut că procesul - verbal a fost întocmit în mod legal și temeinic, reclamantei fiindu-i imputabile cele trei fapte descrise în procesul verbal.

Astfel, cu privire la prima faptă săvârșită de reclamantă, instanța de fond a subliniat că „reclamanta avea obligația să notifice, înainte de efectuarea oricărei prelucrări de date cu caracter personal prin serviciul Wallet, obligație pe care nu a îndeplinit-o”.

Cu privire la cea de-a doua faptă săvârșită de reclamantă, instanța de fond a arătat că această faptă „este, de asemenea, imputabilă reclamantei”.

Pentru a hotărî astfel, instanța a reținut că pentru efectuarea unei plăți cu cardul pentru un bilet cumpărat de pe site-ul în discuție, utilizatorul era direcționat automat pe pagina de internet a reclamantei, unde i se prelucrau datele cu caracter personal, dar nu s-a probat de reclamantă că utilizatorul a fost informat în prealabil că datele sale vor fi prelucrate de altă societate.

În ceea ce privește cea de-a treia faptă săvârșită de reclamantă, instanța de fond a stabilit că „și cea de-a treia faptă prevăzută de art. 32 din Legea nr. 677/2001 a fost indicată în mod corect în procesul-verbal, reclamanta prelucrând în mod nelegal date cu caracter personal prin încălcarea dispozițiilor art. 5 din Legea nr. 677/2001, pentru lipsa consimțământului expres și neechivoc al utilizatorului privind prelucrarea datelor personale”.

Prin decizia pronunțată în cauză, instanța de judecată a respins ca nefondat apelul formulat de către operator, confirmând definitiv abordarea Autorității naționale de supraveghere.

❖ Hotărâre pronunțată într-un litigiu privind transmiterea de mesaje comerciale nesolicitate, fără consimțământul prealabil al destinatarului, cu încălcarea prevederilor Legii nr. 506/2004

O persoană fizică a sesizat Autorității naționale de supraveghere o posibilă încălcare a prevederilor Legii nr. 506/2004, în contextul primirii, prin mesageria electronică, fără consimțământul său prealabil, a unui mesaj care cuprindea oferte de produse ale unui operator.

Autoritatea națională de supraveghere a constatat săvârșirea următoarelor fapte:

- nerespectarea prevederilor art. 12 referitoare la comunicările nesolicitate, prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004, întrucât operatorul a transmis către adresa de e-mail a petentului o comunicare comercială fără consimțământul acestuia.

- nerespectarea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, faptă prevăzută de art. 33 din Legea nr. 677/2001, sub forma încălcării art. 20 alin. (2) și (5) din aceeași lege întrucât, la data controlului, operatorul nu făcut dovada existenței unei politici de securitate, conform Ordinului nr. 52/2002, și nici a implementării cerințelor minime prevăzute de acesta.

Pentru faptele constatate, Autoritatea națională de supraveghere a aplicat o amendă și un avertisment.

Operatorul sancționat a contestat în instanță procesul-verbal de constatare/sancționare.

Instanța a reținut că reclamanta nu a putut dovedi în niciun fel susținerile sale și a respins plângerea formulată, menținând sancțiunile aplicate prin procesul-verbal de constatare/sanționare emis de Autoritatea națională de supraveghere.

❖ Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal și transmiterea de comunicări comerciale nesolicitate de către o entitate specializată în activități de asistență medicală generală

Reprezentanții Autorității naționale de supraveghere au realizat un control din oficiu la un operator, pentru verificarea condițiilor de aplicare a Legii nr. 677/2001, precum și a dispozițiilor Legii nr. 506/2004.

În urma discuțiilor purtate cu reprezentanții societății și a verificărilor efectuate în timpul controlului a rezultat că operatorul, începând cu vara anului 2013, oferea pacienților analize medicale și carduri de fidelitate.

Totodată s-a reținut că, în activitatea desfășurată, operatorul prelucra următoarele date cu caracter personal: numele, prenumele, CNP-ul, telefonul, sexul și data nașterii pacienților, în vederea efectuării programării pacienților pentru consultații.

Din verificările efectuate a rezultat că operatorul, începând cu data de 5 martie 2013, trimitea newslettere persoanelor din baza de date, utilizând o platformă on-line, în vederea oferirii acestora de pachete medicale promoționale pe sezoane, cu ocazia sărbătorilor.

De asemenea, s-a constatat că operatorul nu realiza informarea pacienților, așa cum prevede art. 12 din Legea nr. 677/2001. Astfel, cu ocazia controlului, s-a prezentat echipei de control doar o listă de dezabonați la newsletter.

În același context, s-a reținut că operatorul instalase un sistem de supraveghere video, funcțional începând cu anul 2013, fără ca persoanele vizate să fie informate despre existența acestuia, cu încălcarea prevederilor Legii nr. 677/2001 și ale Deciziei ANSPDCP nr. 52/2012.

Totodată, operatorul investigat nu a făcut dovada notificării prelucrării datelor cu caracter personal în scopurile "reclamă, marketing și publicitate" și "monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private", încălcându-se astfel dispozițiile art. 22 din Legea nr. 677/2001.

Pentru faptele constatate prin procesul-verbal de constatare/sanționare operatorul a fost sancționat cu trei amenzi contravenționale.

Instanța a respins plângerea, reținând în privința notificării că reclamanta nu a dovedit existența acesteia.

Pe cale de consecință, în mod corect s-a reținut în sarcina reclamantei și săvârșirea contravențiilor prevăzute de 13 alin. (1) lit. q) din Legea nr. 506/2004, constând în nerespectarea art. 12 referitor la comunicările nesolicitate.

Decizia instanței de respingere a plângerii operatorului a rămas definitivă.

Secțiunea a 5-a Informare publică

În cursul anului 2015, 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 pe postul public de televiziune a unui clip de informare privind datele personale.

De asemenea, instituția noastră a participat activ la cele mai importante evenimente la care a fost invitată, organizate de diverse instituții publice sau de entități private. La aceste reuniuni, reprezentanții Autorității naționale de supraveghere au clarificat anumite aspecte referitoare la obligația de notificare a prelucrărilor de date efectuate, respectarea drepturilor persoanelor vizate și asigurarea confidențialității prelucrărilor datelor cu caracter personal

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

✓ Ziua Europeană a Protecției Datelor

În data de 28 ianuarie 2015 s-a marcat aniversarea a 34 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 persoanelor 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, un Simpozion care s-a bucurat de participarea prestigioasă a unor înalți oficiali și reprezentanți ai justiției, mediului academic și ai organizațiilor nonguvernamentale, care au discutat aspectele esențiale privind reforma europeană a cadrului normativ în domeniul protecției datelor personale.

✓ **Dezbatere publică aniversară – 10 ani de la înființare**

O altă manifestare de înaltă ținută a fost organizată de instituția noastră la Palatul Parlamentului, în data de 10 iunie 2015, pentru sărbătorirea împlinirii a 10 ani de la adoptarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității naționale de supraveghere.

Astfel, cu această ocazie a avut loc dezbaterea publică cu tema „Protecția datelor personale în contextul dezvoltării noilor tehnologii”, ce a reunit reprezentanți ai mediului academic, ai instituțiilor publice centrale și ai mediului de afaceri.

În anul 2015, Autoritatea națională de supraveghere a continuat campania de informare, la nivel național, în sectorul public și privat.

Cu sprijinul Instituției Prefectului din județele Alba și Sibiu 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 au fost invitați reprezentanți ai administrației publice locale și ai serviciilor publice deconcentrate de la nivel județean.

În același timp, au fost organizate reuniuni de informare la nivelul camerelor județene ale notarilor publici pentru creșterea gradului de conștientizare a operatorilor cu privire la obligațiile care le incumbă, cu sprijinul Uniunii Naționale a Notarilor Publici (Camera Notarilor Publici București, Pitești și Constanța).

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 și obligațiile ce revin operatorilor de date din sectorul public și privat.

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.

În scopul popularizării activității instituției și a reglementărilor specifice în materie, au fost publicate 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.

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 IV

ACTIVITATEA DE CONTROL

Secțiunea 1: Prezentare generală

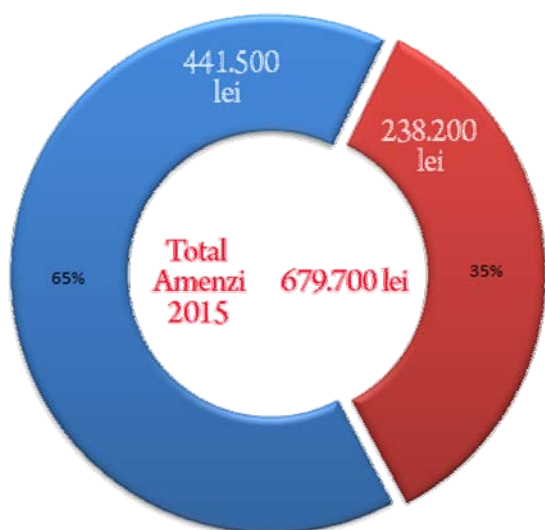


Fig. 1

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.

Cuantumul total al amenzilor aplicate în cadrul investigațiilor efectuate pentru soluționarea plângerilor și sesizărilor este de 238.200 lei, iar cuantumul total al amenzilor aplicate în cadrul investigațiilor din oficiu este de 441.500 lei. (Fig. 1)

Cuantumul total al amenzilor aplicate în 2015 în investigațiile efectuate este de 679.700 lei, reprezentând o creștere cu 141% a cuantumului amenzilor comparativ cu anul 2014. (Fig. 2)

În cursul anului 2015 numărul plângerilor și sesizărilor a crescut în mod considerabil prin raportare la anii precedenți. Astfel, au fost primite și soluționate un total de 1335 petiții din care 1074 plângeri și 175 sesizări. (Fig. 3)

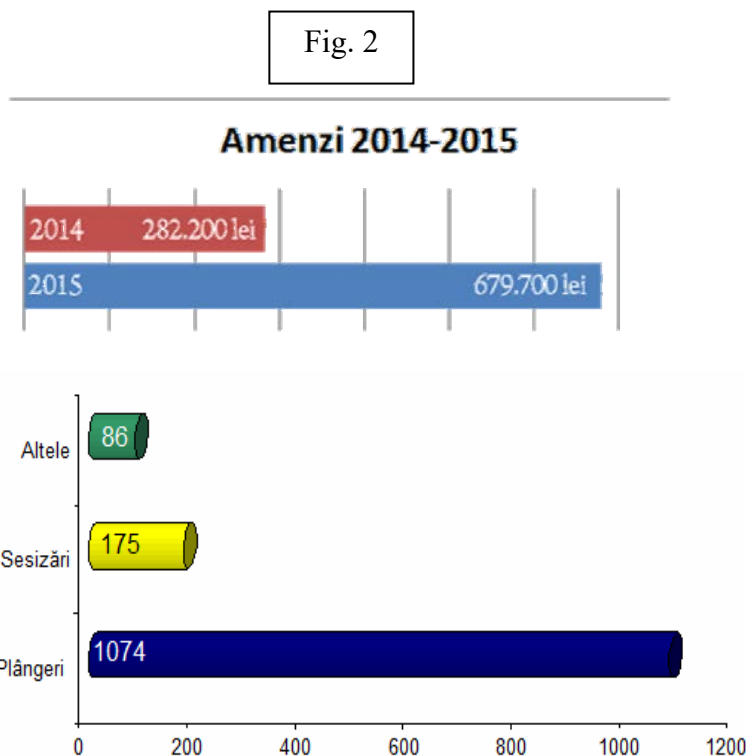


Fig. 3

Secțiunea a 2-a: Investigații din oficiu

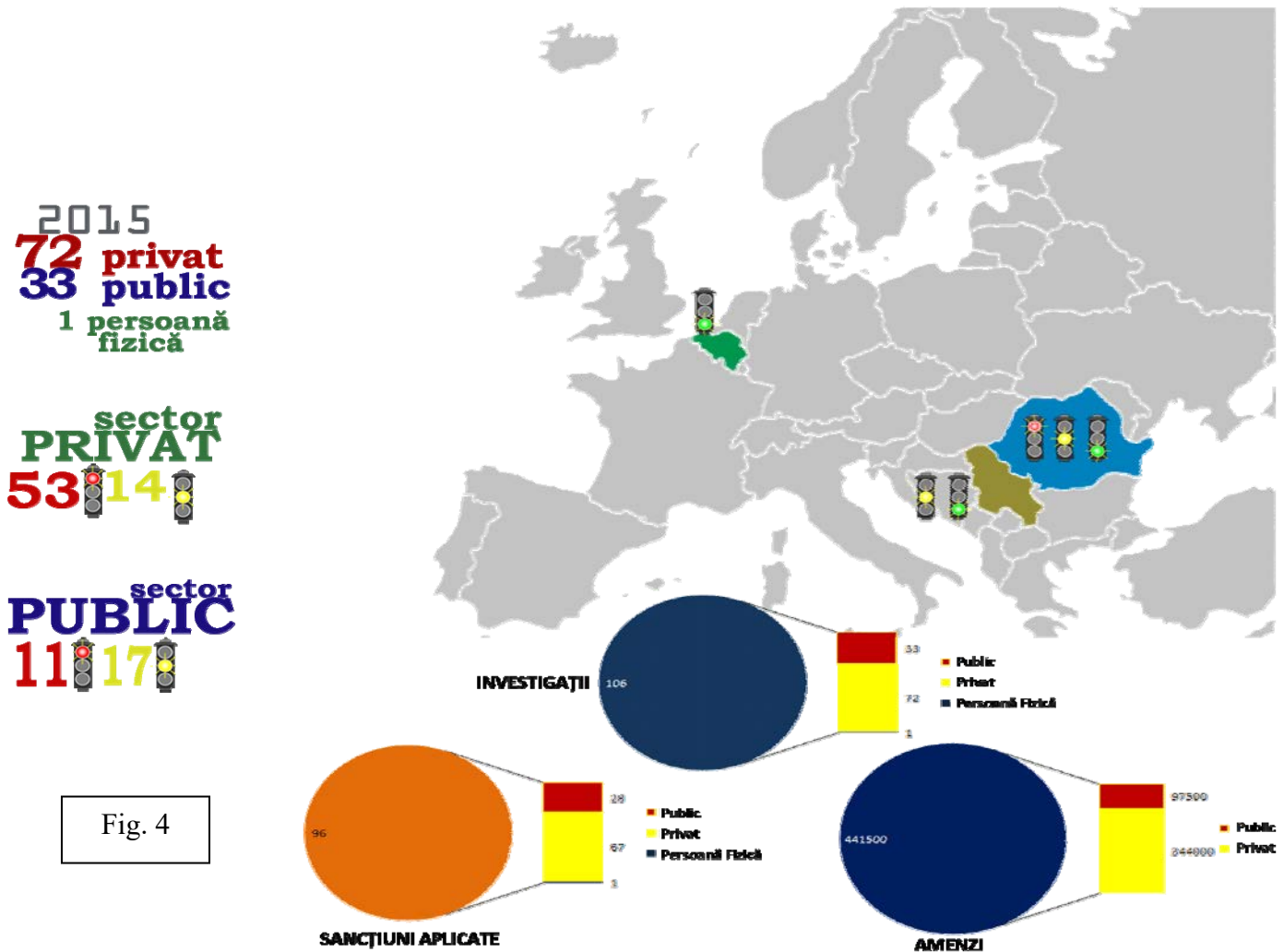


Fig. 4

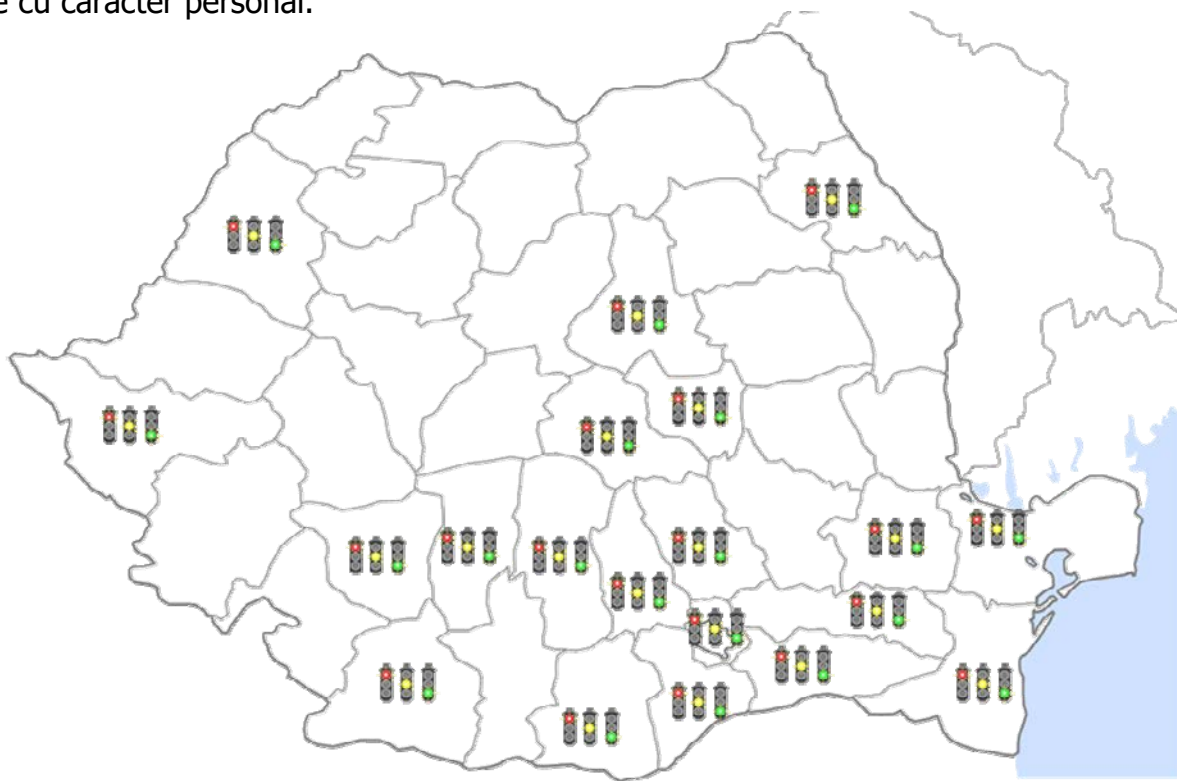
În anul 2015 a fost efectuat un număr total de 106 acțiuni de control din oficiu la sediile operatorilor verificați, ca urmare a extinderii verificării condițiilor de prelucrare a datelor cu caracter personal în mai multe domenii de activitate, a abordării unui număr mai mare de obiective principale și a monitorizării adecvate a semnalărilor din mass-media, din care 72 controale în sectorul privat, 33 în sectorul public și 1 operator persoană fizică. (Fig. 4)

Astfel, pentru investigațiile din oficiu efectuate au fost aplicate sancțiuni contravenționale constând în amenzi (64), în quantum total de 441.500 lei, și în avertismente (32).

Totodată, Autoritatea națională de supraveghere a decis continuarea investigațiilor din oficiu la misiunile diplomatice și oficiile consulare ale României, pentru verificarea respectării prevederilor Legii nr. 677/2001, în cadrul prelucrărilor de date cu caracter personal, inclusiv în ceea ce privește respectarea drepturilor persoanelor vizate și a măsurilor de securitate implementate.

Autoritatea națională de supraveghere a formulat 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.

Fig. 5



Sector PRIVAT

Integratori/procesatori de plăți online
Servicii Cloud
Unități de cazare și turism

Sector PUBLIC

Institua Prefectului
Inspectorate județene de poliție

CNP date **BIOMETRICE** nume voce
ONLINE supraveghere **VIDEO** DATE DE
TRAFIC PRENUME **IMAGINEA**e-mail
INCIDENTE **COOKIES**
DE SECURITATE **STOCARE**



amenzi

avertismente

recomandări

Activitatea de monitorizare și control din oficiu desfășurată la nivel teritorial 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. (Fig. 5)

În urma controalelor au fost constatate următoarele deficiențe:

- 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 de date cu caracter personal prin utilizarea mijloacelor de supraveghere video,

- omisiunea de a notifica prelucrările de date cu caracter personal prin prelucrarea datelor biometrice (amprente) în scopul realizării pontajului salariaților,
- prelucrarea codului numeric personal și a altor date de identificare de aplicabilitate generală, fără respectarea prevederilor Deciziei nr. 132/2011,
- utilizarea de module cookies la nivelul site-urilor operatorilor fără respectarea, în mod cumulativ, a prevederilor art. 4 alin. (5) lit a) și b) din Legea nr. 506/2004.

I. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către societățile care oferă servicii cloud

Autoritatea națională de supraveghere a dispus efectuarea de investigații din oficiu într-un sector aflat în continuă dezvoltare în România, în vederea verificării respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de către societățile care oferă servicii cloud în zona soluțiilor IT de business din România.

Orientarea operatorilor de date, prin externalizarea serviciilor IT, către servicii cloud (servicii de e-mail, de stocare de fișiere, baze de date sau software) a reprezentat un motiv în plus pentru efectuarea de investigații din oficiu, tematice.

Totodată, trebuie menționat că și un număr ridicat de persoane vizate folosesc serviciile cloud pentru sincronizarea fișierelor (video, documente, foto, etc.) cu dispozitivele terminale proprii (telefoane mobile, tablete, calculatoare personale/de serviciu).

Serviciile de tip "cloud computing" pot fi definite ca soluții de utilizare a resurselor informatice externe (putere de calcul, spațiu de stocare, aplicații etc.) prin intermediul Internetului. Cele trei servicii de bază oferite de către societățile care furnizează servicii cloud sunt: software ca serviciu (Software as a Service), platformă ca serviciu (Platform as a Service) și infrastructură ca serviciu (Infrastructure as a Service). Pentru furnizarea acestor servicii se folosesc propriile centre de date sau prin închirierea resurselor de la alți deținători de centre de date.

O concluzie generală, în ceea ce privește aceste societăți verificate, este că centrele de date utilizate de acești furnizori de servicii cloud sunt situate pe teritoriul României. Societățile care oferă servicii cloud, supuse controalelor din oficiu, prelucrează date cu caracter personal în scopul furnizării acestor servicii în calitate de împuterniciți, iar nu în calitate de operatori de date cu caracter personal.

Având în vedere expansiunea serviciilor de cloud și faptul că utilizarea acestora poate

genera o serie de riscuri asociate protecției datelor, Autoritatea națională de supraveghere recomandă utilizatorilor de servicii cloud să se informeze în prealabil cu privire la modalitatea, locul și entitatea de prelucrare, transparența, măsurile de securitate, certificate prin standarde actualizate, disponibilitate, integritate, confidențialitate, portabilitate etc.

Totodată, Autoritatea națională de supraveghere recomandă furnizorilor de servicii cloud din România alinierea la standardele internaționale de securitate, în funcție de riscurile prezentate de prelucrare și de natura datelor care trebuie protejate, precum și respectarea tuturor prevederilor legale, în ceea ce privește prelucrarea datelor cu caracter personal care fac obiectul acestor servicii cloud.

II. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal la nivelul operatorilor care dețin website-uri

Concepute inițial pentru a veni în ajutorul navigării pe Internet, în sensul asigurării unei interacțiuni mai rapide și mai ușoare între utilizatori și site-urile web, cookie-urile sunt definite ca fișiere mici alfanumerice, unice, care se stochează în echipamentul terminal al unui abonat/utilizator. Acestea au devenit un mijloc de colectare a preferințelor, comportamentului sau obișnuințelor utilizatorilor, prin colectarea și furnizarea unor informații care de multe ori conțin date cu caracter personal (de ex. locația geografică, sexul, vârsta, adresa IP, interese ale utilizatorului).

Astfel, prin utilizarea acestor module cookies, utilizatorului i se poate oferi conținut similar și publicitate on-line orientată pe un istoric recent al utilizatorului/abonatului pe echipamentul terminal al acestuia, iar prin stocarea și accesarea informațiilor stocate în echipamentele utilizatorilor se oferă posibilitatea creării de profile predictive și explicite pe baza identificatorilor unici ai modulelor cookies.

Având în vedere aceste aspecte, Autoritatea națională de supraveghere a efectuat în anul 2015 mai multe investigații la operatori care dețin website-uri, atât din domeniul public cât și din domeniul privat, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001, precum și a prevederilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Potrivit prevederilor art. 4 alin. 5 din Legea nr. 506/2004, „stocarea de informații sau obținerea accesului la informația stocată în echipamentul terminal al unui abonat ori utilizator

este permisă numai cu îndeplinirea în mod cumulativ a următoarelor condiții:

a) abonatul sau utilizatorul în cauză și-a exprimat acordul;

b) abonatului sau utilizatorului în cauză i s-au furnizat, anterior exprimării acordului, în conformitate cu prevederile art. 12 din Legea nr. 677/2001, cu modificările și completările ulterioare, informații clare și complete care să fie expuse într-un limbaj ușor de înțeles și să fie ușor accesibile abonatului sau utilizatorului și să includă mențiuni cu privire la scopul procesării informațiilor stocate de abonat sau utilizator ori informațiilor la care acesta are acces.”

Ca urmare a investigațiilor efectuate, s-a constatat că cea mai mare parte a operatorilor investigați prelucrau date cu caracter personal prin intermediul cookie-urilor cu nerespectarea prevederilor legale, întrucât nu îndeplineau în mod cumulativ cerințele stabilite de art. 4 alin. (5) din Legea nr. 506/2004.

Această verificare a website-urilor a avut caracter permanent în toate investigațiile din oficiu, controlul fiind extins indiferent de versiunea website-ului mobil/desktop, după caz. Astfel, aceste verificări s-au realizat în aproximativ toate investigațiile efectuate la nivelul prefecturilor, inspectoratelor județene de poliție, unităților de cazare și turism, furnizorilor de servicii Cloud etc.

Cea mai mare sancțiune aplicată unui operator a fost în quantum total de 45.000 lei (aprox. 10.000 Euro), pentru săvârșirea contravenției prevăzute de art. 13 alin. (1) lit. i), art. 13 alin. (2) și art. 13 alin. (5) din Legea nr. 506/2004, modificată și completată, coroborat cu art. 5 și art. 8 din O.G. nr. 2/2001, iar quantumul total al amenzilor aplicate pentru această contravenție în 2015 a fost de aproximativ 300.000 lei.

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

I. Prezentare generală

Una dintre principalele atribuții legale prin care Autoritatea națională de supraveghere își îndeplinește obiectivul pentru care a fost înființată prin Legea nr. 102/2005, acela de apărare a drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, în legătură cu prelucrarea datelor personale și cu libera circulație a acestor date, constă în soluționarea plângerilor și a sesizărilor ce vizează încălcarea acestui drept.

Persoanele fizice se pot adresa cu 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; de asemenea, orice persoană poate sesiza Autoritatea națională de supraveghere asupra aspectelor legate de prelucrarea datelor personale, care ar putea să contravină dispozițiilor legale. În scopul informării celor interesați, pe pagina de Internet a instituției noastre sunt disponibile atât modele de plângere, cât și o procedură detaliată privind condițiile în care sunt înregistrate, analizate și soluționate plângerile și sesizările ce privesc posibile încălcări ale Legii nr. 677/2001 sau ale Legii nr. 506/2004.

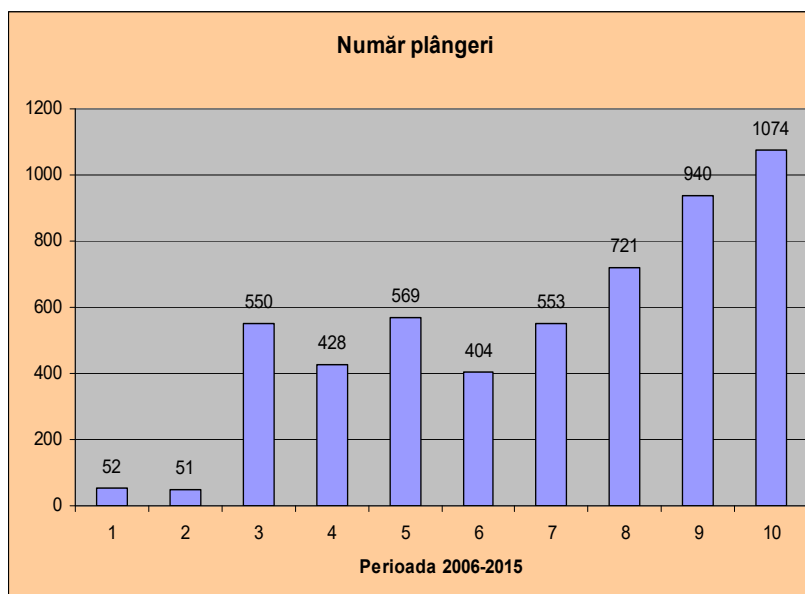
În cazul plângerilor, sunt stipulate o serie de condiții, în lipsa îndeplinirii cărora acestea putând fi respinse ca inadmisibile: persoanele vizate nu trebuie să fi introdus anterior o acțiune în justiție cu același obiect și cu aceleași părți; persoanele vizate trebuie să fi înaintat anterior (15 zile) o cerere cu același conținut către operatorul de date de la care nu a primit un răspuns sau răspunsul a fost unul nesatisfăcător. Din acest punct de vedere, ca și în anii precedenți, principalul motiv de respingere a plângerilor în anul 2015 a fost legat de neîndeplinirea procedurii legale prealabile de către petenți. Alte motive pentru care plângerile și sesizările nu au primit o soluționare favorabilă au constat în: neprezentarea dovezilor în susținerea aspectelor reclamate sau a calității de reprezentant al persoanei vizate; sesizarea unor fapte în legătură cu care Autoritatea națională de supraveghere nu deține competența materială sau teritorială să intervină; imposibilitatea identificării exacte a entității reclamate (spre exemplu, expeditorul unei comunicări comerciale electronice nesolicitate sau a deținătorului unui website); preexistența unui litigiu pe rolul instanțelor judecătorești cu identitate de părți și obiect.

În anul 2015, numărul petițiilor soluționate de compartimentul de specialitate din cadrul Autorității naționale de supraveghere a crescut în mod considerabil prin raportare la anii precedenți. Astfel, au fost primite și soluționate **un total de 1335 petiții, din care 1074 plângeri și 175 sesizări**. Prin aceste petiții au fost sesizate aspecte legate de posibile încălcări ale prevederilor ce guvernează dreptul la viață privată, în cadrul prelucrărilor de date personale sau în sectorul comunicațiilor electronice, în speță, din Legea nr. 677/2001 și Legea nr. 506/2004.

Creșterea numărului petițiilor primite în cursul anului 2015 și diversificarea obiectului acestora demonstrează faptul că atribuțiile legale ale Autorității naționale de supraveghere sunt mult mai bine cunoscute persoanelor fizice prin comparație cu perioada de început a

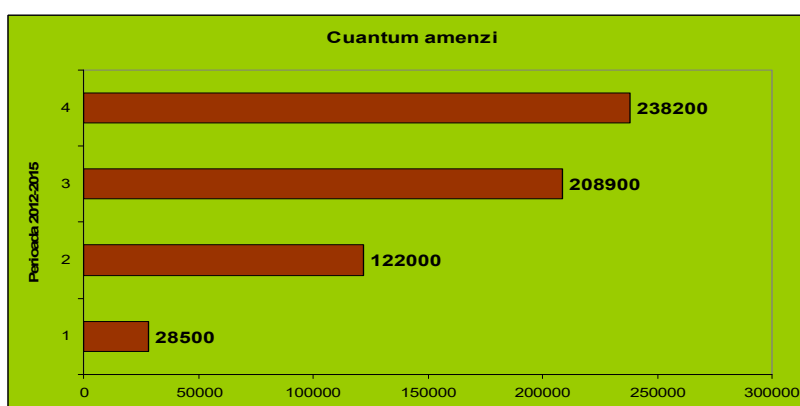
funcționării sale, iar eficiența acțiunilor ce au ca finalitate restaurarea drepturilor încălcate reprezintă un criteriu important pentru manifestarea încrederii de către petiționarii care ni se adresează.

Figura 1: Numărul plângerilor în perioada 2006-2015



Pentru soluționarea plângerilor și sesizărilor primite, au fost efectuate **224 de investigații pe teren și 71 de investigații în scris; în 43 de cazuri**, investigațiile au fost finalizate prin încheierea la sediul Autorității naționale de supraveghere a unor procese-verbale de constatare/sanționare. În cazurile în care instituția noastră a considerat întemeiate aspectele verificate în cadrul investigațiilor efectuate pentru soluționarea plângerilor și sesizărilor, au fost aplicate sancțiuni contravenționale, **cuantumul total al amenzilor aplicate în 2015 în cadrul acestor investigații fiind de 238.200 lei.**

Figura 2: Cuantumul amenzilor aplicate în activitatea de soluționare a plângerilor și sesizărilor în perioada 2012-2015



Totodată, în urma demersurilor de soluționare a plângerilor și sesizărilor adresate autorității, au fost emise **8 decizii** ale președintelui Autorității naționale de supraveghere, prin care s-a dispus ștergerea datelor personale sau a anumitor categorii de date, majoritatea privind situații de raportare a datelor negative către biroul de credit.

Plângerile și sesizările primite au vizat o gamă largă de domenii, însă, la fel ca și în anii precedenți, cele mai multe dintre plângeri au vizat prelucrarea datelor personale în următoarele domenii: sectorul financiar-bancar, monitorizarea spațiilor publice sau private prin mijloace de supraveghere video, sectorul comunicațiilor electronice, dezvăluirea datelor către diverse entități, diseminarea datelor pe Internet. Ca element de noutate, se remarcă problematica prelucrării datelor biometrice în contextul relațiilor de muncă, care a făcut obiectul unora dintre petițiile transmise Autorității naționale de supraveghere, într-un procent sporit față de alți ani. De asemenea, indiferent de domeniul de activitate al operatorilor, multe dintre plângerile primite au avut ca obiect nerespectarea condițiilor legale ce privesc exercitarea drepturilor persoanelor vizate (drepturile de informare, acces, intervenție, opoziție).

Astfel, în sectorul financiar-bancar, în care operatorii reclamați sunt, în principal, bănci, instituții financiare nebancale, societăți de recuperare creanțe și cele care dețin sisteme de evidență de tipul birourilor de credit, s-a constatat și în anul 2015 o continuă creștere a numărului petițiilor. Principalul motiv de nemulțumire a persoanelor vizate, care a determinat sesizarea Autorității naționale de supraveghere, a fost legat de raportarea datelor personale 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 vigoare din luna februarie 2008.

În urma investigațiilor efectuate, în multe cazuri s-a constatat faptul că operatorii au încălcat prevederile legii și ale deciziei susmenționate, în special în ceea ce privește lipsa unei informări prealabile cu privire la transmiterea datelor negative la biroul de credit, conținutul incomplet al notificărilor prealabile, nerespectarea termenului 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 nebancale) 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).

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 în viitor. De aceea, Autoritatea națională de supraveghere a acordat atenție fiecărei plângeri admisibile având ca obiect astfel de pretinse încălcări, adoptând în final măsurile legale care s-au impus pentru restabilirea drepturilor nesocotite în raport cu operatorii reclamați, în funcție de circumstanțele individuale ale fiecărui caz.

O pondere însemnată a plângerilor și sesizărilor adresate la Autoritatea națională de supraveghere în anul 2015 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 sau diverse categorii de angajatori care au instalat camere de supraveghere la locul de muncă. Au mai fost sesizate și investigate situații de prelucrare a datelor personale prin intermediul sistemelor de supraveghere video instalate la nivelul unităților de învățământ sau în spații folosite de persoane fizice. În urma investigațiilor realizate, s-a constatat că operatorii nu cunosc, nu respectă sau ignoră dispozițiile legale aplicabile prelucrării 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.

În anul 2015 a fost înregistrat, de asemenea, un număr mare de petiții având ca obiect dezvăluirea datelor personale pe Internet, fără consimțământul persoanelor vizate sau alt temei legal, precum și transmiterea de mesaje comerciale nesolicitate prin mijloace de comunicație electronică. Operatorii reclamați au fost, în principal, societăți care administrează diferite site-uri de socializare, de popularizare a informațiilor din dosare aflate pe rolul instanțelor judecătorești, care efectuează activități de comerț on-line sau marketing direct, furnizori de servicii de comunicații electronice. Autoritatea națională de supraveghere a continuat să primească în anul 2015 plângeri care au vizat nerespectarea de către Google a "dreptului de a fi uitat", urmare a refuzului acestei companii de a da curs cererilor prin care se solicita dezindexarea de pe Internet a rezultatelor căutărilor asociate numelui unei persoane.

În majoritatea cazurilor investigate, operatorii s-au conformat măsurilor dispuse de Autoritatea națională de supraveghere, prin asigurarea drepturilor persoanelor vizate și înlăturarea efectelor rezultate din încălcarea legii (ștergerea datelor publicate, eliminarea unor rezultate de pe Internet, încetarea prelucrării datelor în scop de marketing direct etc.).

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 2015 numărul plângerilor ce vizează transmiterea datelor personale către biroul de credit a ocupat o pondere considerabilă din numărul total al petițiilor primite de Autoritatea națională de supraveghere. Multe dintre persoanele care au formulat o astfel de plângere au luat cunoștință de existența datelor negative (întârzieri la plata ratelor de credit) în sistemul de evidență al biroului de credit cu ocazia solicitării altor produse bancare. Lipsa informării prealabile, condiție obligatorie impusă de Decizia nr. 105/2007 pentru a putea fi raportate date negative către aceste sisteme, a constituit așadar principalul motiv pentru care s-a solicitat intervenția instituției noastre.

Ca urmare a constatărilor din cadrul investigațiilor desfășurate, au rezultat o serie de aspecte privind nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul biroului de credit, perpetuate în fiecare an, 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 sau recomandărilor adresate cu ocazia acestor investigații, 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, petentul a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 prin faptul că o bancă comercială, al cărei client a fost, a transmis date negative la biroul de credit, fără ca aceasta să-l fi înștiințat în prealabil cu 15 zile, conform dispozițiilor Deciziei nr. 105/2007.

În cadrul investigației efectuate, reprezentanții băncii au precizat faptul că au transmis date negative la biroul de credit, întrucât petentul acumulasese restanțe pe parcursul derulării creditului. Cu toate acestea, banca nu a putut să prezinte dovezi din care să rezulte că a realizat informarea prealabilă a clientului său înainte de fiecare transmitere a datelor negative, așa cum prevede art. 8 alin. (2) din Decizia nr. 105/2007, într-o perioadă de timp cuprinsă între anii 2011-2015.

La solicitarea petentului de ștergere a datelor negative înregistrate de bancă la biroul de credit, instituția bancară a transmis un răspuns prin care îi comunica refuzul de a da curs cererii sale, răspuns comunicat cu depășirea termenului de 15 zile prevăzut de art. 14 din Legea nr. 677/2001 ce reglementează dreptul de intervenție.

În baza acestor constatări, banca în cauză a fost sancționată contravențional pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, pentru nerespectarea prevederilor acestei legi și ale Deciziei nr. 105/2007. Totodată, s-a pus în vedere băncii obligația de ștergere a datelor negative transmise la biroul de credit, aferente contractului de credit semnat cu petentul, fără respectarea prevederilor legale.

FIȘĂ DE CAZ

Prin petiția înregistrată la Autoritatea națională de supraveghere, un petent a sesizat faptul că o instituție financiară nebanară (IFN) a transmis datele sale personale, inclusiv date negative, la biroul de credit, fără a-l informa în prealabil cu privire la aceste operațiuni de prelucrare. Petentul a susținut că, urmare a solicitării sale, IFN-ul a refuzat să șteargă respectivele date negative raportate la biroul de credit.

În cadrul investigației efectuate, s-a constatat că IFN-ul în cauză a transmis, într-adevăr, date negative la biroul de credit cu încălcarea dispozițiilor art. 8 alin. (2) din Decizia nr. 105/2007, întrucât nu a asigurat informarea petentului cu cel puțin 15 zile calendaristice înainte de fiecare transmitere a datelor negative ale acestuia la biroul de credit.

Față de această situație, s-a aplicat o sancțiune contravențională în baza art. 32 din Legea nr. 677/2001. În urma demersurilor efectuate de Autoritatea națională de supraveghere, datele negative transmise ilegal la biroul de credit de acest IFN pe numele petentului au fost șterse.

În cazul respectivei instituții financiare nebancale, din verificarea mai multor plângeri primite de Autoritatea națională de supraveghere, s-a constatat faptul că aceasta nu respecta nici termenul de transmitere a datelor negative la biroul de credit (după 30 de zile de la data scadenței), realizând raportarea săptămânal. Ca atare, s-a pus în vedere operatorului în cauză să își modifice această practică, în sensul respectării conforme a prevederilor art. 5 alin. (1) din Decizia nr. 105/2007.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 și ale Deciziei nr. 105/2007 de către o bancă, prin raportarea datelor sale personale la biroul de credit. Astfel, petentul a reclamat faptul că banca a transmis date negative la biroul de credit fără a-l informa în prealabil, înainte de fiecare raportare. De asemenea, acesta a mai susținut faptul că i-au fost încălcate drepturile de acces, de intervenție și de a nu fi supus unei decizii automate individuale, prevăzute de Legea nr. 677/2001, întrucât banca nu a dat curs cererilor sale de exercitare a drepturilor menționate anterior și nu i-a transmis un răspuns în termenul legal de 15 zile.

În cadrul investigației, s-a constatat că banca a transmis date negative la biroul de credit, în decurs de mai mult de un an de zile, fără să informeze în prealabil petentul, așa cum prevede art. 8 din Decizia nr. 105/2007.

În acest context, banca în cauză a fost sancționată contravențional pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, pentru nerespectarea prevederilor acestei legi și ale Deciziei nr. 105/2007, dar și pentru nerespectarea drepturilor exercitate de persoana vizată.

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

2. Prelucrarea datelor personale prin mijloace de supraveghere video

Referitor la prelucrarea datelor personale prin mijloace de supraveghere video, petițiile transmise Autorității naționale de supraveghere au fost în continuare într-un număr semnificativ, 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, dar și a rolului Autorității naționale de supraveghere în apărarea acestora.

Prelucrarea datelor personale 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.

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, cât și la nivelul unor persoane juridice de drept public și privat care au montat astfel de sisteme la locurile de muncă ale salariaților proprii.

În acest context, art. 8 din Decizia nr. 52/2012 stabilește situațiile în care prelucrarea datelor personale ale angajaților prin mijloace de supraveghere video este permisă, și anume: pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora. Alin. (3) al aceluiași articol din Decizia nr. 52/2012 prevede că „nu este permisă prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video în interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă, cu excepția situațiilor prevăzute expres de lege sau a avizului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal”.

Având în vedere dispozițiile legale de mai sus, Autoritatea națională de supraveghere a apreciat faptul că efectuarea supravegherii video la locul de muncă poate fi admisă numai în situații particulare, operatorii vizați trebuind să prezinte argumente temeinice pentru a susține interesul legitim al instalării unui asemenea sistem de supraveghere, astfel încât acesta să prevaleze asupra drepturilor și libertăților fundamentale sau intereselor persoanelor

monitorizate prin utilizarea acestui sistem. În același timp, trebuie făcută dovada faptului că a fost efectuată în prealabil consultarea sindicatului sau a reprezentanților angajaților cu privire la scopurile pentru care se ia decizia de montare a camerelor de supraveghere video, cu argumentarea necesității prelucrării datelor personale ale angajaților prin aceste mijloace. De asemenea, pe tot parcursul funcționării sistemelor de supraveghere video este necesară realizarea unei informări permanente, care de obicei se asigură prin afișarea unor pictograme reprezentative, în apropierea locurilor monitorizate, însoțite de o serie de informații impuse prin Decizia nr. 52/2012.

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 inclusiv imagini din spațiul public.

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. Pe fondul proliferării instalării de camere video la nivelul condominiilor, cu ocazia investigațiilor efectuate la asociațiile de proprietari reclamate, pentru o mai bună înțelegere a obligațiilor ce le revin, a fost distribuit *Ghidul privind prelucrările de date cu caracter personal efectuate prin intermediul sistemelor de*

supraveghere video instalate în cadrul asociațiilor de proprietari, emis de Autoritatea națională de supraveghere în anul 2014 (disponibil inclusiv pe pagina de Internet a autorității).

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, inclusiv în lifturi, fără a exista o hotărâre a adunării generale a proprietarilor și fără să se realizeze informarea persoanelor vizate.

În urma investigației efectuate la respectiva asociație de proprietari, o parte dintre aspectele sesizate s-au confirmat, astfel că aceasta a fost sancționată pentru săvârșirea contravențiilor prevăzute de art. 31 (omisiunea de a notifica la Autoritatea națională de supraveghere prelucrarea efectuată prin intermediul sistemului de supraveghere video instalat), precum și de art. 32 din Legea nr. 677/2001, prin raportare la art. 4 alin. (1) lit. c) (datele prelucrate să nu fie excesive prin raportare la scopul în care sunt colectate și ulterior prelucrate) și la art. 5 alin. (1) din aceeași lege (prelucrare nelegală, fără consimțământul persoanei vizate).

De asemenea, s-a recomandat asociației, printre altele, să notifice la autoritate prelucrările de date efectuate în scop de "monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private" și să înceteze prelucrarea imaginilor prin intermediul camerelor de supraveghere instalate în lifturi.

FIȘĂ DE CAZ (unități de învățământ)

Prin petiția înregistrată la Autoritatea națională de supraveghere, petenta a reclamat faptul că școala gimnazială unde își desfășoară activitatea a instalat camere de supraveghere video în cancelaria școlii, în birourile secretariat și în anticamerele acestora, fără informarea salariaților și fără acordul lor.

Întrucât cu ocazia investigației efectuate la sediul școlii reclamate, conducerea acesteia nu a prezentat argumente temeinice care să justifice necesitatea instalării de camere de supraveghere în spații unde cadrele didactice și personalul auxiliar își desfășoară activitatea, s-a dispus sancționarea contravențională pentru săvârșirea faptei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal), prin raportare la art. 4 alin. (1) lit. c), dar și pentru nesocotirea dreptului de informare al persoanelor vizate (art. 12 din

Legea nr. 677/2001). Totodată, având în vedere că școala nu a transmis un răspuns petentei la cererea sa, prin care aceasta își exercita dreptul de acces, a fost aplicată o sancțiune și în temeiul art. 32, raportat la dispozițiile art. 13 din Legea nr. 677/2001.

În urma investigației, unitatea școlară a informat Autoritatea națională de supraveghere că a dat curs recomandărilor primite, în sensul demontării camerelor instalate nelegal și a transmiterii unui răspuns adecvat la cererea petentei.

FIȘĂ DE CAZ (supraveghere video la locul de muncă)

Un inspectorat teritorial de muncă a redirectionat la Autoritatea națională de supraveghere petiția salariaților din cadrul unui agent economic din industria confecțiilor, spre a fi efectuate verificări sub aspectul prelucrării datelor personale prin utilizarea mijloacelor de supraveghere video, instalate, conform sesizării, în scopul monitorizării și intimidării angajaților.

În cadrul investigației dispuse, s-au confirmat aspectele sesizate, motiv pentru care operatorul a fost sancționat contravențional pentru săvârșirea faptelor prevăzute de art. 31 din Legea nr. 677/2001, întrucât a omis să notifice prelucrarea efectuată prin intermediul camerelor de supraveghere, așa cum prevede art. 22 din aceeași lege, și respectiv, de art. 32 din Legea nr. 677/2001, atât pentru prelucrarea în mod excesiv a datelor personale (imaginea) ale angajaților săi, prin intermediul camerelor video instalate, cât și pentru inexistența unei informări corespunzătoare a persoanelor vizate. De asemenea, s-a mai aplicat o sancțiune contravențională în temeiul art. 33 din aceeași lege, întrucât s-a constatat că nu au fost adoptate suficiente măsuri de confidențialitate și securitate a datelor prelucrate (în privința restricționării accesului la înregistrări, spre exemplu), așa cum impun dispozițiile art. 19 și 20 din Legea nr. 677/2001.

În prezent, se află pe rolul instanțelor judecătorești contestația introdusă împotriva actului de control al Autorității naționale de supraveghere.

FIȘĂ DE CAZ (persoane fizice)

Prin petiția transmisă la Autoritatea națională de supraveghere, s-a reclamat instalarea și funcționarea unui sistem de supraveghere video compus din două camere, care surprinde imagini atât din exteriorul blocului, cât și de la nivelul palierului de la etajul patru, fără acordul locatarilor din acest bloc.

La data efectuării investigației, s-au confirmat aspectele sesizate, motiv pentru care în urma investigației, proprietarul care a instalat camerele de supraveghere video a fost sancționat contravențional pentru săvârșirea faptelor prevăzute de art. 31 din Legea nr. 677/2001, întrucât a omis să notifice în calitate de operator prelucrarea efectuată prin intermediul camerelor de supraveghere, așa cum prevede art. 22 din Legea nr. 677/2001, precum și de art. 32 din aceeași lege, pentru lipsa unei informări corespunzătoare a persoanelor vizate și prelucrarea în mod excesiv a datelor personale (imaginea) ale persoanelor vizate, prin intermediul camerelor video instalate. De asemenea, s-a mai constatat faptul că nu a fost transmis un răspuns la cererea petentei, formulată în baza art. 15 din Legea nr. 677/2001, fiind aplicată o sancțiune și pentru această faptă.

În baza constatărilor, s-a recomandat persoanei în cauză să notifice prelucrările de date (imaginea) pe care le efectuează prin intermediul sistemului de supraveghere video, să adopte măsurile de informare a persoanelor vizate, conform art. 12 din Legea nr. 677/2001 și art. 11 din Decizia nr. 52/2012, să obțină acordul scris al tuturor vecinilor de pe palierul etajului patru sau să schimbe unghiul camerei astfel încât să surprindă imagini exclusiv de pe proprietatea sa. Totodată, i s-a recomandat să răspundă la cererea petentei, conform Legii nr. 677/2001.

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 publicului larg (prin publicarea pe site-uri, blog-uri etc.) sau către diverse entități de drept public și privat, fără să fi fost obținut în prealabil acordul persoanelor vizate sau fără informarea 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.

Urmare a publicării datelor personale pe diverse site-uri, acestea sunt indexate ulterior pe Internet cu ajutorul motoarelor de căutare. De aceea, în cazul în care informațiile respective nu prezintă relevanță pentru interesul public, nu mai sunt de actualitate ori nu sunt corecte, se impune ștergerea acestora; în acest sens, persoanele vizate pot solicita direct motoarelor de căutare să le respecte "dreptul de a fi uitat", așa cum a fost acesta consacrat în dreptul european și în jurisprudența CJUE.

a) "Dreptul de a fi uitat" pe Internet

În anul 2015, Autoritatea națională de supraveghere a înregistrat o serie de plângeri având ca obiect dezvăluirea datelor personale pe Internet, indexate ulterior cu ajutorul motoarelor de căutare, în legătură cu derularea unor proceduri judiciare, pe diverse pagini administrate de către persoane fizice sau entități private ori în cadrul unor articole de presă publicate electronic. În cazul plângerilor considerate admisibile au fost efectuate investigații pentru soluționarea aspectelor reclamate.

În cele mai multe dintre cazuri, Google Inc. nu a dat curs solicitării petenților de ștergere a adreselor URL la care se găseau datele lor personale, pe motiv că respectivele informații sunt de interes public. La solicitarea Autorității naționale de supraveghere, cazurile au fost soluționate în favoarea petenților, în majoritatea lor.

În analizarea fiecărei plângeri primite care se află în această arie de interes, Autoritatea națională de supraveghere a luat în considerare argumentele reținute prin Hotărârea 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), dar și liniile directoare stabilite potrivit "Ghidului 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", adoptat de Grupul de Lucru Art. 29, din care face parte și Autoritatea națională de supraveghere din România.

FIȘĂ DE CAZ

O petentă a sesizat faptul că datele sale personale au fost publicate pe două site-uri (administrare de entități private), ca urmare a calității sale de parte în mai multe dosare soluționate de instanțele judecătorești. Petenta s-a adresat Google Inc. cu solicitarea de eliminare din lista de căutări a unei singure adrese URL la care erau publicate datele sale personale, însă nu s-a dat curs solicitării, pe motiv că respectiva adresă URL include informații de interes public. Totodată, i s-a recomandat petentei să se adreseze autorității naționale pentru protecția datelor, în cazul în care este nemulțumită de răspunsul primit.

În urma primirii adresei transmise de Autoritatea națională de supraveghere, în cadrul investigației demarate, Google Inc. nu a șters adresa URL din căutări, pe motiv că aceasta ar aparține "de o organizație sau de o agenție guvernamentală".

Printr-o adresă ulterioară, Autoritatea națională de supraveghere a menționat că adresa URL care face obiectul plângerii nu aparține "de o organizație sau de o agenție guvernamentală", site-ul unde au fost publicate datele personale ale petentei este înregistrat pe teritoriul altui stat (SUA) și nici nu conține date de identificare ale deținătorului acestui site, pentru a permite celor interesați să i se adreseze direct. De asemenea, s-a mai adus la cunoștința Google Inc. faptul că, în România, cele două portaluri oficiale care oferă informații publice privind cauzele aflate pe rolul instanțelor judecătorești (portal.just.ro și www.scj.ro) nu sunt indexate pe Internet.

În urma demersurilor efectuate, Google Inc. a luat decizia de a bloca adresa URL respectivă, astfel încât aceasta nu mai este generată de motorul de căutare Google ca urmare a efectuării unei căutări pe baza numelui și prenumelui petentei.

FIȘĂ DE CAZ

Un petent a sesizat faptul că datele sale personale (imaginea), asociate cu o serie de informații false și defăimătoare, au fost publicate pe un blog, de către o persoană necunoscută. Informațiile considerate false se refereau la infracțiunea de trafic de droguri, infracțiune de care a fost acuzat petentul în urmă cu patru ani, acesta susținând că afirmațiile sunt false.

Potentul a făcut dovada că s-a adresat la Google Inc. cu solicitarea de a i se șterge datele sale cu caracter personal din motorul de căutare, însă nu s-a dat curs solicitării sale în termen de 15 zile, transmițându-i-se un răspuns automat prin care se comunica faptul că solicitarea sa a fost primită, mesajul este în așteptare și solicitarea va fi procesată imediat ce fluxul de lucru o va permite.

În urma demersurilor efectuate de Autoritatea națională de supraveghere, adresa URL la care se aflau datele personale ale petentului a fost eliminată de Google Inc. din lista de căutări.

b) Alte cazuri

Autoritatea națională de supraveghere a fost sesizată prin diverse plângeri cu privire la dezvăluirea datelor personale către alte entități care nu aveau niciun drept să intre în posesia acestora, ori cu privire la publicarea pe Internet a unor informații fără consimțământul persoanei vizate sau alt temei legal; în unele cazuri, dezvăluirea datelor poate să aibă ca efect chiar producerea unor prejudicii de imagine.

FIȘĂ DE CAZ

O petentă a reclamat că pe un anumit site, administrat de către o asociație, este afișat numele și prenumele său, titlul profesional, faptul că a făcut obiectul unei decizii a Consiliului Național de Etică a Cercetării Științifice, Dezvoltării Tehnologice și Inovării din cadrul Autorității Naționale pentru Cercetare Științifică și că în sarcina sa a fost constatat un plagiat, cu posibilitatea de accesare a conținutului unei decizii prin care se aprobă un Raport final care conține, printre altele, recomandări privind sancționarea petentei, fără a se menționa termenul de "plagiat".

Petenta a considerat excesivă prelucrarea datelor sale personale pe site-ul asociației și pentru faptul că, pe site-ul instituției de pe care a fost preluată decizia în care apar datele personale ale petentei, respectiva decizie este listată fără asociere cu numele său.

Asociația a susținut că scopul invocării numelui petentei, în legătură cu fișierul care cuprinde Decizia în care apar datele acesteia, este informarea corectă și eficientă a vizitatorilor site-ului asociației asupra cazurilor de plagiat pe care organul Ministerului Educației le-a tratat și soluționat, asociația rezumând conținutul documentului și facilitând, din punct de vedere tehnic, accesul la acesta.

Ca urmare a investigației efectuate, s-a constatat faptul că asociația, al cărei scop declarat este prevenirea și combaterea plagiatului în mediul universitar, a prelucrat în mod excesiv pe site-ul pe care îl administrează, numele și prenumele petentei, precum și informații legate de persoana sa (titlul profesional, faptul că a făcut obiectul unei decizii a Consiliului Național de Etică a Cercetării Științifice, Dezvoltării Tehnologice și Inovării din cadrul Autorității Naționale pentru Cercetare Științifică, precum și că în sarcina sa a fost constatat un plagiat), având în vedere faptul că, pe site-ul emitentului hotărârii în cauză, respectivul document este publicat fără referințe la numele petentei sau alte informații care ar putea duce la identificarea acesteia sau la constatarea unui plagiat, datele personale ale petentei putând fi vizualizate numai după accesarea documentului. Totodată, s-a constatat că adresa URL de pe site-ul Asociației, unde se află datele personale ale petentei, este indexată în motoarele de căutare.

Ca atare, la finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a aplicat asociației o sancțiune contravențională în baza art. 32 din Legea nr. 677/2001, pentru prelucrarea excesivă a datelor personale ale petentei, prin raportare la scopul în care au fost colectate de către asociație. Totodată, a fost emisă o decizie de ștergere a datelor personale ale petentei de pe site-ul administrat de asociație.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că un birou de executori judecătorești i-a dezvăluit datele personale din dosarul de executare silită către terți, persoane fizice și juridice, care nu au nicio calitate în dosarul de executare.

În urma investigației realizate, s-a constatat faptul că nu datele petentului au fost dezvăluite de către biroul de executori judecătorești, ci datele unui alt client al operatorului au fost dezvăluite către petent. Această dezvăluire a avut loc dintr-o eroare materială datorată modului de numerotare a dosarelor de executare.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat biroul de executori judecătorești, în baza art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale), dar și a art. 33 din aceeași lege, întrucât nu a aplicat măsuri tehnice și organizatorice adecvate pentru protejarea datelor personale împotriva dezvăluirii ilegale sau neautorizate a datelor personale către terți.

4. Prelucrarea excesivă a datelor personale

Din practica de soluționare a plângerilor și sesizărilor adresate Autorității naționale de supraveghere în cursul anului 2015, se constată situații diverse de încălcare a prevederilor Legii nr. 677/2001, sub aspectul nerespectării principiului proporționalității în luarea deciziei de a prelucra anumite date personale. Astfel, unii operatori au ales să prelucreze date personale (chiar din categoria celor protejate prin reguli speciale, cum sunt codul numeric personal ori datele biometrice), în scopuri pentru realizarea cărora se puteau limita categoriile de date la cele strict necesare. Coroborat cu aceste aspecte, s-a mai constatat faptul că, în anumite cazuri, datele au continuat să fie stocate sau prelucrate după expirarea perioadei legale, deși acestea nu mai erau necesare, prin raportare la justificarea colectării lor inițiale. De asemenea, Autoritatea națională de supraveghere, potrivit opiniilor sale constante, nu a permis prelucrarea datelor biometrice în scopul realizării accesului la locul de muncă sau pontării orelor de muncă, în situațiile incidente putând fi alese de către operatori mijloace mai puțin intruzive pentru viața privată a persoanelor.

FIȘĂ DE CAZ

Printr-o petiție înregistrată la Autoritatea națională de supraveghere, un avocat a sesizat o posibilă încălcare a prevederilor legale de către o societate de avocatură. Astfel, s-a sesizat că, în calitate de titular al cabinetului său de avocatură, acesta a încheiat un contract de conlucrare cu societatea de avocatură respectivă, deținând în cadrul acestei societăți calitatea de avocat senior. În acest context, în cadrul societății i-a fost alocată o adresă de e-mail profesională, pe care erau transferate și e-mailurile primite de petent pe o adresă personală.

Urmare a transmiterii unei notificări de reziliere a contractului de conlucrare, cu efect imediat, petentului i-a fost interzis accesul la adresa sa de e-mail, fără însă ca societatea de avocatură să șteargă efectiv acest cont, continuând să acceseze contul de e-mail și parcurgând corespondența care îi era adresată petentului, conform dovezilor deținute de acesta.

Potentul a sesizat faptul că nu a semnat niciodată vreun document cu societatea de avocatură nici la momentul înființării societății, prin contractul de conlucrare, nici ulterior, pe perioada derulării activității societății, până la momentul încetării raporturilor juridice, care să ateste drepturile și obligațiile în privința utilizării și accesării conturilor profesionale.

Urmare a investigației efectuate de Autoritatea națională de supraveghere, aspectele sesizate au fost confirmate, astfel că s-a constatat săvârșirea faptei prevăzute de art. 32 din Legea nr. 677/2001, prin încălcarea prevederilor art. 4 potrivit cărora datele personale trebuie să fie prelucrate în scopuri legitime, neexcesive prin raportare la scopul în care sunt prelucrate și stocate numai pe durata necesară realizării scopului. De asemenea, s-au mai aplicat sancțiuni pentru nerespectarea drepturilor de informare și opoziție, prevăzute de art. 12 și 15 din Legea nr. 677/2001.

În prezent, se află pe rolul instanțelor judecătorești contestația introdusă împotriva actului de control al Autorității naționale de supraveghere.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată că la o fabrică de mobilă sunt instalate camere de supraveghere video pentru a urmări activitatea angajaților. De asemenea, Autoritatea națională de supraveghere a fost sesizată că au fost prelucrate datele biometrice (amprente) ale salariaților în scopul realizării pontajului.

Urmare a investigației efectuate, s-a constatat că angajații acestei fabrici au fost obligați să se înregistreze în sistemul de pontare cu datele biometrice, fără să semneze în acest sens

niciun document care să ateste acordul sau informarea lor prealabilă privind scopul prelucrării și destinării datelor ori drepturile prevăzute de Legea nr. 677/2001.

Întrucât în cadrul controlului s-a constatat că au fost prelucrate în mod excesiv datele personale (imaginea) ale angajaților prin intermediul camerelor video instalate în spațiul în care aceștia își desfășoară activitatea, prin raportare la scopul colectării datelor (asigurarea securității spațiilor și bunurilor private), s-a reținut săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001. Totodată, s-a emis o decizie de încetare a prelucrării datelor personale, prelucrate prin intermediul camerelor de supraveghere video orientate direct spre spațiile de lucru în care angajații își desfășoară activitatea în mod curent, precum și al celor plasate în mod excesiv în secțiile de lucru, raportat la numărul de angajați, riscul activității din fiecare secție în parte și antecedentele existente; prin decizie s-a dispus inclusiv ștergerea înregistrărilor preluate prin respectivele camere.

În ceea ce privește prelucrarea datelor biometrice ale angajaților, dat fiind scopul declarat al prelucrării (evidența timpului de lucru al angajaților) și existența altor mijloace alternative de prelucrare, mai puțin intruzive, ce puteau fi utilizate pentru atingerea aceluiași scop, această prelucrare s-a considerat, de asemenea, excesivă, intrând sub incidența art. 32 din Legea nr. 677/2001; s-a emis, totodată, o decizie prin care s-a dispus încetarea prelucrării datelor biometrice ale angajaților și ștergerea acestora din baza de date, societatea urmând să implementeze alte metode de evidențiere a timpului de lucru al angajaților, cu respectarea principiului proporționalității datelor personale.

În prezent, se află pe rolul instanțelor judecătorești contestația introdusă împotriva actelor emise de Autoritatea națională de supraveghere în urma acestei investigații.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată prin mai multe petiții cu privire la prelucrarea codului numeric personal, colectat în cadrul campaniilor promoționale desfășurate de o societate de comercializare a produselor din tutun și utilizat ulterior în scopuri legate de publicitate și marketing.

Urmare a investigației efectuate, societatea respectivă a justificat necesitatea colectării obligatorii a codului numeric personal de la toți participanții la campaniile lor promoționale, pentru a evita implicarea minorilor în activitatea de publicitate la produsele de tutun, activitate interzisă prin legislația specifică. Autoritatea națională de supraveghere a constatat că, urmare

a colectării codului numeric personal al consumatorilor, nu se realizează o altă verificare a identității decât cea privind validarea formulei de calcul a acestuia și nici nu s-a încercat o altă modalitate de verificare a exactității și corectitudinii datelor personale colectate de la consumatori, în special cea legată de data nașterii, pentru a se evita colectarea inițială a datelor personale de la persoane minore și prelucrarea ulterioară a acestora în scop de marketing pentru produse din tutun. De asemenea, în baza de date folosită de operator erau în continuare stocate datele personale, inclusiv codul numeric personal al consumatorilor, indiferent de vârsta (majoră) a acestora, pe o perioadă excesivă față de scopul declarat.

În consecință, operatorul a fost sancționat pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a colectat și stocat excesiv date personale, inclusiv codul numeric personal, ale persoanelor participante la diverse acțiuni promoționale ale produselor sale de tutun, prin raportare la scopul declarat al prelucrării, și s-a dispus identificarea unor mijloace adecvate de identificare a persoanelor adulte fumătoare în scopuri legate de promovarea produselor de tutun, fără a fi necesară colectarea codului numeric personal al acestora; s-a mai recomandat instruirea corespunzătoare în acest sens a angajaților/reprezentanților/persoanelor împuternicite care participă la colectarea efectivă a datelor personale.

5. Nerespectarea drepturilor de informare, acces, intervenție și opoziție

Nerespectarea drepturilor prevăzute de Legea nr. 677/2001, respectiv dreptul la informare (art. 12), dreptul de acces la date (art. 13), dreptul de intervenție asupra datelor (art. 14) și dreptul de opoziție (art. 15), ca urmare a exercitării acestora de către persoanele vizate, a continuat să reprezinte obiectul multor petiții adresate instituției noastre în 2015. În urma investigațiilor efectuate, s-a constatat că operatorii fie nu cunosc obligațiile care le incumbă potrivit reglementărilor legale susmenționate, fie le ignoră cu bună-știință, fie transmit persoanelor vizate răspunsuri incomplete sau/și fără respectarea termenului de 15 zile prevăzut de lege.

Cu privire la dreptul de informare, se reține faptul că importanța deosebită pe care trebuie să o acorde operatorii acestui drept, indiferent de calitatea lor de persoane de drept public ori privat, a fost confirmată prin Hotărârea pronunțată de CJUE la 1 octombrie 2015 în cauza Smaranda Bara și alții împotriva Președintelui Casei Naționale de Asigurări de Sănătate, Casei Naționale de Asigurări de Sănătate și Agenției Naționale de Administrare Fiscală (ANAF) –

(C-201/14), în contextul transferului datelor personale ale contribuabililor între aceste două instituții, pe baza unui protocol bilateral.

FIȘĂ DE CAZ

O petentă a sesizat faptul că a solicitat unui operator de date mai multe informații referitoare la condițiile în care sunt prelucrate datele sale personale și ale membrilor familiei sale, în calitate de client/clientă ai unei rețele private de sănătate. Petenta menționa că nu a primit vreun răspuns la solicitarea sa, trimisă prin poștă, cu confirmare de primire.

Din informațiile obținute în cadrul investigației, a rezultat că datele petentei și ale familiei sale erau prelucrate de către respectivul operator de date, în scopul oferirii de servicii medicale la solicitarea acestora, prin intermediul a două aplicații interconectate, putând fi identificate, pe bază de user și parolă, persoanele care au accesat sistemul.

În cadrul investigației, operatorul de date a declarat că nu a comunicat un răspuns la cererea petentei, deoarece această petiție nu a putut fi identificată în evidențele proprii. Întrucât din documentele verificate, a reieșit că petenta și-a exercitat dreptul de acces printr-o cerere transmisă în scris, prin poștă, cu confirmare de primire semnată de reprezentanții operatorului, acesta a fost sancționat pentru încălcarea obligației prevăzute de art. 13 din Legea nr. 677/2001, conform căreia operatorul este obligat să comunice persoanei vizate informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele, în termen de 15 zile de la data primirii cererii (art. 13 din Legea nr. 677/2001).

De asemenea, s-a mai aplicat o sancțiune pentru contravenția prevăzută de art. 33 din Legea nr. 677/2001, având în vedere că operatorul nu a aplicat măsuri tehnice și organizatorice adecvate împotriva pierderii datelor personale.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001, de către o societate de telefonie, reclamând că aceasta i-a încălcat drepturile de acces și de intervenție și nu i-a furnizat toate informațiile solicitate prin cererea adresată.

Întrucât petentul era nemulțumit de dezvăluirea datelor sale în mod ilegal către o societate de recuperare creanțe, a solicitat informații cu privire la dezvăluirea datelor sale personale, precum și luarea măsurilor necesare astfel încât datele sale să nu mai fie folosite de

către terți. Din verificările efectuate în cadrul investigației, s-a constatat că societatea de recuperare creanțe deținea calitatea de persoană împuternicită în relația cu societatea de telefonie, iar datele petentului au fost transmise în mod eronat către aceasta de operatorul de date. Deși reprezentanții societății de telefonie au declarat că la cererea petentului s-a transmis un răspuns, din verificările efectuate în cursul investigației s-a constatat că, prin acest răspuns, operatorul nu i-a comunicat petentului informații complete privind destinatarii către care a dezvăluit datele sale personale; de asemenea, modul de soluționare a solicitării privind încetarea prelucrării datelor sale personale de către împuternicit era în contradicție cu prevederile art. 13 și art. 14 din Legea nr. 677/2001.

În consecință, operatorul a fost sancționat contravențional pentru faptele prevăzute de art. 32 din Legea nr. 677/2001, prin raportare la art. 13 și art. 14 din Legea nr. 677/2001, punându-i-se în vedere să reformuleze un răspuns complet petentului.

FIȘĂ DE CAZ

Un petent s-a adresat Autorității naționale de supraveghere reclamând faptul că o autoritate publică i-a încălcat dreptul de opoziție prevăzut de Legea nr. 677/2001, întrucât nu a încetat prelucrarea datelor sale personale aferente contului înregistrat pe numele său la două adrese de Internet asociate serviciilor on line puse la dispoziție de autoritate, deși a solicitat acest lucru prin mai multe petiții. De asemenea, petentul a susținut că nu a primit răspuns în termenul de 15 zile prevăzut de Legea nr. 677/2001.

Din afirmațiile petentului a reieșit că înregistrarea contului său a avut loc în decembrie 2014, în urma promovării serviciului "Spațiul Privat Virtual" de către autoritatea publică reclamată. În urma investigației efectuate, a rezultat că acest cont, înregistrat pe numele petentului în cadrul respectivului serviciu, a fost dezactivat de operator în luna martie 2015.

În ceea ce privește cererile petentului, s-a constatat că acesta s-a adresat operatorului și i s-a comunicat că a fost anulat contul deschis pe numele său în spațiul privat virtual de pe portal. Astfel, întrucât operatorul nu a comunicat petentului un răspuns în termenul de 15 zile prevăzut de art. 15 alin. (4) din Legea nr. 677/2001, a fost sancționat contravențional pentru fapta prevăzută la art. 32 din Legea nr. 677/2001.

De asemenea, autoritatea publică a fost sancționată deoarece nu a dovedit că asigura informarea persoanelor vizate, conform prevederilor art. 12 din Legea nr. 677/2001, în special

cu privire la drepturile de care beneficiază persoanele vizate potrivit acestei legi (dreptul de acces, dreptul de intervenție și dreptul de opoziție) și condițiile de exercitare a acestora.

6. Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

În cursul anului 2015, s-a menținut numărul ridicat de plângeri și sesizări 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, respectiv primirea de mesaje comerciale nesolicitate prin poșta electronică, fără consimțământul expres și neechivoc al destinatarului în acest sens.

În vederea soluționării 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, unul dintre motive fiind legat de nefuncționarea unor mecanisme adecvate de abonare (dublu "opt-in") și dezabonare.

FIȘĂ DE CAZ

Prin mai multe petiții, Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că persoane fizice sunt contactate telefonic și în scris, în mod repetat, în scopul promovării produselor unei societăți, în condițiile în care petiționarii nu și-au furnizat datele personale (nume, prenume, adresă, telefon) către societatea respectivă.

Ca urmare a investigației efectuate la această societate (S1), s-a constatat faptul că apelurile telefonice inițiate către petenți s-au realizat urmare a utilizării unei baze de date achiziționate de la o altă societate (S2), în baza unui contract de prestări servicii, ce conținea nume, prenume, adresă completă, unul sau mai multe numere de telefon (fix și/sau mobil). Contractul nu conținea clauze privind proveniența datelor din baza de date furnizată de S2 sau existența consimțământului persoanelor de a le fi prelucrate datele sau de a fi contactate în scop de marketing.

În urma investigației efectuate la S2, s-a constatat faptul că baza respectivă de date provenea de la o altă societate (S3), în baza unui contract, dar care nu conținea clauze din care să rezulte că datele urmau să fie furnizate către S1 și nici clauze privind asumarea răspunderii pentru legalitatea colectării și prelucrării datelor de către S3.

Ca urmare a investigațiilor efectuate la cele trei societăți, s-a constatat faptul că acestea au colectat, utilizat, stocat temporar, transmis date personale ale unor persoane fizice sau au prelucrat date personale ale potențialilor clienți, fără consimțământul unora dintre aceste persoane și fără să realizeze o informare completă, corespunzătoare, inclusiv sub aspectul drepturilor prevăzute de Legea nr. 677/2001. Prima societate a fost sancționată inclusiv în baza Legii nr. 506/2004, pentru transmiterea de comunicări comerciale fără consimțământul prealabil al persoanelor apelate telefonic.

FIȘĂ DE CAZ

O petentă a reclamat faptul că a primit de la o societate un mesaj comercial nesolicitat pe adresa sa de e-mail, în conținutul căruia se promovează produse alimentare, deși nu s-a abonat la un astfel de serviciu (trimitere electronică de "newsletter") și în consecință nu a solicitat să primească comunicări comerciale sau de altă natură de la societate. Petenta s-a adresat în prealabil operatorului, solicitând informații în legătură cu primirea mesajului comercial, însă nu a primit niciun răspuns.

În urma investigației efectuate, s-a constatat faptul că societatea nu a obținut consimțământul expres al petentei pentru transmiterea de mesaje comerciale și nici nu a formulat și transmis un răspuns petentei la solicitarea sa.

Față de constatări, operatorului reclamat i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001 și a Legii nr. 506/2004.

FIȘĂ DE CAZ

O petentă a reclamat primirea mai multor mesaje comerciale, pe numărul său de telefon, din partea unei bănci cu care nu avea o relație contractuală.

Petenta s-a adresat băncii prin intermediul mai multor sesizări, iar din răspunsul operatorului a rezultat că numărul său de telefon a fost furnizat (în mod eronat) ca număr de contact de către o altă persoană, client al băncii și că se vor întreprinde demersuri astfel încât

asemenea situații să fie evitate. Cu toate acestea, petenta a continuat să primească mesaje comerciale din partea băncii.

Față de constatări, operatorului reclamat i-a fost aplicată o sancțiune contravențională în baza Legii nr. 506/2004, întrucât a trimis către numărul de telefon al petentei comunicări comerciale nesolicitate, fără consimțământul acesteia, deși a fost sesizat de către petentă în repetate rânduri că numărul de telefon îi aparține și că nu dorește să primească mesaje din partea operatorului, pe acest număr de telefon.

CAPITOLUL AL V-LEA

ACTIVITATEA ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE

Activitatea Autorității naționale de supraveghere a fost marcată de participarea la reuniunile europene, dominate de probleme complexe și tehnologice. Acest angajament a fost necesar pentru a aprofunda respectivele aspecte în toate domeniile de aplicare și în toată complexitatea lor. Autoritatea națională de supraveghere, reprezentantă de membrii săi, a participat în 2015 la o serie de reuniuni și diverse grupuri de lucru la nivel european. Printre acestea se numără:

- Grupul de Lucru Articolul 29 (înființat în temeiul art. 29 din Directiva 95/46/CE) care reunește toate autoritățile europene, precum și Autoritatea Europeană pentru Protecția Datelor. În acest context, Autoritatea națională de supraveghere, prin membrii săi, a participat la următoarele subgrupuri de lucru: Tehnologie, Transferuri Internaționale, Probleme financiare și BTLE,
 - Comitetul Consultativ al Convenției 108 al Consiliului Europei (T-PD),
 - Organismul comun de control în domeniul Europol și domeniul Vamal,
 - Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II și Grupul de coordonare comună Eurodac,
 - Grupul Internațional de lucru pentru protecția datelor în domeniul Telecomunicațiilor, dedicat protecției datelor cu caracter personal în sectorul comunicațiilor electronice,
 - Seminarul european pentru schimbul de experiență în rezolvarea cazurilor practice (Case Handling Workshop),
 - Grupul de Lucru pentru protecția datelor în cadrul Convenției pentru stabilirea Centrului Sud-Est European de aplicare a legii.

❖ Grupul de Lucru Articolul 29

Grupul de Lucru Articolul 29, înființat în temeiul art. 29 din Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, reprezintă un organism independent, cu rol consultativ. Obiectivul

acestui organism, ce reunește autoritățile naționale pentru protecția datelor de la nivel european, este acela de a examina aspecte referitoare la protecția datelor cu caracter personal și de a promova o aplicare uniformă a directivei în statele membre ale Uniunii Europene. Printre subiectele dezbătute în anul 2015, menționăm următoarele documente ce au fost adoptate, fie sub formă de avize, fie sub formă de documente de lucru:

- *analiză a căutărilor în vederea identificării de cookie* – această căutare pune în evidență diferențele în utilizarea cookie în diferite sectoare și în statele membre;

- *schimburile automate de date cu caracter personal în scop fiscal* – autoritățile pentru protecția datelor de la nivelul Uniunii Europene au analizat noile tendințe prin care intenționează introducerea de noi mecanisme pentru schimburile automate de date personale în scop fiscal, precum și impactul acestora asupra vieții private și a protecției datelor personale, deoarece schimbul de informații este văzut ca un instrument esențial în lupta împotriva evaziunii fiscale. În acest context, este esențial să se asigure că sunt respectate condițiile necesare pentru o prelucrare legală și corectă a datelor. Prevenirea evaziunii fiscale reprezintă un obiectiv al interesului public general și, în același timp, o activitate ce are un impact asupra oricărui cetățean. Astfel, statele trebuie să urmărească aceste obiective, însă cu respectarea în totalitate a drepturilor fundamentale ale persoanelor, în special dreptul la viață privată și dreptul la protecția datelor cu caracter personal, cu respectarea instrumentelor juridice europene și internaționale;

- *regulile corporatiste obligatorii pentru împuterniciți* – Grupul de Lucru Articolul 29 consideră că un astfel de ghid poate facilita aplicarea art. 26 (2) din Directiva 95/46/CE pentru situația regulilor corporatiste obligatorii pentru împuterniciți. Ar trebui, de asemenea, să conducă la un anumit grad de simplificare pentru organizațiile multinaționale ce prelucrează și efectuează în mod curent schimb de date la nivel mondial, pe seama operatorilor. Conținutul acestui document de lucru nu trebuie considerat ca fiind ultimul cuvânt al Grupului de Lucru Articolul 29 pe această temă, ci mai degrabă o primă fază solidă de a evidenția posibilitatea de a utiliza regulile corporatiste obligatorii pentru împuterniciți pe baza unei abordări de auto-reglementare și cooperare între autorități, fără a prejudicia posibilitatea de a utiliza alte instrumente pentru transferul de date cu caracter personal în străinătate, cum ar fi clauzele contractuale standard;

- *confidențialitatea și protecția datelor personale în contextul utilizării de drone* – documentul include abordarea impactului asupra vieții private și a protecției datelor personale,

precum și consecințele utilizării extinse a diferitelor aplicații de drone pentru diferite utilizări civile. De asemenea, au făcut obiectul analizei și particularitățile și criticile referitoare la îndeplinirea cerințelor specifice potrivit cadrului normativ existent pe protecția datelor. În concluzie, sunt emise recomandări privind modul în care sunt abordate în mod adecvat riscurile ce pot apărea în legătură cu dronele, precum și recomandări legate de scopul utilizării acestora, astfel încât prelucrarea datelor personale să fie legală și conformă cu cadrul normativ în materie;

➤ *codul de conduită privind serviciile de cloud (cloud computing)* – prin opinia Grupului de Lucru Articolul 29 este analizat codul de conduită pentru furnizorii de servicii cloud. Grupul de lucru nu a aprobat proiectul de cod întrucât acesta nu respecta cerințele legale minime, iar valoarea adăugată a respectivului cod cu privire la Directiva 95/46/CE și legislația națională nu a fost foarte clară. Astfel, opinia a analizat principalele aspecte prin evidențierea punctelor de interes, în special următoarele: consecințele aderării la codul de conduită, responsabilitatea, transparența cu privire la locația prelucrării datelor cu caracter personal, prelucrarea categoriilor speciale de date, transferul internațional de date și accesul autorităților de aplicare a legii, măsurile de securitate;

➤ *proiectul de directivă privind protecția persoanelor fizice referitor la prelucrarea datelor personale de către autoritățile competente în scopul prevenirii, identificării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date;*

➤ *ghid privind criteriile pentru asigurarea conformității cu cerințele pe protecția datelor în cadrul schimbului automat de date cu caracter personal în scopuri fiscale* – scopul acestui ghid este de a asigura respectarea cerințelor pe protecția datelor în cadrul schimbului automat de date între autoritățile competente din diferite state în scopuri fiscale.

❖ **Comitetul Consultativ al Convenției 108 al Consiliului Europei**

Autoritatea națională de supraveghere a participat la reuniunile Comitetului Consultativ al Convenției 108 pentru protecția persoanelor cu privire la procesarea automată a datelor personale, în cadrul cărora s-au dezbătut, în principal, următoarele subiecte:

- modernizarea Convenției 108
- protecția datelor medicale
- protecția datelor personale și utilizarea acestora în sectorul polițienesc

- schimbul automat de date cu caracter personal în scopuri administrative și fiscale
- protecția datelor și „Big Data”
- utilizarea profilării în contextul luptei împotriva terorismului.

De asemenea, Comitetul Consultativ al Consiliului Europei a continuat promovarea sărbătoririi Zilei europene a protecției datelor și a asigurat că sensibilizarea și educația în domeniul protecției datelor cu caracter personal rămân elemente esențiale pentru activitățile diferitelor părți interesate.

❖ **Organismul comun de control în domeniul Europol și domeniul Vamal**

În cadrul reuniunilor din 2015 subiectele ce au făcut obiectul discuțiilor au privit în principal modificările care vor surveni în activitatea de supraveghere a Europol în urma intrării în vigoare a noului Regulament Europol. Astfel, această reformă aliniază temeiul legal al Europol cu prevederile Tratatului de la Lisabona.

O schimbare importantă va consta în modificarea organismului de supraveghere – JSB Europol, care va fi înlocuit de un Grup de Coordonare Comună, alcătuit din reprezentanții autorităților de supraveghere de la nivel național și cei ai Autorității Europene pentru Protecția Datelor. Începând cu 1 aprilie 2017, data la care vor intra în vigoare prevederile noului Regulament Europol, se va modifica și modul de lucru în cadrul noului grup de supraveghere, astfel fiind necesară asigurarea unei tranziții eficiente a documentelor/avizelor adoptate sau în curs de adoptare la nivelul Organismului comun de control în domeniul Europol.

❖ **Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II și Grupul de coordonare comună Eurodac**

Cooperarea dintre autoritățile pentru protecția datelor a avut loc sub forma reuniunilor organizate periodic împreună cu Autoritatea Europeană pentru Protecția Datelor, care acționează sub denumirea de grup de coordonare comună VIS, grup de coordonare comună SIS II și grup de coordonare comună Eurodac. Scopul principal al acestor întâlniri este de a analiza problemele comune legate de activitatea de supraveghere/monitorizare și de a identifica soluții sau abordări comune ori de câte ori este posibil. La reuniunile grupurilor de coordonare comună pot participa reprezentanți ai Comisiei Europene și ai Agenției IT a Uniunii Europene - LISA (eu-LISA) cu scopul de a oferi informații privind noile evoluții ale respectivelor sisteme de informații.

Potrivit programului de lucru, Grupul de coordonare comună VIS a decis să evalueze activitatea la nivel național prin a analiza, *inter alia*, ce autorități au de fapt acces la sistemul VIS, dacă există alte autorități în afară de cele deja menționate în listele autorităților ce au acces la VIS notificate de statele membre și modul efectiv de realizare a accesului. Așadar, au fost elaborate și circulat în cadrul grupului 2 chestionare cuprinzând întrebări cu privire la aceste aspecte, după cum urmează:

- chestionar privind autoritățile ce au acces la datele VIS,
- chestionar privind accesul la VIS în scop de aplicare a legii.

Totodată, s-a decis verificarea modalității de respectare în practică a drepturilor persoanelor vizate. Astfel, a fost elaborat un al treilea chestionar privind drepturile persoanelor vizate, întrucât garantarea drepturilor persoanelor vizate reprezintă un aspect important al legislației privind protecția datelor cu caracter personal. Aceste considerații sunt tot mai relevante într-un domeniu, cum este cel al solicitărilor de viză, unde respectarea cadrului legal este deosebit de importantă.

În ceea ce privește Sistemul de Informații Schengen generația a II-a, având în vedere programul de lucru stabilit la nivelul Grupului de coordonare comună SIS II, una dintre activități a fost aceea de elaborare a unui model comun de inspecție a alertelor. Acest model este destinat a servi ca instrument de asistență pentru autoritățile de protecția datelor în efectuarea inspecțiilor la Sistemul de Informații Schengen II. În plus, acesta prevede o abordare comună a verificărilor, permițând o mai bună analiză și comparare a rezultatelor.

În acest context, a fost înființat un subgrup format din reprezentanți ai autorităților pentru protecția datelor din Belgia, Franța, Lituania, Malta și România, al cărui mandat a fost acela de a elabora o serie de întrebări și de a oferi consultanță pentru verificarea alertelor SIS II, considerate a fi esențiale din punctul de vedere al protecției datelor cu caracter personal și al cerințelor cadrului legal, astfel încât să se asigure o verificare adecvată a respectării prevederilor legale.

Un alt subgrup format din reprezentanți ai autorităților pentru protecția datelor din Germania, Italia și România a primit mandatul de a elabora o poziție comună cu privire la ștergerea alertelor privind vehiculele căutate pentru sechestru sau pentru folosirea ca probe în instanță, precum și cu privire la interpretarea art. 38 din Decizia Consiliului 2007/533/JAI.

Nevoia unei supravegheri amănunțite a protecției datelor cu caracter personal în cadrul Eurodac este evidentă atunci când avem în vedere categoriile de persoane afectate de sistemul

Eurodac, respectiv solicitanții de azil și (într-o măsură mai mică) imigranții neregulați. Această necesitate este, de asemenea, întărită de evoluția politicilor în zona de libertate, securitate și justiție din ultimii ani.

Protecția datelor personale reprezintă un factor cheie pentru succesul funcționării sistemului Eurodac și, în consecință, pentru funcționarea corespunzătoare a sistemului Dublin. Elemente precum securitatea datelor, calitatea datelor și legalitatea consultării datelor din Eurodac contribuie la buna funcționare a sistemului.

Reforma Eurodac a devenit aplicabilă la data de 20 iulie 2015. Există mai multe aspecte ce au devenit proeminente potrivit noilor norme Eurodac, dar schimbările cele mai relevante în ceea ce privește protecția datelor se referă la accesul autorităților din sectorul polițienesc (inclusiv Europol) la datele Eurodac.

În vederea pregătirii etapei pentru noile reguli Eurodac, Grupul de coordonare comună a decis efectuarea unui exercițiu, și anume completarea unui chestionar ce a avut drept scop verificarea modalității în care autoritățile naționale responsabile pe Eurodac au implementat reforma Eurodac, dar și verificarea posibilelor probleme referitoare la accesul la date în scop de aplicare a legii, a modalității de exercitare a drepturilor conferite persoanelor vizate.

❖ Grupul Internațional de Lucru pentru Protecția Datelor în domeniul Telecomunicațiilor

Grupul Internațional de lucru pentru Protecția Datelor în domeniul Telecomunicațiilor, cunoscut sub denumirea de „Grupul de la Berlin” a fost înființat în anul 1983 în cadrul Conferinței Internaționale a comisarilor pentru protecția datelor, la inițiativa comisarului pentru protecția datelor din Berlin. Activitatea acestui grup de lucru se concentrează în principal pe problema protecției vieții private în domeniul telecomunicațiilor și al serviciilor de Internet.

În cadrul reuniunilor sunt elaborate și ulterior adoptate documente de lucru în domeniul telecomunicațiilor, acestea fiind completate cu o serie de rezoluții adoptate în cadrul Conferinței internaționale a comisarilor pentru protecția datelor.

Astfel, cele mai recente documente de lucru adoptate în cadrul Grupului de la Berlin se referă la:

➤ *urmărirea localizării prin dispozitive mobile de comunicații* – acest document analizează în mod special riscurile aduse atât protecției datelor personale, cât și vieții private,

asociate cu colectarea de informații legate de dispozitive și informații care derivă din datele de localizare a comunicațiilor;

➤ *tehnologiile inteligente de analiză video* – sunt evaluate implicațiile de confidențialitate ale tehnologiilor inteligente de analiză video care sunt tot mai des utilizate pentru a detecta și a urmări persoanele fizice, cu scopul de a oferi publicitate personalizată, securitate sporită, precum și soluții de management al clienților. Aceste tehnologii permit unei game largi de entități, inclusiv muzee, aeroporturi și agenții de publicitate să stabilească mai bine tipurile de persoane cărora doresc să li se adreseze, să își adapteze mai bine serviciile și să comunice într-o manieră eficientă cu clienții;

➤ *protecția vieții private și riscurile la adresa securității prin raportare la utilizarea propriilor dispozitive în cadrul rețelelor corporative.*

❖ **Seminarul european pentru schimbul de experiență în rezolvarea cazurilor practice (Case Handling Workshop)**

Seminarul pentru schimbul de experiență (Case Handling Workshop) se organizează de autoritățile pentru protecția datelor pentru a veni în sprijinul acestora în activitatea practică. În cadrul reuniunilor se realizează un schimb de informații privind aspectele practice de la nivel operațional.

În 2015, seminarul pentru schimbul de experiență a fost organizat de autoritatea pentru protecția datelor din Albania și a abordat teme precum: protecția datelor personale în sectorul financiar și public, schimbul de informații între autoritățile pentru protecția datelor cu privire la cazurile transfrontaliere: metodele și implicațiile legislației naționale, nevoia de noi servicii și tehnologii, marketing direct și Internet.

❖ **Grupul de Lucru pentru protecția datelor în cadrul Convenției pentru stabilirea Centrului Sud-Est European de aplicare a legii (PCC SEE)**

În 2015 a avut loc prima reuniune a Grupului de Lucru pe protecția datelor în cadrul Convenției pentru stabilirea Centrului Sud-Est European de aplicare a legii (PCC SEE).

Una din atribuțiile Grupului de Lucru pe protecția datelor în cadrul PCC SEE este de a monitoriza aderarea la prevederile PCC SEE. Implementarea uniformă a acestora în ceea ce privește protecția datelor cu caracter personal necesită o abordare comună a autorităților pentru protecția datelor în exercitarea competențelor lor legate de activitatea de supraveghere.

Astfel, domeniul protecției datelor cu caracter personal continuă să aibă o importanță crucială pentru continuarea progreselor în conformitate cu standardele europene în cadrul cooperării în cadrul PCC SEE, având în vedere faptul că prevederile Convenției se referă în special la schimbul de informații.

❖ **Misiuni de evaluare Schengen**

În anul 2015, Autoritatea națională de supraveghere a participat la misiunea de evaluare Schengen în domeniul protecției datelor a Austriei și la misiunea de evaluare Schengen în domeniul protecției datelor a Regatului Țărilor de Jos.

În cadrul misiunilor Schengen a fost evaluat stadiul de implementare a cerințelor pe protecția datelor în spațiul Schengen, urmărindu-se, în același timp, asigurarea faptului că statele membre aplică regulile Schengen în mod eficient, în conformitate cu principiile și normele fundamentale.

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

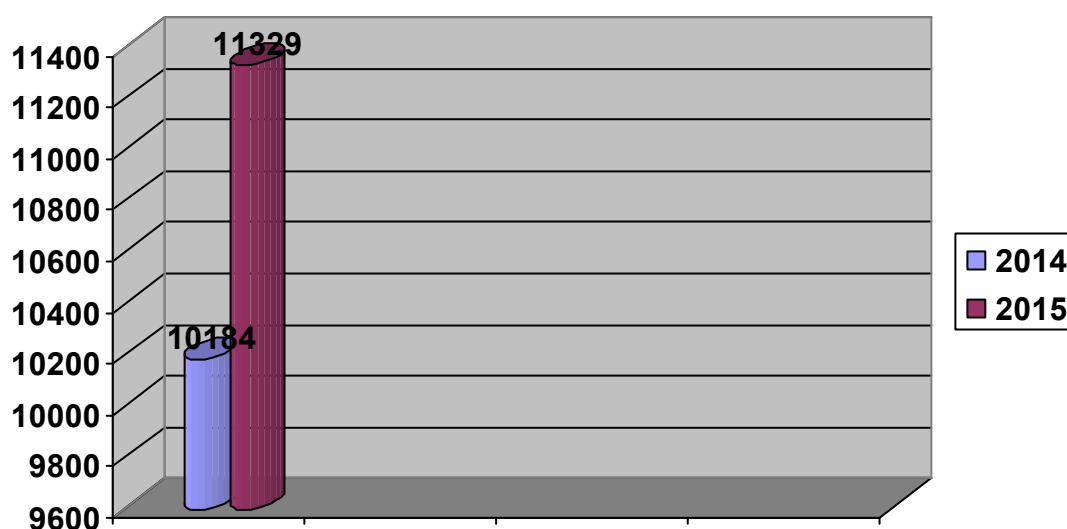
În 2015 a avut loc vizita de studiu a unei delegații din Georgia formată din reprezentanți ai autorităților naționale cu atribuții în domeniul protecției datelor cu caracter personal, precum și din reprezentanți ai organizațiilor societății civile cu activități în acest domeniu. Vizita de studiu a fost organizată ca parte a proiectului „Sprijinirea procesului de liberalizare a vizelor în Georgia prin acordarea de asistență în domeniul protecției datelor cu caracter personal și anti-discriminării”.

Proiectul derulat la inițiativa Centrului Român de Politici Europene, în parteneriat cu Open Society Georgia, a fost susținut de Ministerul Afacerilor Externe din România, în cadrul Politicii sale de Asistență Oficială pentru Dezvoltare, și a avut drept scop 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, componente importante ale Planului de acțiune pentru liberalizarea vizelor din cadrul dialogului U.E. – Georgia.

CAPITOLUL VI

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRIILOR
DE DATE CU CARACTER PERSONAL

În anul 2015, Autoritatea națională de supraveghere a soluționat **11.329** de solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări și cereri prin care a fost solicitat punctul de vedere al autorității sau clarificarea unor aspecte privind prelucrările de date cu caracter personal efectuate. Față de anul anterior, numărul solicitărilor a fost mai mare și cu un grad de complexitate crescut. Astfel, comparativ cu anul 2014, numărul de solicitări înregistrate în anul 2015 a crescut cu aproximativ 15%.



Au fost soluționate 10.819 notificări privind prelucrări de date cu caracter personal, dintre care 9803 efectuate pe teritoriul României și 1.016 transferuri de date către state din Uniunea Europeană, Zona Economică Europeană și state terțe.

Din cele 1.016 notificări cu transferuri de date către entități din străinătate, în 893 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, precum și transferuri către state terțe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată și completată.

Totodată, au fost notificate 110 transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, în baza contractelor cu clauze standard și 13 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 12 autorizații de transfer.

În același timp, au fost analizate 510 solicitări ale operatorilor privind aspecte referitoare la dispozițiile Legii nr. 677/2001, modificată și completată, rapoarte anuale ale autorităților publice și au fost emise 302 puncte de vedere.

Secțiunea 1 – Activitatea de înregistrare a prelucrărilor de date

Referitor la prelucrările de date notificate de operatori în anul 2015, s-a constatat o creștere a numărului operatorilor care desfășoară activități în domeniile organizării cursurilor de formare profesională, selecției și plasării forței de muncă, comerțului on-line, pregătirii în vederea obținerii permisului auto și a montării, reparării și verificării tahografelor digitale.

De asemenea, ca și în anul precedent, numeroși operatori au notificat Autoritatea națională de supraveghere pentru prelucrările efectuate în scopul monitorizării/securității persoanelor, spațiilor și/sau bunurilor publice/private. Dintre aceștia, menționăm asociațiile de proprietari care au declarat instalarea echipamentelor de supraveghere video pe căile de acces în imobile, precum și unitățile de învățământ care au notificat utilizarea sistemelor de supraveghere video a sălilor de clasă în care se desfășoară probele examenului de bacalaureat.

Totodată, din analizarea formularelor de notificare se evidențiază cele referitoare la monitorizarea propriilor angajați efectuată, în general, de entități din mediul privat, prin diverse mijloace de supraveghere. În acest sens, sunt de menționat prelucrările datelor (imaginilor) angajaților prin intermediul mijloacelor de supraveghere video, al sistemelor de comunicare puse la dispoziție de către angajator, precum și prelucrările amprentelor digitale ale angajaților pentru a realiza un sistem de pontaj.

În ceea ce privește supravegherea video a angajaților, Autoritatea națională de supraveghere a atras atenția că prevederile art. 8 alin. (1) din Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, emisă de președintele autorității, stabilesc regula potrivit căreia, în situația în care prelucrarea datelor cu caracter personal prin mijloace de supraveghere video vizează angajații, aceasta este

permisă pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

Dispozițiile art. 8 alin. (3) din același act normativ menționează faptul că prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video nu este permisă în interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă, cu excepția situațiilor prevăzute expres de lege sau a avizului instituției noastre.

În contextul necesității asigurării unei protecții eficiente a dreptului la viață intimă, familială și privată, raportat la principiul proporționalității prelucrărilor, Autoritatea națională de supraveghere a considerat, în mod constant, că prelucrarea datelor biometrice în scop de control acces persoane și/sau pontaj este excesivă.

De asemenea, un mare număr de prelucrări de date declarate Autorității naționale de supraveghere au avut ca obiect derularea unor proiecte finanțate din fonduri europene nerambursabile, precum și proiecte finanțate de Regatul Norvegiei prin mecanismul financiar norvegian.

Autoritatea națională de supraveghere a îndrumat, în continuare, 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 consimțământul 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, modificată și completată, și la modalitatea concretă prin care acestea pot fi exercitate (care trebuie să fie adecvată mijloacelor de prelucrare a datelor).

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, dintre care precizăm:

- verificarea condițiilor în care se efectuează prelucrarea datelor cu caracter personal ale minorilor;
- verificarea condițiilor în care se efectuează prelucrarea datelor angajaților prin mijloace de supraveghere video;

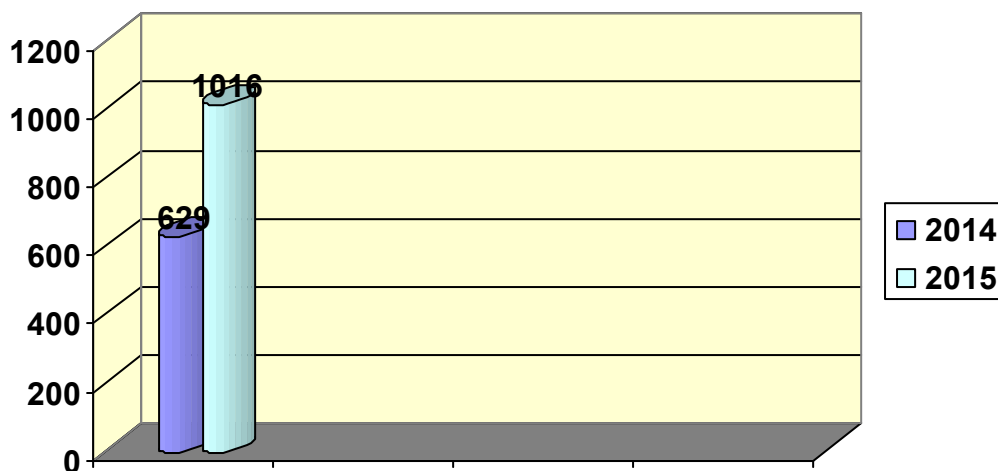
- verificarea modalității de obținere a consimțământului expres și neechivoc al persoanelor vizate cu privire la prelucrarea și transferul în străinătate al datelor cu caracter personal, îndeosebi al datelor cu caracter special;
- clarificarea condițiilor în care se efectuează prelucrarea având ca scop monitorizarea utilizării adecvate a tehnologiei informației și comunicațiilor și transferul datelor în străinătate;
- verificarea modalității de prelucrare a codului numeric personal în activități de reclamă, marketing și publicitate;
- clarificarea condițiilor în care se realizează prelucrarea datelor biometrice ale angajaților;
- verificarea condițiilor în care se prelucrează datele cu caracter personal ale angajaților prin intermediul mijloacelor de supraveghere video.

Un aspect deosebit de important cu privire la activitatea de prelucrare a datelor cu caracter personal este faptul că Autoritatea națională de supraveghere a continuat, și în anul 2015, îmbunătățirea cadrului de reglementare în acest domeniu de activitate, prin emiterea Deciziei nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum și pentru modificarea și abrogarea unor decizii, care a intrat în vigoare la data de 28 decembrie 2015.

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

Din cele **1016** notificări cu transferuri de date către entități din străinătate, în **893** 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 la principiile Safe Harbor), precum și transferuri către state terțe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată și completată.

Au fost, de asemenea, notificate **110** 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 **13** transferuri în baza regulilor corporatiste obligatorii (Binding Corporate Rules). Se constată și sub acest aspect, comparativ cu anul anterior, o creștere a notificărilor cu transferuri de date către entități din străinătate.



În ceea ce privește transferurile de date efectuate în baza principiilor Safe Harbor, precizăm că, în data de 6 octombrie 2015, Curtea de Justiție a Uniunii Europene a declarat nevalidă Decizia 2000/520/CE a Comisiei Europene, adoptată în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului. Această decizie reglementa transferul de date cu caracter personal din state membre ale Uniunii Europene către entități din Statele Unite ale Americii, ca urmare a adeziunii acelor entități la principiile Safe Harbor.

În consecință, după această dată, Autoritatea națională de supraveghere nu a mai înscris în registrul de evidență a prelucrărilor de date cu caracter personal prelucrările/transferul datelor către entități din Statele Unite ale Americii în baza acestor principii. Totodată, Autoritatea națională de supraveghere a recomandat operatorilor să efectueze transferuri în Statele Unite ale Americii în baza celorlalte garanții prevăzute de art. 29 alin. (4), respectiv clauze contractuale standard și reguli corporatiste obligatorii – BCR.

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 de părțile între care are loc transferul de date, în baza prevederilor Deciziilor privind clauzele contractuale tip pentru transferul de date cu caracter personal către operatorii sau persoanele împuternicite de către operator, stabilite în țări terțe, în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului, acestea au vizat activități din următoarele domenii:

- managementul conferințelor și remunerarea specialiștilor în baza angajamentelor încheiate cu aceștia;

- resurse umane, respectiv realizarea de verificări cu privire la istoricul candidaților pentru locuri de muncă vacante; administrarea personalului; conturi și evidențe; educație (traininguri);
- gestiune economico-financiară și administrativă;
- servicii de asigurări și reasigurări;
- asigurare suport IT externalizat în caz de incidente;
- emiterea/folosirea tichetelor de masă sau a voucherelor de vacanță pe suport electronic și a altor tipuri de tichete pe suport electronic;
- activități de cooperare și comunicare între angajații operatorului;
- servicii de suport comercial;
- realizarea de studii clinice și cercetare medicală.

Transferurile de date în străinătate efectuate în baza normelor corporatiste obligatorii (binding corporate rules) au vizat activități din următoarele domenii:

- resurse umane, respectiv recrutare, administrarea salariilor și plata cheltuielilor;
- gestionarea relației cu clienții, menținerea și îmbunătățirea relației cu aceștia;
- gestionare și raportare financiară, administrare fiscală, înregistrare și raportare de reglementare legală și alte raportări de conformitate;
- analiză de afaceri și dezvoltarea afacerilor;
- activități de contabilitate, revizie contabilă, consultanță fiscală în domeniul fiscal, servicii de salarizare;
- soluționarea sesizărilor formulate de orice persoană interesată cu privire la fapte de încălcare a legii, infracțiuni de corupție, abateri disciplinare, contravenții, asigurarea conformității respectării legilor în vigoare.

În urma analizării transferurilor de date în străinătate către state terțe, a fost emis un număr de **12** autorizații de transfer.

Este de menționat faptul că, potrivit art. 2 alin. (1) din Decizia nr. 200/2015, nu mai este necesară notificarea transferului de date cu caracter personal către state din Uniunea Europeană, Zona Economică Europeană, precum și către state cărora Comisia Europeană le-a recunoscut, prin decizie, un nivel de protecție adecvat.

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

În anul 2015, 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 supuse analizei Autorității naționale de supraveghere.

✓ O autoritate publică a solicitat punctul de vedere cu privire la necesitatea notificării în cazul monitorizării accesului persoanelor prin camere video, raportat la prevederile art. 1 lit. e) din Decizia nr. 23/2012 (notificarea 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).

În contextul solicitării formulate, s-a apreciat că prelucrările de date prin sistemul de supraveghere video nu se încadrează în situațiile de excepție de la obligația de notificare stabilite de dispozițiile art. 22 alin. (2) din Legea nr. 677/2001, modificată și completată, și de cele ale Deciziilor nr. 90/2006, nr. 100/2007 și nr. 23/2012 ale președintelui Autorității naționale de supraveghere.

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

În consecință, s-a apreciat că este necesară depunerea notificării pentru prelucrarea efectuată în scopul monitorizării accesului persoanelor în sediul autorității respective.

✓ O societate comercială furnizoare de servicii IT&C a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la obligația de a notifica activitățile desfășurate ca parte a unui proiect co-finanțat de Comisia Europeană. Proiectul presupune cercetarea, testarea și validarea unor noi soluții tehnologice astfel încât acestea să fie cât mai eficiente și performante. Coordonatorul acestui proiect este un operator din Marea Britanie, societatea din România contribuind doar la activitățile de cercetare desfășurate în cadrul proiectului.

S-a precizat că, potrivit dispozițiilor art. 3 lit. e) din Legea nr. 677/2001, modificată și completată, 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; persoană împuternicită de către operator este o persoană fizică sau juridică, de drept privat ori de drept public (...) care prelucrează date cu caracter personal pe seama operatorului. Reprezentant al operatorului este o persoană juridică sau fizică care are sediul sau domiciliul/reședința stabilite pe teritoriul statului român sau o altă entitate fără personalitate juridică, desemnată de operator pentru prelucrarea datelor în România.

Având în vedere informațiile furnizate, Autoritatea națională de supraveghere a apreciat că societatea are calitatea de împuternicit și nu este necesar să notifice prelucrarea efectuată.

De asemenea, s-a menționat că operatorul cu sediul în Marea Britanie trebuie să se asigure că împuternicitul din România ia toate măsurile necesare, astfel încât operațiunile de prelucrare a datelor cu caracter personal efectuate pe teritoriul României să respecte dispozițiile Legii nr. 677/2001 aplicabile împuternicitului, în special cele privind măsurile necesare pentru asigurarea confidențialității și securității acestora.

✓ O societate de avocatură a solicitat punctul de vedere al autorității în ceea ce privește transferul datelor cu caracter personal, prin utilizarea serviciilor de cloud computing, în Statele Unite ale Americii în baza principiilor Safe Harbor.

Față de informațiile transmise, Autoritatea națională de supraveghere a arătat că operatorului din România, ce utilizează tehnologia tip cloud, îi revine obligația de a notifica Autorității naționale de supraveghere prelucrarea efectuată, precum și transferul în străinătate, în vederea înscrierii acesteia în Registrul de evidență a prelucrărilor de date cu caracter personal.

De asemenea, s-a subliniat necesitatea identificării unor condiții care să permită transferul datelor cu caracter personal în Statele Unite ale Americii, întrucât prin decizia Curții Europene de Justiție din data de 06.10.2015 s-a declarat nevalidă decizia Comisiei Europene din 26 iulie 2000 prin care se constata că Statele Unite asigură un nivel adecvat de protecție a datelor cu caracter personal transferate (Safe Harbor).

Totodată, s-a prezentat modalitatea de obținere a înregistrării în Registrul electronic de evidență a prelucrărilor de date cu caracter personal.

✓ O societate care oferă clienților săi persoane juridice, din mediul public sau privat, un serviciu on-line, pentru a urmări situația contractelor avute în desfășurare, a solicitat punctul de vedere al instituției noastre în ceea ce privește necesitatea notificării acestei prelucrări. Datele vor fi introduse în aplicație de clienți, fiecare utilizator având acces la datele

clienților proprii. De asemenea, aplicația generează automat facturi pentru plata serviciilor proprii.

Raportat la aceste aspecte, Autoritatea națională de supraveghere a precizat că, în măsura în care scopul și mijloacele prelucrării au fost stabilite de către clienți, iar furnizorul aplicației prelucrează date personale pe seama acestora, acesta îndeplinește calitatea de persoană împuternicită.

În schimb, dacă furnizorul asigură numai anumite servicii și prin aceasta i se dezvăluie o serie de date și categorii de date, potrivit definiției date de art. 3 lit. h) și g) din Legea nr. 677/2001, modificată și completată, va avea calitatea de destinatar sau terț, fără obligația de a notifica.

✓ Entități care desfășoară activități în domeniul imobiliar, precum și entități care desfășoară o activitate independentă, autorizată în baza unei legi speciale, care prelucrează date în scopul îndeplinirii atribuțiilor lor legale (mediatori, avocați, medici) au solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la calitatea lor de operator și obligația de a notifica, prin completarea formularului on-line.

Aceste entități au fost informate că au calitatea de operator și, implicit, obligația de a respecta legislația din domeniul protecției datelor, în special condițiile reglementate de art. 12, 19 și 20 din Legea nr. 677/2001, modificată și completată, fiind scutite de obligația de a completa formularul de notificare, prin modalitatea on-line, potrivit Deciziei Președintelui Autorității Naționale de supraveghere a Prelucrării Datelor cu Caracter personal nr. 23/2012, în vigoare la momentul formulării răspunsului.

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, în anul 2015, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal i s-a alocat prin Legea bugetului de stat nr. 186/2014, un buget în sumă de 2.994.000 lei, cu următoarea structură:

- mii lei -

Denumire indicator	Cod	Buget inițial 2015	Buget actualizat la 31.12.2015	Sume cheltuite până la 31.12.2015	Execuție (%)
Total cheltuieli	51.01	2.994	2.949	2.868	97,25
Cheltuieli de personal	10	2.223	2.237	2.229	99,64
Bunuri și servicii	20	750	701	630	89,87
Cheltuieli de capital	71	21	11	9	81,81

Întrucât 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 obiectivelor propuse, ținând cont de solicitările permanente privind eficiența utilizării fondurilor publice.

În ceea ce privește modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorității naționale de supraveghere a constituit un procent de 76% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 2.229.370 lei (prin ocuparea temporară, prin detașare, a unor posturi), înregistrându-se în continuare un deficit major de personal (9 posturi neocupate, 5 posturi ocupate temporar prin detașare, reprezentând 28% din numărul total de 50 de posturi –

exclusiv demnitarii - prevăzute de Legea nr. 102/2005). Majoritatea cheltuielilor de personal au fost aferente plăților făcute pentru munca salariată a angajaților din compartimentele de specialitate.

Cheltuielile ocazionate de deplasări au reprezentat, în anul 2015, 12,96 % din totalul cheltuielilor titlului Bunuri și servicii, datorită creșterii numărului de plângeri primite și a controalelor efectuate la operatori de date din teritoriu.

În anul 2015, cheltuielile cu bunuri și servicii au crescut cu 5,57% față de anul 2014, avându-se permanent în vedere mai mulți factori – oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice alături de unele cerințe tehnice atent stabilite.

Politicile contabile utilizate la întocmirea situațiilor financiare anuale sunt în conformitate cu reglementările legale 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 acestea în bugetul autorității.

Cheltuielile bugetare s-au efectuat 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*

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 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 efectueze 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 naționale 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.”

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.”