AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

R A P O R T A N U A L

2016

Raportul de activitate este prezentat Senatului României, în temeiul art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal

Bucureşti

CUVÂNT ÎNAINTE

Stimate Domnule Preşedinte al Senatului,

Stimaţi Senatori,

Anul 2016 marchează începutul unui proces amplu de reformă a domeniului protecției datelor personale la nivel național, ca efect direct al adoptării, pe data de 27 aprilie 2016, de către Parlamentul European și Consiliul, a Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor), precum și a Directivei privind protecţia persoanelor fizice faţă de prelucrările efectuate de către autorităţile competente în scopul prevenirii, cercetării, constatării sau urmăririi penale a infracţiunilor ori executării pedepselor penale şi libera circulaţie a acestor date.

Aplicabilitatea directă a Regulamentului General privind Protecția Datelor începând cu data de 25 mai 2018, va avea ca efect uniformizarea principiilor de protecție a datelor personale în toate statele membre ale Uniunii Europene, prin înlocuirea reglementărilor naționale existente în prezent.

În ceea ce priveşte această nouă reglementare europeană, remarcăm o consolidare a drepturilor persoanelor fizice fie prin dezvoltarea celor existente, fie prin statuarea unor noi drepturi, cum sunt dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării. În mod corelativ, s-a pus un accent deosebit pe responsabilitatea operatorilor în legătură cu prelucrările efectuate.

Un alt element de noutate din Regulament, pe care aş dori să-l supun atenţiei dumneavoastră, este cel al obligației instituţiilor publice şi, în anumite situații, entităţilor private, de a-şi desemna o persoană responsabilă cu protecţia datelor la nivel intern, în funcţie de anumite criterii. Subliniem că aceasta va implica o schimbare semnificativă în activitatea operatorilor din România, destinată să responsabilizeze operatorii, și sperăm că va avea efecte benefice în ceea ce priveşte respectarea drepturilor persoanelor fizice.

În condițiile în care Regulamentul General privind Protecția Datelor conține unele dispoziții care oferă posibilitatea statelor membre de a interveni adiacent cu anumite reglementări naționale, s-au demarat, în cursul anului 2016, consultări cu ministerele responsabile pentru analizarea și pregătirea cadrului național legislativ adecvat.

Întrucât Regulamentul General privind Protecția Datelor prevede o extindere a competențelor și sarcinilor autorităților naționale de supraveghere, apare necesitatea anumitor modificări legislative naționale prin care să se consolideze capacitatea instituţională şi administrativă a Autorităţii naționale de supraveghere, inclusiv prin alocarea și asigurarea unor resurse umane, materiale și financiare corespunzătoare.

Întrucât următorul an va avea un impact major în asigurarea unei aplicări corespunzătoare a acestor noi reglementări, ne propunem ca acţiunile Autorităţii să fie subsumate următoarelor obiective principale:

- implicarea activă în vederea pregătirii cadrului normativ național în concordanță cu noile reglementări ale Uniunii Europene, alături de instituțiile responsabile;
- creşterea gradului de informare a operatorilor și cetăţenilor cu privire la aplicarea noilor reguli, cu sprijinul reprezentanţilor mass-media și al societății civile.

În acest context, consolidarea capacităţii administrative a Autorităţii de îndeplinire a noilor competențe stabilite la nivel adecvat reprezintă o prioritate și implică alocarea de resurse materiale, financiare şi umane, în vederea asigurării unei reale respectări a dreptului la viață privată și la protecția datelor cu caracter personal, la standarde europene.

În final, permiteți-mi să îmi exprim speranța că Autoritatea va beneficia și pe viitor de întregul dumneavoastră sprijin în acest moment deosebit de important al reformei în domeniul protecției datelor cu caracter personal.

Ancuţa Gianina OPRE,

Preşedinte

CUPRINS

CAPITOLUL I

PREZENTARE GENERALĂ

Raportul de activitate pe anul 2016 al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe şapte capitole, după cum urmează:

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

În cuprinsul **Capitolului al II-lea** sunt prezentate aspecte relevante referitoare la pachetul legislativ de reformă în domeniul protecţiei datelor cu caracter personal, adoptat pe data de 27 aprilie 2016 la nivelul Uniunii Europene, în special cu privire la aplicabilitatea Regulamentului General privind Protecția Datelor în toate statele membre începând cu data de 25 mai 2018.

Capitolul al III-lea cuprinde informații relevante referitoare la activitatea de avizare a proiectelor de acte normative şi la aceea de consultare referitoare la aplicarea regulilor de protecţie a datelor personale, inclusiv de clarificare a unor chestiuni semnalate de diverşi operatori. Aceasta s-a concretizat în emiterea avizelor asupra unui număr aproape dublu de proiecte de acte normative şi a unui număr semnificativ de puncte de vedere.

Persoanele fizice şi operatorii de date au solicitat, în principal, informaţii privind condiţiile prelucrării datelor personale, inclusiv a celor cu caracter special, precum și referitoare la legalitatea dezvăluirii unor date.

În secţiunea privind reprezentarea în faţa instanţelor de judecată, sunt prezentate cele mai semnificative litigii finalizate, în care a fost parte Autoritatea naţională de supraveghere, cu evidenţierea soluţiilor pronunţate.

Secţiunea privind informarea publică conturează principalele modalităţi de popularizare a domeniului protecţiei datelor cu caracter personal, utilizate în cursul anului 2016, în limitele resurselor bugetare alocate.

Capitolul al IV-lea constă într-o prezentare a activităţii de control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite, ce implică verificarea modului de aplicare a dispoziţiilor legale în materie. În condițiile intensificării investigaţiilor efectuate în cursul anului 2016, au fost aplicate amenzi în cuatum total de peste 1 milion de lei.

Investigaţiile efectuate din oficiu au vizat verificarea respectării de către operatorii din anumite domenii de activitate a dispoziţiilor Legii nr. 677/2001, precum şi a celorlalte acte normative care privesc domeniul datelor cu caracter personal.

În unele cazuri s-a dispus încetarea prelucrării sau ştergerea datelor, prin decizia preşedintelui Autorităţii naţionale de supraveghere.

Capitolul al V-lea prezintă activitatea de relaţii externe a Autorităţii naţionale de supraveghere.

Capitolul al VI-lea privind activitatea de supraveghere a prelucrărilor de date cu caracter personal cuprinde principalele concluziile rezultate din analizarea formularelor transmise de operatorii de date, persoane fizice şi juridice, care au avut obligaţia depunerii acestora. Au fost înregistrate un număr total de 6930 de notificări privind prelucrări de date, în condițiile în care sarcinile administrative ale operatorilor au fost reduse prin aplicarea Deciziei nr. 200/2015 a Autorității naționale de supraveghere.

Capitolul al VII-lea referitor la resursele materiale şi financiare conţine informaţii privind creditele bugetare puse la dispoziţia Autorităţii naţionale de supraveghere şi sumele cheltuite pe fiecare articol al clasificaţiei bugetare.

CAPITOLUL II
NOI ACTE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secţiunea 1: **Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC, precum și Directiva (UE) 2016/680 privind protecţia datelor prelucrate în scopul prevenirii, detectării, investigării şi punerii sub urmărire a infracţiunilor şi a altor activităţi judiciare**

Pachetul legislativ adoptat pe data de 27 aprilie 2016 cuprinde două acte normative:

- Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC;
- Directiva (UE) 2016/680 privind protecţia datelor prelucrate în scopul prevenirii, detectării, investigării şi punerii sub urmărire a infracţiunilor şi a altor activităţi judiciare

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

Adoptarea Regulamentului General privind Protecția Datelor constituie un moment crucial în domeniul protecției datelor personale, cu efecte directe asupra activității operatorilor, în condițiile în care se realizează o consolidare a drepturilor specifice ale persoanelor fizice.

Astfel, se remarcă o consolidare a dreptului la ștergerea datelor, prin consacrarea expresă a „dreptului de a fi uitat”, iar pe de altă parte se stabilește dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării, de natură să ofere cetățenilor un control mai eficient asupra datelor lor personale.

Un element de noutate din proiectul de Regulament constă în obligativitatea instituţiilor publice şi entităţilor private de a-şi desemna o persoană responsabilă cu protecţia datelor la nivel intern, în funcţie de anumite criterii.

Aceasta va implica o schimbare semnificativă în activitatea operatorilor din România, deoarece va presupune desfiinţarea actualelor notificări ale prelucrărilor de date declarate la Autoritatea naţională de supraveghere.

În același timp, s-a realizat o reglementare mai detaliată a obligaţiilor operatorilor, un accent deosebit fiind pus pe creşterea gradului de responsabilizare a acestora.

Consacrarea expresă a principiilor de prelucrare privacy by design și privacy by default reprezintă un alt element de noutate a acestei reglementări, implicând asigurarea protecției datelor din momentul inițial al stabilirii mijloacelor de prelucrare.

În același timp, subliniem că Regulamentul conține anumite dispoziții care oferă posibilitatea statelor membre de a interveni cu anumite reglementări naționale.

În același timp, se stabilește și un mecanism nou de cooperare între autoritățile pentru protecția datelor care va implica un organism european cu personalitate juridică – Comitetul European pentru Protecția Datelor (European Data Protection Board - EDPB). Acesta va răspunde de medierea dezacordurilor dintre autoritățile pentru protecția datelor, precum și de elaborarea unor ghiduri și recomandări destinate unei aplicări unitare a acestei noi reglementări în spațiul Uniunii Europene.

În același timp, se prevede o extindere a competențelor și sarcinilor autorităților naționale de supraveghere și, pe cale de consecință, apare necesitatea anumitor modificări legislative naționale prin care să se consolideze capacitatea instituţională şi administrativă a Autorităţii naționale de supraveghere, inclusiv prin alocarea și asigurarea unor resurse umane, materiale și financiare corespunzătoare.

Prevederile Regulamentului general privind protecția datelor vor fi aplicabile începând cu data de 25 mai 2018.

CAPITOLUL III
ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

Secţiunea 1 Avizarea actelor normative

Autoritatea naţională de supraveghere a emis, în temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, avize asupra unui număr de 56 de proiecte de acte normative elaborate de instituţii şi autorităţi publice, care implicau diverse aspecte privind prelucrarea datelor cu caracter personal.

În condițiile creșterii numărului de acte normative transmise în vederea avizării, în cele mai multe dintre situații s-a apreciat că este necesară completarea textelor respective, s-au efectuat observații și propuneri, prin raportare la necesitatea respectării principiilor și condițiilor de prelucrare a datelor cu caracter personal.

Asupra majorității proiectelor de acte normative analizate s-au efectuat recomandări pentru reanalizarea acestora și armonizarea lor cu dispozițiile legale privind protecția datelor.

În continuare prezentăm, pentru exemplificare, unele dintre cele mai relevante proiecte de acte normative avizate:

- **Autoritatea Națională pentru Protecția Consumatorilor a transmis spre avizare proiectul de "Ordonanță privind contractele de credit oferite consumatorilor pentru bunuri imobile"**

Au fost efectuate următoarele observații și propuneri:

Referitor la prevederile art. 9 alin. (2) lit. a) din Capitolul III, coroborate cu cele din Capitolul XIII "Evaluarea bonității" din proiect, s-a subliniat că, în contextul prelucrării datelor cu caracter personal, operatorilor de date cu caracter personal le revine obligația de informare a persoanelor vizate, potrivit dispozițiilor art. 12 alin. (1) din Legea nr. 677/2001 coroborate cu prevederile Deciziei nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit.

Raportat la art. 21 alin. (1) din proiect s-a considerat că este necesară corelarea dispozițiilor acestuia cu cele din Legea nr. 677/2001, potrivit cărora la exercitarea dreptului de acces la date, a dreptului de intervenție și a celui de opoziție, operatorii de date au obligația de

a răspunde persoanelor vizate în termen de 15 zile de la data primirii unei cereri din partea acestora.

De asemenea, s-a apreciat ca fiind oportună reanalizarea prevederii art. 27 alin. (1) lit. o) din proiect cu privire la informarea consumatorilor privind efectele specifice pe care produsele propuse le pot avea asupra acestora, inclusiv consecinţele în eventualitatea neplăţii de către consumator, cu luarea în considerare a prevederilor art. 12 din Legea nr. 677/2001, coroborate cu prevederile Deciziei nr. 105/2007, precum și cu prevederile legale referitoare la Centrala Riscului de Credit.

Referitor la Capitolul XII din proiect, ”evaluarea bonității consumatorilor”, s-a atras atenția că prevederile nu transpun corespunzător art. 18 alin. (5) lit. c) din Directiva 2014/17/UE și, ca atare, s-a considerat că este necesară reformularea acestuia.

Cât privește conținutul art. 73 alin. (1) din proiect, s-a apreciat ca fiind necesară completarea acestuia, raportat la dispozițiile art. 4 alin. (1) lit. e) din Legea nr. 677/2001, care prevăd că datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate.

Referitor la art. 74 alin. (1) din proiect s-a atras atenția că ”nivelul veniturilor și cheltuielilor consumatorilor” și ”informații financiare și economice” ale solicitanților de credit sunt date cu caracter personal, a căror prelucrare se supune condițiilor stabilite de Legea nr. 677/2001.

Raportat la dispozițiile art. 74 alin. (3) din proiect referitoare la ”obținerea” de către creditori a informațiilor anterior menționate și din ”surse interne sau externe relevante”, s-a considerat că este necesară completarea acestora în sensul includerii mențiunii că informațiile necesare evaluării bonității consumatorilor trebuie să fie necesare, suficiente și proporționale, în concordanță cu prevederile art. 20 alin. (1) din Directiva 2014/17/UE.

Raportat la conținutul art. 78 din proiect, s-a subliniat, cu referire la prelucrarea datelor cu caracter personal ale consumatorilor persoane fizice în scopul evaluării bonității acestora, că

respectarea Legii nr. 677/2001 implică, pe lângă luarea în consideraţie a principiilor de protecţie a datelor, respectarea tuturor drepturilor persoanelor vizate, stabilirea persoanelor, respectiv a entităților autorizate (raportat și la prevederile art. 79 din proiect) care vor avea acces la date în scopuri legitime, precum și asigurarea confidențialității și securității prelucrărilor de date cu caracter personal.

Având în vedere prevederile din proiect referitoare la ”accesul la bazele de date” s-a precizat, cu referire la comunicările electronice ale datelor între diverse entităţi la care face referire proiectul de act normativ, că o comunicare de acest tip se poate expune la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor. Or, la alegerea modalităţilor de transmitere a datelor sau a documentelor ce conţin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii au obligaţia de a aplica măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispoziţiile art. 17 alin. (1) din Directiva 95/46/CE a Parlamentului European şi prevederile art. 20 din Legea nr. 677/2001.

În contextul dispozițiilor art. 104 alin. (3) din proiect, s-a propus reformularea acestuia având în vedere faptul că, potrivit art. 20 alin. (5) din Legea nr. 677/2001, efectuarea prelucrărilor prin persoane împuternicite trebuie să se desfăşoare în baza unui contract încheiat în formă scrisă, care va cuprinde în mod imperativ obligaţia persoanei împuternicite de a acţiona doar în baza instrucţiunilor primite de la operator şi faptul că îndeplinirea obligaţiilor privind aplicarea de măsuri de securitate revine şi persoanei împuternicite.

În consecință, Autoritatea națională de supraveghere **a avizat cu observații** proiectul de ”Ordonanță privind contractele de credit oferite consumatorilor pentru bunuri imobile”.

- **Oficiul Național pentru Jocuri de Noroc a solicitat punctul de vedere cu privire la proiectul de Hotărâre pentru aprobarea Normelor metodologice de punere în aplicare a Ordonanţei de urgenţă nr. 77/2009 privind organizarea şi exploatarea jocurilor de noroc și pentru modificarea și completarea Hotărârii Guvernului nr. 298/2013 privind organizarea şi funcţionarea Oficiului Naţional pentru Jocuri de**

Noroc şi pentru modificarea Hotărârii Guvernului nr. 870/2009 pentru aprobarea Normelor metodologice de aplicare a Ordonanţei de urgenţă a Guvernului nr. 77/2009 cu modificările și completările ulterioare privind organizarea şi exploatarea jocurilor de noroc

Referitor la acest proiect de hotărâre, Autoritatea națională de supraveghere a formulat observaţii și propuneri, astfel:

Activităţile ce urmează a fi desfăşurate în cadrul sistemelor de evidență de către entitățile implicate în organizarea şi exploatarea jocurilor de noroc presupun efectuarea de prelucrări de date cu caracter personal ale persoanelor fizice (inclusiv date cu caracter special, precum codul numeric personal, seria și numărul cărții de identitate sau alte informații din documentele ce dovedesc identitatea persoanelor).

Ca atare, s-a apreciat că este necesară luarea în considerare a principiilor de protecţie a datelor statuate de art. 4 alin. (1) din Legea nr. 677/2001, încă de la crearea evidențelor în format automatizat, întrucât activitatea de organizare şi exploatare a jocurilor de noroc se desfășoară în cadrul unor sisteme informatice.

De asemenea, s-a considerat necesară acordarea unei atenții sporite stabilirii garanţiilor adecvate pentru respectarea drepturilor persoanelor vizate, precum și identificării responsabilităţilor și a modalităților de acces la date ale tuturor entităților implicate, raportat la competențele legale ale acestora, precum și clarificarea calităţii lor, respectiv de operatori sau împuterniciţi, în sensul definiţiilor date de Legea nr. 677/2001.

Astfel, s-a recomandat o enumerare completă a datelor colectate, pentru evitarea încălcării principiului statuat de art. 4 alin. (1) lit. c) din Legea nr. 677/2001.

S-a apreciat ca necesară stabilirea clară a datelor și a categoriilor de date colectate și prelucrate de către entitățile abilitate, pentru a conferi normei previzibilitate și predictibilitate.

Raportat la principiul statuat de art. 4 alin. (1) lit. e) din Legea nr. 677/2001, s-a considerat ca fiind necesară stabilirea unei perioade exacte de păstrare a datelor, în concordanță cu durata necesară realizării scopurilor.

Totodată, s-a apreciat ca necesară identificarea și precizarea expresă a calității de operator sau împuternicit, după caz, a fiecărei entități care colectează și prelucrează date cu caracter personal, și inserarea în textul proiectului de hotărâre a mențiunilor privind faptul că acestea au obligația să asigure respectarea dispozițiilor Legii nr. 677/2001 și ale Legii nr.

506/2004, cu precădere a drepturilor persoanelor vizate și a confidențialității și securității datelor.

În același timp, în ceea ce privește informarea persoanelor vizate, s-a subliniat faptul că această obligație le revine tuturor entităților implicate în activitatea de organizare şi exploatare a jocurilor de noroc.

Cu privire la obligațiile sus-menționate, s-a recomandat fie introducerea unui articol separat, fie efectuarea de mențiuni la articolele în cauză care vizează activitatea operatorilor economici de colectare și prelucrare a datelor.

Având în vederea aspectele de mai sus, **Autoritatea a apreciat că proiectul de hotărâre necesită reanalizare.**

- **Ministerul Muncii, Familiei, Protecției Sociale și Persoanelor Vârstnice a transmis spre avizare proiectul Legii privind venitul minim de incluziune**

În ceea ce priveşte proiectul supus analizei, Autoritatea națională de supraveghere a formulat următoarele observaţii și propuneri:

Referitor la art. 29 alin. (1) din proiect, precum și la celelalte articole care menționează modalitatea de comunicare electronică a cererilor privind acordarea venitului minim de incluziune, s-a atras atenția că acest sistem poate expune comunicarea la o serie de riscuri.

La art. 29 alin. (2) şi (4) din proiect, s-a remarcat faptul că aceste dispoziții nu realizează o enumerare completă a datelor și categoriilor de date solicitate, prin formularea sintagmei „în principal”, care denotă ambiguitate și poate conduce la colectarea în mod excesiv a datelor personale, încălcându-se astfel principiul statuat de art. 4 alin. (1) lit. c) din Legea nr. 677/2001, respectiv caracterul adecvat, pertinent și neexcesiv al datelor.

Prin urmare, pentru a conferi normei previzibilitate și predictibilitate, s-a recomandat stabilirea concretă a datelor și categoriilor de date care vor fi colectate și prelucrate de către entitățile abilitate.

Aceleași argumente au fost susținute și cu privire la sintagma ”date privind persoana îndreptățită”, care nu denotă cu claritate datele strict necesare îndeplinirii scopului (acordarea

venitului minim de incluziune) și care de asemenea poate conduce în practică la aplicarea neunitară a legii.

În acest context, întrucât la alin. (6) al art. 29 din propunerea legislativă se prevede faptul că vor fi elaborate norme metodologice pentru aplicarea legii, s-a recomandat a se avea în vedere, în aceste acte normative subsecvente, precizarea informațiilor privind modalitatea de colectare a datelor, respectarea principiilor stabilite de art. 4 din Legea nr. 677/2001 (caracterul adecvat al colectării datelor şi categoriilor de date, actualizarea datelor, termene de stocare, condiţii de ştergere a datelor), modalitatea de exercitare a drepturilor persoanelor vizate, în special a dreptului de acces, și că operatorul este obligat să aplice măsuri de confidenţialitate şi securitate a datelor.

Faţă de conţinutul art. 32 din propunerea legislativă, s-a atras atenția asupra faptului că activităţile ce urmează a fi desfăşurate în cadrul sistemelor de evidență de către entitățile implicate în activitatea de acordare a venitului minim presupun prelucrarea unui volum foarte mare de date cu caracter personal ale persoanelor fizice (inclusiv date cu caracter special, precum starea de sănătate, codul numeric personal, seria și numărul cărții de identitate etc.).

Astfel, implementarea, la nivel național, a unui sistem electronic de colectare şi prelucrare a datelor persoanelor care solicită venitul minim de incluziune este susceptibilă de a prezenta riscuri speciale pentru drepturile şi libertăţile acestei categorii de persoane. În consecință, asigurarea unei protecţii eficiente a datelor personale, în conformitate cu dispoziţiile Legii nr. 677/2001, modificată şi completată, este deosebit de importantă.

Ca atare, atunci când se propun şi se concep sisteme de evidenţă automatizate, aşa cum este şi cel la care se face referire în conţinutul propunerii legislative, este necesară luarea în considerare a principiilor de protecţie a datelor statuate de art. 4 alin. (1) din Legea nr. 677/2001, încă de la crearea evidențelor în format automatizat, respectiv Sistemul Național Informatic pentru Asistență Socială.

În acest context, s-a considerat necesară acordarea unei atenții sporite stabilirii garanţiilor adecvate pentru respectarea drepturilor persoanelor vizate, precum și identificării responsabilităţilor și a modalităților de acces la date pentru toate entitățile implicate raportat la

competențele legale ale acestora, precum și clarificarea calităţii lor, respectiv de operatori sau împuterniciţi, în sensul definiţiilor date de Legea nr. 677/2001.

De asemenea, la art. 32 din proiect s-a considerat utilă adăugarea unui nou alineat care să prevadă faptul că „Colectarea şi prelucrarea datelor necesare acordării venitului minim de incluziune se va face cu respectarea prevederilor Legii nr. 677/2001, cu precădere a drepturilor persoanelor vizate și a confidențialității și securității datelor."

La art. 37 s-a apreciat că este necesar fie să se introducă un nou alineat care să prevadă faptul că „Personalul autorităților administrației publice locale are obligația respectării confidenţialităţii şi securității informațiilor și a datelor cu caracter personal, în conformitate cu prevederile Legii nr. 677/2001".

Totodată, faţă de formularea art. 38 alin. (1) din proiect, referitor la accesarea "și a altor baze de date disponibile ale altor autorități publice cu care are încheiate protocoale de colaborare", aceasta nu denotă claritate, contravine principiului caracterului adecvat, pertinent și neexcesiv al datelor, fiind încălcate și principiile de previzibilitate și predictibilitate pe care trebuie să le respecte un act normativ.

Mai mult, protocoalele de colaborare sunt cunoscute doar de către entitățile semnatare și mai puțin de către persoana fizică în cauză, care, astfel, nu are cunoștință despre datele care o privesc și care sunt solicitate, precum și de autoritatea sau instituția furnizoare.

S-a precizat faptul că, în sensul celor de mai sus, și-a exprimat opinia și Curtea de Justiție a Uniunii Europene în Cauza C-201/14 (Bara și alții, cerere preliminară trimisă de Curtea de Apel Cluj) referitoare la baza legală a transmiterii unor date personale privind veniturile persoanelor, între ANAF și CNAS, astfel: "modalităţile de efectuare a transmiterii acestor informaţii au fost elaborate nu prin intermediul unei măsuri legislative, ci prin intermediul Protocolului din 2007 încheiat între ANAF și CNAS, care nu ar fi făcut obiectul unei publicări oficiale."

Totodată, sintagma "în formatul electronic convenit" din alin. (2) al aceluiași articol denotă ambiguitate, putând genera o aplicare practică neuniformă, motiv pentru care este necesară stabilirea concretă a formatului electronic, precum și a modalității de transmitere pe cale electronică, în vederea evitării situațiilor de risc despre care au fost efectuate mențiuni la art. 29 alin. (1) din proiect.

Având în vedere aspectele de mai sus, Autoritatea națională de supraveghere a apreciat că **proiectul de Lege privind venitul minim de incluziune necesită reanalizare**, sub aspectul observațiilor și propunerilor menționate anterior.

- **Guvernul României a solicitat propuneri și observații în ceea ce privește propunerea legislativă privind modificarea și completarea Legii nr. 1/2011, versiune actualizată la 02.10.2015, privind educația națională (Plx 182/2016)**

Autoritatea națională de supraveghere a prezentat următoarele observații și propuneri:

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme video se supune atât prevederilor Legii nr. 677/2001, modificată şi completată, Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video (publicată în M. Of. nr. 389 din 11.06.2012), celor ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată, și Normelor metodologice de aplicare a acesteia, aprobate prin Hotărârea Guvernului nr. 301/2012.

Propunerea legislativă reglementează restrângerea unor drepturi și libertăți, care trebuie să respecte condițiile stabilite de art. 53 din Constituție, în special să îndeplinească condiția necesității și proporționalității măsurii cu situația care a determinat-o.

Prin urmare, stabilirea prin lege, în mod obligatoriu, a unei monitorizări permanente prin supraveghere video a unor persoane fizice, inclusiv minori, poate fi efectuată numai dacă această măsură este proporţională cu riscurile cu care se confruntă operatorul (unitatea de învățământ în cauză).

Expunerea de motive nu face referire la o eventuală insuficiență legislativă în acest domeniu, astfel încât să fie imperios necesară adoptarea unei astfel de reglementări legale. Or, așa cum s-a arătat mai sus, în prezent există cadru normativ în vigoare în acest domeniu.

În același timp, raportat la dispozițiile art. 13 din Legea nr. 24/2000, modificată și completată, și având în vedere mențiunile de la Secțiunea a V-a din Expunerea de motive, precizăm că, în jurisprudenţa Curţii Europene a Drepturilor Omului referitoare la art. 8 din Convenţia pentru apărarea drepturilor omului şi libertăţilor fundamentale (dreptul la respectarea vieții private și de familie), instanța europeană a statuat faptul că nu este întotdeauna posibil să

se facă o diferenţiere netă între activităţile individului, care fac parte din viaţa sa profesională, şi acelea care nu intră în această categorie (Cauza Niemietz contra Germaniei, 16 decembrie 1992) și nicio rațiune nu permite excluderea activității profesionale sau comerciale din sfera

noțiunii de ”viață privată” (Halford c. Regatul Unit, 25 iunie 1997), precum şi faptul că protecţia oferită de articolul 8 ar fi diminuată în mod inacceptabil dacă folosirea de tehnici ştiinţifice moderne ar fi permisă cu orice preţ şi fără realizarea unui echilibru între beneficiile folosirii extensive a acestor tehnici şi interesele importante legate de viaţa privată (Cauza S. şi M. Marper contra Regatului Unit, 4 decembrie 2008).

În ceea ce privește propunerea legislativă, s-a apreciat că aceasta, în forma prezentată, este în contradicție cu cadrul normativ în vigoare și creează un paralelism legislativ.

Astfel, la art. 274 din proiect se face referire în mod eronat la Directiva nr. 52/2012, aceasta fiind, în realitate, Decizia nr. 52/2012, act administrativ cu caracter normativ emis de Autoritatea națională de supraveghere.

Emiterea acestei decizii s-a efectuat în baza Legii nr. 677/2001 și a atribuțiilor Autorității naționale de supraveghere conferite de Legea nr. 102/2005, luându-se în considerare cerinţele care reclamau intervenţia normativă, precum prelucrarea datelor cu caracter personal prin utilizarea de mijloace tehnice specifice – sisteme de supraveghere video, principiile de bază şi finalitatea reglementării propuse, precum și efectele avute în vedere, raportat la obiectul reglementării, respectiv asigurarea unei protecţii eficiente a drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la protecţia datelor cu caracter personal în cazul prelucrărilor efectuate prin utilizarea tehnicilor pentru captarea, transmiterea, manipularea, înregistrarea, stocarea sau comunicarea datelor constituite din imagini privind persoanele fizice ce reprezintă operaţiuni de prelucrare a datelor cu caracter personal.

Astfel, Decizia nr. 52/2012 cuprinde reglementări de principiu (care sunt, de altfel, prevăzute și în Legea nr. 677/2001) destinate unui număr nedeterminat de persoane și conţine nu numai norme juridice imperative (care impun o anumită activitate, de exemplu informarea persoanelor vizate), ci și prohibitive (care interzic o anumită activitate, de exemplu stocarea imaginilor pe o perioadă mai mare de 30 de zile) sau permisive (care oferă posibilitatea de a realiza o anumită activitate, în condiții determinate).

În considerarea diferitelor ipoteze care se pot ivi în aplicarea sa, textul deciziei reglementează și situația supravegherii video a angajaților, indiferent de domeniul de activitate, precum și a minorilor, indiferent de mediul în care se află.

Astfel, art. 3 coroborat cu art. 6, art. 8 şi art. 9 din Decizia nr. 52/2012 stabileşte 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 şi completările ulterioare, în special a principiului proporţionalităţii scopului, şi la consimţământul persoanei vizate sau în alte condiţii de excepţie prevăzute de lege.

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

Alin. (3) al aceluiaşi articol din Decizia nr. 52/2012 prevede că „nu este permisă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, cu excepţia situaţiilor prevăzute expres de lege sau a avizului Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal”.

Astfel, în ceea ce priveşte angajaţii (cadrele didactice, personalul auxiliar), întrucât implementarea unui sistem de supraveghere video poate afecta drepturile lor în calitate de angajaţi, în plus faţă de dispoziţiile Legii nr. 677/2001, modificată şi completată, şi ale art. 8 din Decizia nr. 52/2012, trebuie respectate şi cele prevăzute de Codul Muncii, precum și Statutul cadrelor didactice.

Totodată, s-a precizat că Autoritatea națională de supraveghere a obținut, în instanță, hotărâri definitive și irevocabile prin care s-a statuat faptul că prelucrarea datelor personale (imaginilor) ale angajaților în birouri s-a realizat în condiții de nelegalitate întrucât, anterior implementării dispozitivelor de videosupraveghere, nu a fost efectuată o analiză temeinică asupra necesităţii şi proporţionalităţii unei astfel de măsuri şi nu au fost identificate soluţii alternative care să aibă un impact mai redus asupra vieţii private a salariaţilor.

De asemenea, instanțele au stabilit faptul că prin instalarea camerelor de supraveghere video a fost încălcat dreptul la viaţă privată al salariaţilor şi s-a creat în rândul celor vizualizaţi o stare de disconfort.

În ceea ce privește elevii, art. 9 din Decizia nr. 52/2012 stabileşte 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 situaţiile prevăzute la art. 5 alin. (2) din Legea nr. 677/2001, cu modificările şi completările ulterioare, cu respectarea drepturilor acestora, în special a informării prealabile.

Aceste dispoziții se coroborează cu cele ale art. 27 din Legea nr. 272/2004 privind protecţia şi promovarea drepturilor copilului, republicată, care garantează copilului dreptul la protejarea imaginii sale publice şi a vieţii sale intime, private şi familiale, fiind interzisă orice acţiune de natură să afecteze imaginea publică a copilului sau dreptul acestuia la viaţă intimă, privată şi familială.

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.

În acest context, subliniem faptul că dreptul la viață privată al elevilor, precum și cel al profesorilor și al altor persoane care lucrează în școală, dar și libertatea esențială a actului didactic (libertatea elevilor de a învăța și de a vorbi, libertatea de predare) ar trebui să fie considerate prioritare necesității de supraveghere permanentă prin camere video.

Legat de aspectele de mai sus, s-a precizat faptul că la nivelul Autorității naționale de supraveghere s-au înregistrat solicitări din partea unor unități școlare, pentru 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 şi în sălile de clasă (pe tot parcursul anului), în considerarea acestor spații ca fiind interiorul birourilor unde cadrele didactice și celălalt personal își desfăşoară activitatea la locul de muncă.

Față de solicitarea de efectuare a supravegherii video în sălile de clasă, în alte perioade decât cele ale desfăşurării examenelor naţionale, precum și a supravegherii video în birouri și cancelarii, Autoritatea națională de supraveghere nu a acordat avizul în vederea instalării sistemelor de supraveghere video, ținând cont de mai multe aspecte, cum ar fi: faptul că

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 şi libertăţilor fundamentale sau intereselor persoanelor supravegheate prin utilizarea acestui sistem; nu s-a făcut dovada faptului că a fost efectuată consultarea sindicatului sau a reprezentanţilor angajaţilor și nici dovada obţinerii consimţământului expres şi

neechivoc al tuturor angajaţilor, precum şi al reprezentanţilor legali ai minorilor; nu s-a indicat explicit scopul şi nu s-a argumentat suficient necesitatea prelucrării datelor cu caracter personal ale persoanelor care îşi desfăşoară activitatea în sălile de clasă, în birouri sau cancelarii, prin intermediul sistemelor de supraveghere video.

Având în vedere aspectele de mai sus și ţinând cont de necesitatea asigurării unei protecţii eficiente a dreptului fundamental la viaţă privată al persoanelor supravegheate prin utilizarea mijloacelor de supraveghere video, Autoritatea naţională de supraveghere a considerat că avizul solicitat poate fi acordat în mod excepțional, numai cu respectarea tuturor condițiilor mai sus enunțate și numai pentru situații temeinic justificate și dovedite.

În acest context, instituția noastră a transmis punctul său 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.

Revenind la textul propunerii legislative, în ceea ce privește art. 276 alin. (1) din proiect, unde se face mențiune despre stocarea înregistrărilor timp de 90 de zile, termenul de stocare vine în contradicție atât cu dispozițiile art. 14 din Decizia nr. 52/2012, care stabilește un termen ce nu trebuie să depășească 30 de zile, cât și cu dispozițiile Legii nr. 333/2003 și normele metodologice de aplicare ale acesteia, care prevăd un termen de 20 de zile, fiind excesiv raportat la scopul prelucrării datelor.

În același timp, propunerea legislativă nu prevede, la același articol, termene de arhivare a înregistrărilor, precum și obligația de distrugere sau ștergere, după caz, în vederea respectării principiului stablit de art. 4 alin. (1) lit. e) din Legea nr. 677/2001 și în concordanță cu dispozițiile art. 14 din decizia sus-menționată.

Totodată, în ceea ce privește condițiile de exercitare a dreptului de acces, de la alin. (2) și (3) ale aceluiași articol 276, precum și cele de dezvăluire a înregistrărilor, stabilite la art. 278,

acestea vin în contradicție cu cele stabilite de art. 13 din Legea nr. 677/2001 și, în același timp, aduc atingere dreptului de opoziție și intervenție din aceeași lege (art. 14 și 15).

De asemenea, art. 277 din propunerea legislativă contravine condițiilor de legitimitate a prelucrării datelor fără consimțământul persoanei vizate, stabilite de art. 5 alin. (2) din Legea nr. 677/2001.

În acest context s-a subliniat faptul că, la alegerea modalităţilor de prelucrare a datelor cu caracter personal, trebuie să se aibă în vedere faptul că entitățile deținătoare ale datelor și cele care intră în posesia acestora au obligaţia de a păstra confidențialitatea datelor prelucrate și de a aplica măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal, raportat la prevederile art. 19 și art. 20 din Legea nr. 677/2001.

În sensul celor de mai sus, s-a atras atenția asupra faptului că o astfel de transmitere a înregistrărilor poate determina apariția unor situații de risc pentru protecţia datelor persoanelor fizice (în speță, mai ales ale minorilor) şi, implicit, pentru respectarea şi garantarea drepturilor fundamentale ale acestora, în special cel la viaţă intimă, familială şi privată. În acest sens, posibilitatea de interceptare a imaginilor transmise prin Internet în timp real, datorită tehnologiilor informatice actuale, avansate, conduce la o vizualizare a acestora de către un număr nedefinit de persoane, cu o potențială utilizare ulterioară neconformă cu dispozițiile legale privind protecția datelor și cu riscul aducerii unor atingeri grave drepturilor și libertăților fundamentale ale persoanelor fizice.

În consecință, raportat la observațiile prezentate anterior, ținând cont de necesitatea respectării cerințelor art. 53 din Constituție, având în vedere prevederile Legii nr. 24/2000, modificată și completată, precum și existența cadrului normativ în domeniu, Autoritatea națională de supraveghere **nu a susținut textul propunerii legislative** privind modificarea și completarea Legii nr. 1/2011, versiune actualizată la 02.10.2015 privind educația națională (Plx 182/2016).

- **Guvernul României a transmis propunerea legislativă pentru modificarea art. 5 din Legea nr. 677/2001 (Bp 181/2016)**

Faţă de conţinutul acestei propuneri, Autoritatea națională de supraveghere a prezentat următoarele observații:

Legea nr. 677/2001 a implementat în România Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Directiva 95/46/CE urmărește, astfel cum reiese în special din considerentul (8) al acesteia, ca nivelul protecției drepturilor și libertăților persoanei în ceea ce privește prelucrarea

datelor cu caracter personal să fie echivalent în toate statele membre. În considerentul (10) al acestei directive se adaugă că apropierea legislațiilor naționale aplicabile în acest domeniu nu trebuie să aibă ca rezultat scăderea protecției pe care o oferă, ci trebuie, dimpotrivă, să aibă drept obiectiv asigurarea unui nivel înalt de protecție în Uniune.

Astfel, dispozițiile art. 7 din Directiva 95/46/CE intitulat ”Criterii privind legitimitatea prelucrării datelor” au fost implementate de art. 5 din Legea nr. 677/2001.

În acest context, precizăm că, potrivit dispozițiilor art. 5 din cadrul capitolului II din Directiva 95/46/CE intitulat „Condițiile generale de legalitate a prelucrării datelor cu caracter personal”, statele membre precizează, în limitele dispozițiilor prezentului capitol, condițiile în care operațiunile de prelucrare a datelor cu caracter personal sunt legale”.

Astfel, acest articol nu permite statelor membre decât să precizeze, în limitele capitolului II din directiva menționată și, prin urmare, ale articolului 7 din aceasta, condițiile în care operațiunile de prelucrare a datelor cu caracter personal sunt legale.

Rezultă că statele membre nu pot nici să adauge principii noi privind legitimarea prelucrărilor de date cu caracter personal la articolul 7 din Directiva 95/46/CE, nici să prevadă cerințe suplimentare care să modifice conținutul unuia dintre cele șase principii prevăzute la acest articol.

Prin urmare, marja de apreciere de care dispun statele membre în temeiul articolului 5 menționat nu poate fi utilizată decât în conformitate cu obiectivul urmărit de Directiva 95/46/CE, care constă în menținerea unui echilibru între libera circulație a datelor cu caracter personal și protecția vieții private.

În consecință, în temeiul articolului 5 din Directiva 95/46/CE, statele membre nu pot nici să introducă alte principii referitoare la legitimarea operațiunilor de prelucrare a datelor cu caracter personal decât cele prevăzute la articolul 7 din această directivă, nici să modifice, prin cerințe suplimentare, conținutul celor șase principii prevăzute la articolul 7 menționat.

Această interpretare este confirmată de termenii „să fie prelucrate numai dacă” și de conjuncția „sau” din textul articolului 7 din Directiva 95/46/CE, care pun în evidență natura exhaustivă și limitativă a listei prevăzute la acest articol.

În sensul celor de mai sus a statuat și Curtea de Justiție a Uniunii Europene în cauzele reunite C-468/10 și C-469/10.

În acest context, precizăm că propunerea de completare a condițiilor art. 5 din Legea nr. 677/2001 adaugă o situație suplimentară care nu se regăsește în principiile referitoare la legitimarea operațiunilor de prelucrare prevăzute de art. 7 din Directiva 95/46/CE și care impune, în lipsa consimțământului persoanei vizate, dezvăluirea datelor acesteia, având ca rezultat scăderea protecției pe care o oferă această directivă.

Prin urmare, propunerea legislativă nu este compatibilă cu Directiva 95/46/CE și contravine jurisprudenței CJUE.

În consecință, Autoritatea națională de supraveghere **s-a exprimat în sensul respingerii acestei inițiative legislative.**

- **Agenția Națională de Administrare Fiscală a solicitat propuneri și observații în ceea ce privește proiectul de Ordin pentru modificarea și completarea Procedurii de publicare a listelor debitorilor care înregistrează obligații fiscale restante, precum și cuantumul acestor obligații, aprobată prin Ordinul președintelui Agenției Naționale de Administrare Fiscală nr. 558/2016**

Față de textul proiectului de Ordin s-au precizat următoarele:

La publicarea de către Agenția Națională de Administrare Fiscală, pe site-ul propriu, a Listei debitorilor - persoane fizice care înregistrează obligații fiscale restante la bugetul general consolidat, precum și cuantumul acestor obligații (Anexa nr. 2 la procedura aprobată prin proiectul de ordin supus analizei), aceasta, în calitate de operator de date cu caracter personal, trebuie să efectueze prelucrarea datelor cu respectarea regulilor generale prevăzute de Legea nr. 677/2001.

S-a atras atenția asupra prevederilor pct. 11, 13, 14, 15, 16 din Procedura aprobată prin proiectul de ordin supus analizei și s-a subliniat că operatorului Agenția Națională de

Administrare Fiscală îi revine întreaga responsabilitate pentru asigurarea exactității și actualizării datelor cu caracter personal dezvăluite prin publicarea listei conținând debitorii persoane fizice, obligațiile fiscale restante la bugetul general consolidat ale acestora și cuantumul obligațiilor respective.

Agenției Naționale de Administrare Fiscală îi revine obligația de respectare a dreptului la informare al persoanelor vizate, prevăzut de art. 12, de respectare a drepturilor persoanelor fizice ale căror date le prelucrează, prevăzute de art. 13 - 18, precum și obligația de asigurare a confidenţialităţii şi securităţii prelucrării datelor, prevăzute de art. 19 și art. 20.

În ceea ce privește necesitatea asigurării unei informări complete a debitorilor, raportat la dispozițiile art. 12 din Legea nr. 677/2001, s-a subliniat că este necesar ca Agenția Națională de Administrare Fiscală să ia în considerare, și în cazul dezvăluirilor de date cu caracter personal prin publicarea Listei debitorilor - persoane fizice care înregistrează obligații fiscale restante la bugetul general consolidat, precum și cuantumul acestor obligații, cele statuate de Curtea de Justiție a Uniunii Europene prin hotărârea din Cauza Smaranda Bara și alții (C-201/14).

Ca efect al aplicării principiilor de prelucrare a datelor prevăzute de art. 4 din Legea nr. 677/2001, s-a propus modificarea pct. 3 și pct. 5 din procedura aprobată prin proiectul de Ordin, astfel încât să nu fie considerate obligații fiscale restante obligațiile fiscale contestate, până la pronunțarea unei hotărâri judecătorești definitive, și implicit, să nu fie publicat cuantumul acestora. Ca atare, propunem eliminarea câmpurilor ”obligații fiscale contestate” din Lista debitorilor - persoane fizice care înregistrează obligații fiscale restante la bugetul general consolidat, precum și cuantumul acestor obligații.

De altfel, raportat la prevederile proiectului de Ordin sus menționat, **s-a considerat că**, deși acesta este emis în baza prevederilor Codului de procedură fiscală, **publicarea de către Agenția Națională de Administrare Fiscală, pe internet, a Listei debitorilor** - persoane fizice care înregistrează obligații fiscale restante la bugetul general consolidat, precum și cuantumul acestor obligații (Anexa nr. 2) **este de natură a aduce atingere dreptului la viață privată, raportat la necesitatea respectării principiilor proporționalității și neexcesivității prelucrărilor de date cu caracter personal.**

În contextul celor de mai sus, Autoritatea națională de supraveghere a supus atenției Agenției Naționale de Administrare Fiscală propunerea de modificare a prevederilor din Codul de procedură fiscală cu privire la publicarea listelor debitorilor persoane fizice (art. 162 din Codul de procedură fiscală), astfel încât persoanele vizate, debitori, să nu fie expuse oprobriului public și să se asigure o reală respectare a vieții private și a protecției datelor.

Sub acest aspect, s-a apreciat că postarea listei menționate pe site-ul Agenției Naționale de Administrare Fiscală și dezvăluirea de date personale ale debitorilor către publicul larg, pe internet, excede scopului de ”colectare de taxe și impozite”, care se realizează prin alte mijloace specifice.

În acest context, s-a menționat că a intrat în vigoare Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), aplicabil în mod direct în toate statele membre ale Uniunii Europene.

S-a subliniat că, potrivit principiului responsabilității din Regulamentul (UE) 2016/679, operatorul nu numai că este responsabil de respectarea tuturor principiilor de prelucrare a datelor ("legalitate, echitate şi transparenţă", "limitări legate de scop", "reducerea la minimum a datelor", "exactitate", "limitări legate de stocare", precum și "integritate şi confidenţialitate"), dar este necesar ca acesta să poată demonstra respectarea principiilor menționate.

- **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește proiectul de Lege privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, investigarea şi urmărirea penală a infracţiunilor de terorism şi a infracţiunilor grave, precum prevenirea şi înlăturarea ameninţărilor la adresa securităţii naţionale**

Faţă de textul proiectului de lege sus-menționat, instituţia noastră a formulat următoarele observaţii şi propuneri:

Autoritatea naţională de supraveghere a reiterat aprecierile exprimate și în corespondența anterioară cu privire la această inițiativă legislativă, potrivit căreia implementarea unui astfel de sistem de colectare şi prelucrare a datelor despre pasageri presupune o prelucrare pe scară largă a datelor cu caracter personal şi poate reprezenta o nouă situaţie de risc pentru protecţia datelor cu caracter personal ale persoanelor fizice şi, implicit, pentru respectarea şi garantarea drepturilor fundamentale ale acestora, în special cel la viaţă privată.

În acelaşi timp, implementarea unui asemenea sistem presupune colectarea unui volum foarte mare de date, motiv pentru care trebuie să se demonstreze clar că acest sistem are un caracter necesar, legitim şi proporţional şi că obiectivul său nu poate fi atins printr-un sistem mai puţin intruziv raportat la viaţa privată.

Legalitatea acestui sistem trebuie evaluată având în vedere principiile statuate în Carta drepturilor fundamentale ale UE, în special în art. 7 privind dreptul la viaţă privată şi familială şi art. 8 privind protecţia datelor personale, două drepturi diferite şi complementare, garantate de Cartă, precum şi cele ale art. 8 din Convenţia pentru apărarea drepturilor şi libertăţilor fundamentale.

În același timp, s-a subliniat importanţa deciziei din 2014 a Curţii de Justiţie a Uniunii Europene, care a invalidat Directiva privind reţinerea datelor întrucât „legiuitorul UE a depăşit limitele impuse de respectarea principiului proporţionalităţii în lumina art. 7, 8 şi 52(1) din Cartă.” Aceste aspecte au fost avute în vedere şi de Curtea Constituţională a României la declararea ca neconstituţională a Legii nr. 82/2012.

De asemenea, amintim faptul că principiile necesităţii şi proporţionalităţii acestui sistem pot fi demonstrate doar după evaluarea funcţionalităţii şi utilităţii sistemelor informatice deja existente la scară largă, în cadrul cărora se prelucrează o multitudine de informaţii.

Prin urmare, atunci când se propune şi se concepe un nou sistem informatic la scară largă, acesta trebuie să respecte principiile necesităţii, proporţionalităţii, responsabilităţii (accountability principle), evaluarea impactului asupra domeniului protecţiei datelor („data protection impact assessment”), luarea în considerare a vieţii private începând din momentul conceperii („privacy by design”), stabilirea setărilor de confidenţialitate încă de la prima utilizare la cel mai înalt nivel („privacy by default”), limitarea scopului, precum şi regulile referitoare la notificarea breşelor de securitate („data breach notification”). Aceste aspecte sunt în acord și cu

Noul Regulament (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) ale cărui prevederi vor fi aplicabile în mod direct în toate statele membre ale Uniunii Europene, începând cu data de 25 mai 2018.

Totodată, s-a apreciat că este necesară analizarea impactului asupra drepturilor fundamentale, precum şi a garanţiilor privind protecţia datelor.

În acest context, s-a reamintit faptul că aspectele prezentate mai sus au făcut obiectul adresei Grupului de Lucru Articolul 29 (care reuneşte toate autorităţile de protecţie a datelor din Statele Membre, înfiinţat pe lângă Comisia Europeană) înaintată Comitetului LIBE din cadrul Parlamentului European cu referire la sistemul UE privind datele pasagerilor, atrăgându-se atenţia, în principal, asupra următoarelor aspecte: demonstrarea necesităţii unui sistem PNR la nivel UE, respectiv asigurarea proporţionalităţii prelucrării datelor.

În ceea ce priveşte textul proiectului de lege, s-au efectuat, în principal, următoarele observaţii:

Raportat la dispozițiile Directivei (UE) 2016/681, s-a subliniat faptul că scopul proiectului de lege referitor la ”prevenirea și înlăturarea amenințărilor la adresa securității naționale” nu se regăsește în sfera de reglementare a acesteia.

Dimpotrivă, directiva sus-menționată face vorbire despre faptul că domeniul său de aplicare este cât se poate de limitat, iar în conformitate cu principiul proporționalității, directiva nu depășește ceea ce este necesar pentru realizarea obiectivelor menționate.

Totodată, Directiva (UE) 2016/681 prevede că aplicarea acesteia ”ar trebui să asigure respectarea deplină a drepturilor fundamentale, a dreptului la viață privată și a principiului proporționalității”.

De asemenea, directiva prevede și faptul că statele membre sunt obligate să asigure că o autoritate națională de supraveghere independentă este responsabilă de consilierea și de monitorizarea privind modul de prelucrare a datelor din registrul cu numele pasagerilor.

Față de dispozițiile legale sus-menționate, raportat la scopul referitor la ”prevenirea și înlăturarea amenințărilor la adresa securității naționale”, prevăzut de titlul proiectului de lege și

la art. 18 lit. b), rezultă că Autoritatea națională de supraveghere ar avea atribuții restrânse, fiind în imposibilitate de a-și îndeplini competențele în integralitatea lor, nefiind respectate, în același timp, exigențele de independență ale acesteia impuse de Directiva (UE) 2016/681.

Potrivit art. 1 alin. (2) din Directiva (UE) 2016/681, „datele PNR pot fi colectate doar în scopul prevenirii, investigării şi urmăririi penale a infracţiunilor de terorism şi a infracţiunilor grave, astfel cum este prevăzut la art. 6 alin. 2 lit. a), b) şi c)".

În aceste dispoziții nu se regăsește sintagma „înlăturarea ameninţărilor la adresa securităţii naţionale", ele referindu-se la prelucrarea datelor PNR exclusiv în vederea prevenirii activităţilor teroriste sau a unor infracţiuni grave.

În plus, raportat la dispozițiile din proiectul de lege ce stabilesc competențele UNIP, scopul sus-menționat vine în contradicție și cu acestea, lăsând să se interpreteze că UNIP îndeplinește ambele scopuri prevăzute de art. 18 (deci inclusiv cel prevăzut de Legea nr. 51/1991), deși este organizat în cadrul Inspectoratului General al Poliției de Frontieră și are calitatea de operator de date cu caracter personal, intrând sub incidența Legii nr. 677/2001.

În sensul celor de mai sus, s-a considerat necesară reanalizarea extinderii scopului proiectului de lege, față de cel stabilit de Directiva (UE) 2016/681 și punerea în acord cu dispozițiile acesteia și ale Legii nr. 677/2001, prin eliminarea acestuia din textul actului normativ.

În același timp, s-a arătat că se impune eliminarea pct. 1 din Anexa proiectului de lege care stabileşte lista infracţiunilor, referitor la „infracţiuni contra securităţii naţionale", punct care nu se regăseşte şi în Anexa II a directivei, anexă ce se referă la lista infracţiunilor grave.

De asemenea, raportat la aplicabilitatea legii inclusiv la zborurile intra-UE, prevăzută la art. 1 alin. (1) lit. a), aceasta este o măsură excepțională, care poate fi luată numai cu respectarea condițiilor art. 2 din Directiva (UE) 2016/681, fiind de natură să afecteze respectarea principiilor proporționalității și necesității, menționate anterior, cu efecte negative asupra respectării dreptului la viață privată al cetățenilor Uniunii Europene.

În ceea ce priveşte categoriile de date despre pasageri, ce se regăsesc la art. 14, prin raportare și la opinia Grupului de Lucru Art. 29 (WP 181/2011), apreciem că lista de elemente ale datelor despre pasageri este excesivă. Mai mult, aşa cum a declarat şi Comisia Europeană, datele PNR sunt de fapt informaţii neverificate. Cu alte cuvinte, acestea nu sunt nici complete şi

nici absolut exacte, aspect ce nu respectă unul dintre principiile protecţiei datelor cu caracter personal, respectiv datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie exacte şi, dacă este cazul, actualizate.

Mai mult, la această listă se adaugă implicit informații suplimentare care, deși nu sunt conţinute în mod expres de art. 14 (1), ele pot fi deduse din anumite categorii de date cum ar fi, spre exemplu, la lit. j) „situaţia de călătorie…" sau la lit. s) „un istoric al tuturor modificărilor

datelor PNR prevăzute la lit. a)-r)". Astfel, pot fi obţinute informaţii privind convingerile religioase, privind starea de sănătate etc., deci implicit mai multe date decât cele deja stabilite, inclusiv dintre cele cu caracter sensibil.

Referitor la prevederile art. 17 din proiect, acesta se impune a fi eliminat, întrucât competențele de monitorizare ale UNIP contravin art. 15 din Directivă, reprezentând o suprapunere cu atribuțiile de investigare ale Autorității nationale de supraveghere și, ca atare, o ingerință gravă în competențele acesteia stabilite conform reglementărilor legale în vigoare.

În ceea ce privește autoritățile competente stabilite la art. 11 alin. (1), pentru claritatea normei, este necesară precizarea denumirii exacte a celor de la lit. a)-d), inclusiv cu menționarea autorității publice în cadrul căreia sunt organizate direcțiile/departamentele în cauză.

De asemenea, s-a solicitat reanalizarea stabilirii în sfera autorităților competente a Poliției Române (lit. a), raportat la art. 5 din Legea nr. 218/2002, republicată, care se referă inclusiv la instituţii de învăţământ pentru formarea şi pregătirea continuă a personalului, precum și la alte unități necesare pentru îndeplinirea atribuţiilor specifice poliţiei, înfiinţate potrivit legii.

Aceleași solicitări s-au adresat și cu privire la Poliția de Frontieră Română (lit. b), raportat la art. 6 din Ordonanța de urgență nr. 104/2001, modificată și completată, care face vorbire și de unităţi sau instituţii de învăţământ, centre de formare profesională, centre, birouri şi puncte de contact, precum și alte unităţi.

Cu privire la art. 11 alin. (1) lit. i) din proiect, s-a recomandat reanalizarea și, în consecință, eliminarea acestei autorități din sfera celor competente, având în vedere motivarea din Expunerea de motive a proiectului de lege, referitoare la atribuțiile ANAF – Direcția Generală a Vămilor privind supravegherea și controlul vamal al mărfurilor, aspecte ce nu se circumscriu sferei de aplicare a Directivei (UE) 2016/681.

La art. 42 (3) din proiect s-a propus eliminarea sintagmei „unui caz de defecţiune tehnică de scurtă durată”, întrucât apreciem că acesta nu poate fi asimilat cazului de forţă majoră, raportat la obligaţiile stabilite de art. 20 din Legea nr. 677/2001 în sarcina operatorului, respectiv de luare a măsurilor necesare inclusiv referitor la distrugerea accidentală și la pierderea datelor.

Referitor la regimul sancționator, s-a remarcat faptul că acesta vine în contradicție cu art. 41 care stabilește competențele Autorității naționale de supraveghere în ceea ce privește monitorizarea prelucrării datelor în sistemul PNR, dar și cu art. 15 (Autoritatea de supraveghere) raportat la art. 4-6 (referitoare la unitatea de informații despre pasageri - UIP) din Directiva (UE) 2016/681, precum și cu dispozițiile art. 35 din Legea nr. 677/2001. Or, prevederile art. 42 alin. (1) lit. a)-c) se referă la operațiuni de prelucrări de date pe care transportatorii aerieni (operatorii de date) trebuie să le respecte, aspecte ce intră în sfera de competență exclusivă a Autorității naționale de supraveghere.

În consecință, s-a arătat că art. 42 alin. (5) și (6) se impun a fi reanalizate și modificate în concordanță cu prevederile Directivei (UE) 2016/681 și ale Legii nr. 677/2001, astfel încât constatarea și aplicarea sancțiunilor să revină în competența exclusivă a Autorității naționale de supraveghere.

Pe cale de consecinţă, faţă de textul proiectului de lege transmis, Autoritatea națională de supraveghere a apreciat că implementarea unui astfel de sistem de evidenţă poate reprezenta o nouă situaţie de risc pentru protecţia datelor cu caracter personal ale persoanelor fizice şi, implicit, pentru respectarea şi garantarea drepturilor fundamentale ale acestora, în special a dreptului la viaţă intimă, familială şi privată cu privire la prelucrarea datelor cu caracter personal.

Prin urmare, Autoritatea națională de supraveghere **nu a susținut proiectul de lege în forma prezentată**.

- **Ministerul Comunicațiilor și pentru Societatea Informațională** a solicitat propuneri și observații în ceea ce privește textul **proiectului de Lege pentru**

completarea Ordonanței de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, modificat și completat

Faţă de textul proiectului de lege sus-menționat, instituţia noastră a formulat următoarele observaţii şi propuneri:

Potrivit Legii nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, expunerea de motive constituie instrumentul de prezentare şi motivare ale noii reglementări propuse.

În acest sens, s-a remarcat faptul că proiectul de lege nu este însoțit și de expunerea de motive.

De asemenea, s-a menționat că, deşi proiectul de lege are ca obiect de reglementare modificarea cadrului normativ general cu privire la comunicaţiile electronice, din textul prezentat analizei rezultă că, în realitate, actul normativ ar urma să completeze cadrul legislativ privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cadru reglementat prin Legea nr. 506/2004.

Astfel, s-a subliniat că proiectul vizează reţinerea şi stocarea datelor de către furnizorii de servicii de comunicații electronice, în cadrul utilizării cartelelor preplătite, ceea ce echivalează cu o restrângere a dreptului la viaţă privată, limitare ce poate opera numai în conformitate cu dispoziţiile art. 53 din Constituție și în acord cu prevederile Legii nr. 677/2001.

În ceea ce privește propunerile de text, s-a arătat că se impune determinarea cu exactitate a sferei datelor personale ce vor fi colectate de către furnizori.

Referitor la precizările de la alin. (13), textul formulat nu denotă claritate și previzibilitate, în sensul că nu este reglementată în detaliu procedura prin care se realizează operațiunea de colectare a datelor personale, inclusiv sub aspectul obligațiilor de confidențialitate și securitate ce revin operatorilor și împuterniciților, raportat și la criticile din Decizia Curții Constituționale nr. 461/2014, exprimate în acest sens.

De asemenea, formularea textului tezei a doua a alin. (13), în special a sintagmei ”acestor documente”, denotă neclaritate și conduce la interpretarea că acestea vizează inclusiv copii ale documentelor de identitate, motiv pentru care este necesară reformularea textului.

La alin. (14) lit. a), termenul de ”abonat” utilizat creează confuzie, întrucât conform OUG nr. 111/2011, în forma actuală, abonat este considerat și cel care beneficiază de servicii cu plata

în avans, motiv pentru care este necesară precizarea clară a categoriei de abonați căreia îi aparține utilizatorul final căruia nu i se solicită datele. În acest sens, este necesară și analizarea și clarificarea termenului ”utilizatorul final” de la alin. (11) și (12).

De asemenea, raportat la excepțiile privind modalitatea de colectare prevăzută de alin. (14), pentru abonații ale căror date sunt deja înregistrate, se impune a fi avută în vedere și respectarea principiului potrivit căruia datele trebuie să fie exacte şi, dacă este cazul, actualizate, inclusiv sub aspectul luării măsurilor necesare pentru ca datele inexacte sau

incomplete din punct de vedere al scopului pentru care sunt colectate şi pentru care vor fi ulterior prelucrate, să fie şterse sau rectificate.

În ceea ce privește ”portarea” prevăzută la lit. c) a alin. (14), este necesară analizarea și coroborarea datelor stabilite de această procedură cu cele stabilite la alin. (12), pentru evitarea unor interpretări și aplicări neunitare în practică.

Referitor la trimiterea de la alin. (15), raportat la referințele Curții Constituționale din Decizia nr. 461/2014, s-a apreciat că menționarea acesteia nu este suficientă pentru a se asigura garanțiile necesare pe care statul trebuie să le asigure în exercitarea drepturilor fundamentale ale cetățenilor, în special a dreptului la viață privată.

Raportat la termenul de 3 ani prevăzut la alin. (16), s-a reiterat observația potrivit căreia acesta se referă la toate operațiunile de prelucrare și la toate datele stabilite de alin. (12) de la pct. 2 din proiect, în dezacord cu principiul stocării datelor strict pe perioada necesară îndeplinirii scopului, statuat de art. 4 alin. (1) lit. e) din Legea nr. 677/2001. În acest sens, remarcăm faptul că textul este ambiguu și conduce la interpretarea potrivit căreia furnizorii de servicii pot efectua orice tip de operațiune de prelucrare a datelor, chiar pe o perioadă mai mare decât cea la care obliga Legea nr. 82/2012 (6 luni), declarată neconstituțională, neexistând o uniformitate și o previzibilitate a modului în care vor acționa furnizorii. În acest sens, semnalăm că propunerea este în neconcordanță și cu prevederile art. 5 din Legea nr. 506/2004, astfel cum a fost modificat prin Legea nr. 235/2015, ținând cont de faptul că prezentul proiect de lege vizează, de asemenea, comunicațiile electronice.

Totodată, s-a învederat faptul că proiectul de lege nu prevede în mod expres condițiile de acces al autorităților la date, precum și scopul în care se realizează acesta, fiind astfel încălcat principiul proporționalității, raportat la cele reținute de Curtea Constituțională în Decizia nr.

461/2014, precum și la dispozițiile art. 53 din Constituție care prevăd condițiile restrângerii exercițiului unor drepturi sau al unor libertăți.

În consecință, Autoritatea națională de supraveghere a apreciat că este necesară prezentarea expunerii de motive care să fundamenteze proiectul de act normativ, luând în considerare caracterul de restrângere a unui drept fundamental, precum și reanalizarea și reformularea textelor în vederea stabilirii unor norme clare și previzibile, pentru respectarea cerinţelor de necesitate şi proporţionalitate stabilite de Legea fundamentală și a normelor de tehnică legislativă.

- **Ministerul Finanțelor Publice** a solicitat propuneri și observații în ceea ce privește textul proiectului de **Hotărâre a Guvernului pentru modificarea şi completarea Normelor metodologice pentru aplicarea Ordonanţei de urgenţă a Guvernului nr. 28/1999 privind obligaţia operatorilor economici de a utiliza aparate de marcat electronice fiscale, aprobate prin Hotărârea Guvernului nr. 479/2003, însoțit de Nota de fundamentare**

Față de conținutul documentelor transmise, Autoritatea națională de supraveghere a formulat următoarele observații:

S-a remarcat faptul că Normele metodologice aprobate prin Hotărârea Guvernului nr. 479/2003 au fost emise pentru aplicarea Ordonanţei de urgenţă a Guvernului nr. 28/1999. Această ordonanță reglementează obligația de a utiliza aparate de marcat electronice fiscale și de a emite bonuri fiscale sau facturi, după caz, în scopul combaterii evaziunii fiscale, vizând activitatea agenților economici, iar nu a persoanelor fizice care au calitatea de cumpărători ai unor bunuri și servicii și care nu desfășoară o activitate economică.

În același timp, ordonanța sus-menționată stabilește obligația operatorilor economici de comunicare către ANAF a datelor fiscale generate de operațiunea de comerț în cauză, iar nu a datelor personale aparținând persoanelor fizice în calitatea acestora de consumatori.

În acest context subliniem faptul că, potrivit normelor de tehnică legislativă, actele normative date în executarea legilor sau ordonanţelor (în cazul de față o hotărâre de Guvern) se emit în limitele şi potrivit normelor care le ordonă.

Or, în cadrul proiectului de hotărâre de Guvern prezentat analizei, se remarcă extinderea sferei datelor fiscale strict necesare operațiunii în cauză, prin adăugarea unor categorii de date

noi, având natura unor date cu caracter personal, pe care operatorii economici sunt obligați să le colecteze și prelucreze fără consimțământul persoanei fizice vizate și să le comunice ANAF.

Față de aspectele de mai sus, subliniem faptul că, raportat la prevederile art. 26 din Constituție, care garantează dreptul la viață privată, restrângerea unui drept fundamental se poate realiza doar în condițiile prevăzute de art. 53 din Constituție, respectiv numai prin lege și numai dacă se impune, iar măsura trebuie să fie proporțională cu situația care a determinat-o.

Totodată, în conformitate cu principiile desprinse din jurisprudența 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 stabilească 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.

Prin urmare, restrângerea unui drept fundamental se poate reglementa numai prin lege și numai în condițiile constituționale sus-amintite.

Astfel, instituirea unei monitorizări permanente a unui număr nedeterminat de persoane fizice, prin înregistrarea a priori a unor date cu caracter personal, indiferent de suma plătită sau produsul achiziționat, poate fi efectuată doar prin lege și numai dacă această măsură este proporţională cu situația care a determinat-o şi dacă necesită o asemenea intruziune în viaţa privată a persoanelor vizate.

De asemenea, este necesar să se ţină cont şi de interesele, drepturile şi libertăţile persoanelor vizate, urmărindu-se realizarea unui echilibru între drepturile lor fundamentale și interesele economice ale statului.

Or, raportat la textul Ordonanței de urgență nr. 28/1999, republicată, din analiza acestuia, remarcăm faptul că nu există prevederi privind prelucrarea de date cu caracter personal, precum cele care figurează în proiectul normelor metodologice.

Raportat la colectarea în masă a unei multitudini de date personale de la un număr potențial foarte mare de persoane, precizăm faptul că, în jurisprudența sa, Curtea de Justiţie a Uniunii Europene (cauzele conexate C-293/12 şi C-594/12), în verificarea validității Directivei

2006/24/CE („Directiva privind reţinerea datelor”), admite că motivele care au stat la baza adoptării acesteia sunt legitime, scopul urmărit fiind combaterea criminalităţii şi siguranţa publică, dar constată că legiuitorul UE a depăşit limitele impuse de respectarea principiului proporţionalităţii.

Astfel, directiva viza toate persoanele, mijloacele de comunicare electronică şi datele privind traficul, fără ca nicio diferenţiere, limitare sau excepţie să fie operată în funcţie de obiectivul combaterii infracţiunilor grave.

În același timp, CJUE a stabilit că directiva nu prevede garanţii suficiente care să permită asigurarea unei protecţii eficiente a datelor faţă de riscurile de abuz, precum şi faţă de orice accesare şi utilizare ilicită a datelor.

Aceleași aspecte au fost analizate și de Curtea Constituțională a României, atunci când, prin Decizia nr. 440/2014, a pronunțat neconstituționalitatea dispoziţiilor Legii nr. 82/2012, statuând că legea nu oferă garanţiile necesare protecţiei dreptului la viaţă intimă, familială şi privată al persoanelor ale căror date stocate sunt accesate.

În acest context, s-a constatat faptul că precizările de la Secțiunea a 5-a, pct. 4 din Nota de fundamentare a proiectului supus analizei nu au suport, în sensul că modificările legislative nu ar contraveni jurisprudenței Curții de Justiție a Uniunii Europene.

În ceea ce privește mențiunile de la Secțiunea a II-a referitoare la Descrierea situației, acestea nu sunt în măsură să justifice necesitatea colectării tuturor datelor personale stabilite ca fiind suplimentare față de cele fiscale, strict necesare îndeplinirii scopului, respectiv acela de combatere a evaziunii fiscale potențial săvârșite de către operatorii economici, iar nu de către persoanele fizice care, în plus, nici nu desfășoară vreo activitate economică.

Raportat la prevederile art. 4 alin. (3) din Anexa 8 (Anexa nr. 11 la normele metodologice) din proiectul de hotărâre, referitoare la ”Conectarea la distanţă”, care se recomandau a fi analizate, cu precădere, s-a precizat că datele personale precum: ”g) numărul cardului utilizat pentru efectuarea plății; h) cod autorizare plată; i) toate detaliile disponibile cu privire la identitatea deținătorului cardului”, comunicate către Agenția Națională de Administrare Fiscală, simultan cu transmiterea tranzacției către instituția acceptantă a plății implică efectuarea de prelucrări de date cu caracter personal.

În contextul reglementărilor legale în vigoare, o comunicare de date personale, în modalitatea stabilită, către Agenția Națională de Administrare Fiscală, poate prezenta riscuri

pentru drepturile fundamentale ale persoanelor fizice, cu atât mai mult cu cât, prin sintagma generică și echivocă referitoare la ”toate detaliile disponibile cu privire la identitatea deținătorului cardului” nu se respectă principiile de previzibilitate și predictibilitate pe care trebuie să le respecte un act normativ, în sensul stabilirii concrete a categoriilor de date personale și a necesității colectării acestora.

În condițiile în care impactul social al proiectului, așa cum acesta este menționat în Nota de fundamentare, se referă la ”creşterea gradului de încredere a populaţiei în corecta utilizare a aparatelor de marcat electronice fiscale de către operatorii economici şi în colectarea corectă de către organele fiscale a impozitelor şi taxelor datorate bugetului de stat” s-a apreciat, raportat la prevederile art. 4 alin. (3) din Anexa 8 (Anexa nr. 11 la normele metodologice) a proiectului de hotărâre, că datele prelucrate de către Agenția Națională de Administrare Fiscală, precum cele în discuție, apar ca fiind excesive scopului menționat de ”colectare de taxe și impozite”, contravenind principiilor legalității, proporționalității și necesității prevăzute de Directiva 95/46/CE și Legea nr. 677/2001.

Or, art. 11 alin. (10) din Legea nr. 207/2015 - Codul de procedură fiscală prevede că: ”Prelucrarea datelor cu caracter personal de către organele fiscale centrale şi locale se realizează cu respectarea prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare.”

Astfel, atât comercianții, cât și Agenția Națională de Administrare Fiscală, în calitate de operatori de date cu caracter personal, trebuie să efectueze prelucrarea datelor cu respectarea principiilor prevăzute de Legea nr. 677/2001, indiferent dacă datele se prelucrează la consimțământul persoanei fizice în cauză sau fără acordul acesteia.

Așadar, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, să fie colectate în scopuri determinate, explicite şi legitime, să fie adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate, să fie exacte şi, dacă este cazul actualizate, să fie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care sunt colectate.

Aceleași observații raportate la respectarea principiului proporționalității scopului și a caracterului neexcesiv al datelor au fost efectuate și cu privire la colectarea datelor personale stabilite la pct. 48 din proiect, referitor la art. 56 alin. (2) lit. a) și alin. (4) lit. a).

Mai mult, se observă faptul că transmiterea datelor se realizează pe cale electronică, context în care subliniem faptul că, la alegerea modalităţilor de prelucrare a datelor cu caracter personal, trebuie să se aibă în vedere faptul că entitățile deținătoare ale datelor și cele care

intră în posesia acestora au obligaţia de a păstra confidențialitatea datelor prelucrate și de a aplica măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal.

Raportat la observațiile prezentate anterior, Autoritatea națională de supraveghere a apreciat că textul proiectului de hotărâre a Guvernului, supus analizei, trebuie să respecte limitele actului normativ în baza căruia este emis, respectiv Ordonanța de urgență nr. 28/1999.

De asemenea, ținându-se cont de faptul că se pune în discuție restrângerea unui drept fundamental, dreptul la viață privată, se impune a fi avută în vedere necesitatea stabilirii unor norme clare și previzibile, pentru respectarea cerinţelor de necesitate şi proporţionalitate stabilite de Legea fundamentală și a normelor de tehnică legislativă.

În consecință, raportat la protecția persoanelor ale căror date personale sunt prelucrate și, implicit, a vieții private a acestora, Autoritatea națională de supraveghere **nu susține proiectul de act normativ în forma prezentată**.

Secţiunea a 2-a Puncte de vedere privind diverse chestiuni de protecţia datelor

a) Cu privire la postarea în mediul on-line de fotografii

O asociaţie a solicitat punctul de vedere al Autorităţii naționale de supraveghere cu privire la condiţiile legale de prelucrare a datelor cu caracter personal, respectiv fotografii şi interviuri cu persoane considerate ca fiind cazuri umanitare.

S-au precizat următoarele:

Regula instituită de Legea nr. 677/2001, modificată şi 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 consimţământul persoanei în cauză, dat în mod expres şi neechivoc.

În mod excepţional însă, datele cu caracter personal pot fi prelucrate (inclusiv dezvăluite) fără consimţământul persoanei vizate, în mai multe situaţii de excepţie. Aceste cazuri, de strictă interpretare și aplicare, sunt menţionate în mod expres la art. 5 alin. (2) din Legea nr. 677/2001, pentru datele care nu au caracter special (cum ar fi numele, prenumele, adresa poştală, de e-mail, nr. de telefon, imagine, voce), precum şi la art. 7, 8, 9 şi 10 din aceeaşi

lege, pentru datele cu caracter special (spre exemplu, datele privind originea rasială sau etnică, convingerile religioase, apartenenţa sindicală, starea de sănătate, codul numeric personal, faptele penale sau contravenţiile).

Faţă de textele legale sus menţionate, raportat la conţinutul adresei transmise, s-a precizat că prelucrarea datelor personale (imagine și voce) ale unor persoane fizice, considerate de asociaţia în cauză ca fiind cazuri umanitare, nu se încadrează în situațiile de excepție de la consimțământ.

În consecință, pentru realizarea scopului propus, respectiv postarea în mediul on-line de fotografii şi interviuri cu persoane considerate ca fiind cazuri umanitare, este necesar acordul persoanei al cărei caz este promovat sau, în situaţia minorului, al reprezentantului legal al acestuia, cu informarea prealabilă a persoanei ale cărei date vor fi prelucrate.

În acest context, s-a atras atenţia asupra faptului că informarea persoanelor vizate trebuie efectuată potrivit art. 12 din Legea nr. 677/2001, modificată şi completată. Totodată, s-a arătat că este necesară și respectarea reglementărilor din domeniul audiovizualului (Legea nr. 504/2002, Decizia nr. 220/2011) în ceea ce privește respectarea demnității umane și a dreptului la propria imagine.

În acelaşi timp, având în vedere că din conţinutul adresei transmise a reieșit că, în scopul păstrării unei evidenţe contabile a asociaţiei respective, aceasta intenţionează să colecteze date cu caracter personal înscrise în documentele de identitate aparţinând persoanelor beneficiare ale ajutoarelor umanitare, s-a precizat că este necesar să se respecte principiul proporţionalităţii datelor statuat de dispoziţiile art. 4 alin. (1) lit. c). din Legea nr. 677/2001. Referitor la intenţia efectuării de copii de pe cărţile de identitate aparţinând persoanelor sus menţionate, în acelaşi scop, respectiv al păstrării unei evidenţe contabile, s-a precizat că, prin Decizia nr. 132/2011 a

Preşedintelui Autorităţii naționale de supraveghere privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală, s-a interzis efectuarea şi reţinerea de copii de pe cartea de identitate sau de pe documente care le conţin, cu excepţia unor situaţii prevăzute la art. 2 din această decizie (consimţământul expres al persoanei vizate/dispoziţie legală expresă/avizul autorităţii de supraveghere).

b) Cu privire la publicarea de către Monitorul Oficial şi de diverse site-uri a unor legi sau hotărâri care conţin date cu caracter personal

Potrivit prevederilor Legii nr. 21/1991 privind cetățenia română, atât acordarea cetățeniei române (la cerere și/sau în cazul repatrierii), cât şi pierderea cetățeniei române (prin retragere sau aprobarea renunțării la aceasta) se fac prin hotărâri ale Guvernului, care se publică în Monitorul Oficial al României.

Aceste hotărâri conţin liste ale persoanelor pentru care s-a aprobat acordarea sau pierderea cetățeniei române.

Referitor la postarea de către alte site-uri a hotărârilor publicate în Monitorul Oficial ce conţin date cu caracter personal, s-a precizat că aceste date pot fi dezvăluite doar în cazul în care persoana vizată şi-a dat în mod expres şi neechivoc consimţământul, potrivit art. 5 alin. (1) din Legea nr. 677/2001 sau în condițiile de excepție prevăzute de alin. (2) al aceluiași articol.

În privinţa solicitării de verificare, rectificare a conţinutului documentelor publicate în Monitorul Oficial, s-a precizat că această atribuţie este în sarcina autorităţii emitente a actului normativ trimis spre publicare în monitor.

Cu toate acestea, faţă de conţinutul adresei, s-a precizat că persoana are dreptul de a solicita administratorului paginii de Internet respective (www.lege5.ro, www.legislatie.just.ro, www.monitoruloficial.ro) ştergerea datelor care consideră că îi aparţin, în temeiul art. 15 din Legea nr. 677/2001 (dreptul de opoziţie). Pentru exercitarea acestui drept, persoana vizată va înainta operatorului o cerere întocmită în formă scrisă, datată şi semnată, în care poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal. Operatorul este obligat să comunice măsurile adoptate în urma exercitării

acestui drept, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului de expediere a răspunsului.

În aceeași adresă s-a precizat că nerespectarea drepturilor prevăzute de Legea nr. 677/2001 îi dă dreptul persoanei vizate a depune plângere la Autoritatea națională de supraveghere, cu respectarea art. 25 alin. (3) din Legea nr. 677/2001.

c) Cu privire la legalitatea implementării unor aplicații de monitorizare a comportamentului consumatorilor

S-a subliniat că principiile privind prelucrarea datelor personale stabilite de art. 4 din Legea nr. 677/2001 se impun a fi respectate, indiferent dacă prelucrarea datelor are loc pe baza consimțământului persoanelor vizate sau în temeiul excepțiilor de la consimțământ prevăzute de lege.

În consecință, datele trebuie să fie cele strict necesare îndeplinirii scopului (minimum de date necesare), aspect ce solicită o analiză prealabilă din partea operatorului, prin evaluarea necesităţii colectării datelor respective, în scopul evitării unor ingerinţe în viaţa privată a persoanei vizate şi găsirea unor soluții alternative, mai puțin intruzive.

Referitor la consimţământ, exercitarea autonomiei de voinţă a persoanei vizate în privinţa prelucrării datelor sale înseamnă că, în orice moment, aceasta își poate retrage consimţământul pentru prelucrarea tuturor sau a unora dintre datele sale personale, fără consecinţe negative asupra sa, raportat la activitatea de marketing.

În măsura în care operatorul invocă interesul legitim, este necesară, pe de o parte, argumentarea temeinică a acestuia, pentru a motiva și dovedi prevalența interesului său asupra drepturilor și libertăților persoanei vizate, iar pe de altă parte, informarea persoanei vizate cu privire la prelucrarea datelor sale.

Informarea persoanelor vizate trebuie realizată indiferent de condițiile de legitimitate a prelucrării datelor, potrivit art. 12 din Legea nr. 677/2001, modificată şi completată. În cadrul acestei informări, persoanelor fizice trebuie să li se aducă la cunoștință toate condițiile prelucrării datelor, inclusiv drepturile de opoziţie, acces şi intervenție, precum și condițiile exercitării acestora, pentru a consimți la o anumită prelucrare în cunoștință de cauză.

Conform dispoziţiilor art. 15 din Legea nr. 677/2001, modificată şi completată, dreptul de opoziţie reprezintă dreptul persoanei vizate de a se opune, în orice moment, la prelucrarea datelor sale, din motive întemeiate şi legitime, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată, prelucrarea nu mai poate viza datele în cauză.

Potrivit acelorași dispoziții legale de mai sus, persoana vizată are dreptul de a se opune în orice moment, în mod gratuit şi fără nicio justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terţ, sau să fie dezvăluite unor terţi într-un asemenea scop.

Garanția acestui drept este expresia prevalenței dreptului de opoziție asupra intereselor economice ale operatorului, mai ales în condițiile folosirii noilor tehnologii pentru activitatea sa, așa cum este cazul de față.

De asemenea, s-a precizat că, potrivit art. 53 din Constituție, exercițiul unor drepturi sau al unor libertăți poate fi restrâns numai prin lege. Dreptul la viață privată este unul dintre drepturile care se înscriu în categoria drepturilor fundamentale ale persoanei fizice, garantat și ocrotit de Legea fundamentală.

Astfel, în ceea ce privește restrângerea unor drepturi, art. 16 din Legea nr. 677/2001 stabilește în ce condiții poate avea loc aceasta, excepţiile fiind aplicabile însă numai pentru domeniul dreptului penal și numai pentru o perioadă limitată de timp, după care operatorii vor lua măsurile necesare pentru a asigura respectarea drepturilor persoanelor vizate și vor înștiința Autoritatea națională de supraveghere asupra acestor situații.

Colectarea datelor unor persoane fizice prin intermediul unor tipuri de software specializate constituie o ingerință în dreptul fundamental la viață privată a acestora, poate conduce la atingeri grave aduse dreptului la viaţă privată și poate reprezenta riscuri majore pentru protecţia datelor lor cu caracter personal, cu atât mai mult cu cât persoanele vizate pot fi inclusiv persoane cu dizabilități și minori.

În plus s-a subliniat faptul că, înainte de crearea și implementarea unui astfel de sistem de colectare şi prelucrare a datelor, se impune necesitatea asigurării unui nivel adecvat de protecție a datelor (respectarea principiului privacy by design), cu atât mai mult cu cât se specifică faptul că ”aplicațiile menționate funcționează împreună cu datele obținute din înregistrări video efectuate în prealabil sau simultan”.

În concluzie, față de situațiile prezentate, întrucât operatorul prestabilește scopurile și mijloacele de prelucrare a datelor, cu caracter obligatoriu, fără consultarea persoanei vizate, acesta nu se mai poate prevala de condiția de legitimitate privind obținerea consimțământului persoanei vizate.

De asemenea, în ceea ce privește condiția existenței interesului legitim, prelucrarea nu se poate întemeia pe această excepție, decât dacă sunt îndeplinite toate condițiile mai sus precizate, în special asigurarea respectării drepturilor persoanelor vizate (în primul rând a dreptului la informare), precum și a celorlalte garanții privind o prelucrare corectă și legală a datelor.

Cât privește dispozițiile art. 5 alin. (2) lit. b) din Legea nr. 677/2001, s-a precizat că acestea nu sunt incidente scopurilor de reclamă, marketing și publicitate.

În plus, s-a subliniat faptul că supravegherea tehnică prin camere de supraveghere audio/video, fără ca persoana vizată să aibă cunoștință de acest fapt, nu poate avea loc decât potrivit Codului de procedură penală, numai în anumite condiții stabilite expres de acest cod. În același sens stipulează și dispozițiile art. 5 alin. (2) și (3) din Decizia nr. 52/2012, potrivit cărora camerele de supraveghere video se montează în locuri vizibile, fiind interzisă utilizarea mijloacelor de supraveghere ascunse, cu excepția situațiilor prevăzute de lege.

Prin urmare, astfel de tipuri de software specializate, cum sunt cele prezentate în conținutul adresei, nu pot fi implementate de către operatorii din domeniul reclamei, marketingului și publicității, decât cu respectarea tuturor prevederilor legale naționale și europene privind protecția datelor personale.

Referitor la reglementările europene în materie, s-a precizat că proiectul de Regulament privind protecția datelor prevede faptul că orice persoană vizată ar trebui să aibă dreptul de a cunoaște și de a i se comunica în special în ce scopuri sunt prelucrate datele, dacă este posibil pentru ce perioadă, identitatea destinatarilor datelor, care este logica de prelucrare automată a datelor și care ar putea fi, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări.

d) Cu privire la dezvăluirea de date ale debitorilor persoane fizice

În ceea ce privește dezvăluirea de către organele fiscale a datelor debitorilor persoane fizice, s-a subliniat că operațiunile de prelucrare menționate nu pot fi efectuate decât dacă

există consimţământul persoanei vizate sau numai în condiţiile legale de excepţie de la consimţământ, de strictă interpretare şi aplicare, cu respectarea principiului proporţionalităţii scopului, consacrat de art. 4 alin. (1) lit. b) din Legea nr. 677/2001.

Prin hotărârea din Cauza Smaranda Bara și alții (C-201/14), Curtea de Justiție a Uniunii Europene a statuat faptul că articolele 10, 11 și 13 din Directiva 95/46/CE trebuie interpretate în sensul că se opun unor măsuri naționale, care permit unei autorități a administrației publice a unui stat membru să transmită date personale unei alte autorități a administrației publice, care va prelucra ulterior aceste date, fără ca persoanele vizate să fi fost informate despre această transmitere sau despre această prelucrare.

Așadar, cerința prelucrării corecte a datelor personale prevăzută la art. 12 din Legea nr. 677/2001, ce implementează art. 6 din Directiva 95/46/CE, obligă o autoritate a administrației publice să informeze persoanele vizate despre transmiterea acestor date unei alte autorități a administrației publice, în vederea prelucrării de către aceasta din urmă în calitate de destinatar al datelor menționate.

Raportat la acest aspect, Autoritatea națională de supraveghere a subliniat faptul că dreptul garantat de art. 12 din Legea nr. 677/2001 trebuie respectat de către toți operatorii de date cu caracter personal, indiferent de condițiile de legitimitate a prelucrării datelor, respectiv la consimțământ sau în baza unor excepții, conform prevederilor art. 5 din Legea nr. 677/2001.

Autoritatea națională de supraveghere a atras atenția asupra necesității respectării dreptului la informare al persoanei vizate, atât sub aspectul informațiilor ce trebuie, în mod obligatoriu, făcute cunoscute acesteia, cât și al exercitării ulterioare a celorlalte drepturi de către persoana vizată, precum dreptul de acces la date, de intervenţie asupra datelor, de opoziţie, pentru a da posibilitatea persoanei respective să utilizeze mijloacele legale în consecință.

S-a atras atenția că Legea nr. 677/2001 stabilește în sarcina operatorilor de date cu caracter personal anumite obligaţii, printre care cea de efectuare a prelucrărilor în condiții de legitimitate (art. 5), de informare a persoanelor vizate (art. 12) și de respectare a drepturilor persoanelor fizice ale căror date le prelucrează (art. 13-18), precum și obligația de asigurare a confidenţialităţii şi securităţii prelucrării datelor (art. 19 și art. 20).

S-a subliniat că toate cele de mai sus nu au fost luate în considerare la emiterea Ordinului nr. 558/2016 privind Procedura de publicare a listelor debitorilor care înregistrează obligaţii fiscale restante, precum şi cuantumul acestor obligaţii, în contextul în care art. 11 alin.

(10) din Legea nr. 207/2015 - Codul de procedură fiscală prevede: ”Prelucrarea datelor cu caracter personal de către organele fiscale centrale şi locale se realizează cu respectarea prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare.”

S-a precizat faptul că Autoritatea națională de supraveghere nu a fost consultată, în conformitate cu dispozițiile art. 21 alin. (3) lit. h) din Legea nr. 677/2001, cu privire la proiectul Ordinului nr. 558/2016 privind Procedura de publicare a listelor debitorilor care înregistrează

obligaţii fiscale restante, precum şi cuantumul acestor obligaţii.

Față de conținutul acestui Ordin, s-a subliniat că nu conține prevederi referitoare la respectarea de către ANAF a obligațiilor prevăzute de art. 12 din Legea nr. 677/2001, a drepturilor persoanei vizate sau a măsurilor de securitate a prelucrărilor.

S-a considerat că, raportat la art. 162 din Codul de procedură fiscală, în aplicarea principiului proporționalității și minimizării datelor, prevăzut de art. 4 din Legea nr. 677/2001, este excesivă publicarea și a localității domiciliului fiscal al persoanei vizate.

e) Cu privire la condițiile legale privind aplicațiile cu date biometrice

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

De asemenea, aceeaşi lege menţionată anterior stabileşte în mod expres şi anumite situaţii de excepţie de la obligativitatea obţinerii consimţământului în cazul prelucrării datelor personale. Printre aceste cazuri de excepţie, reglementate de art. 5 alin. (2) din Legea nr. 677/2001, modificată şi completată, se numără şi cel în care prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului ori în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate.

Principiile privind prelucrarea datelor personale stabilite de art. 4 din Legea nr. 677/2001 se impun a fi respectate, indiferent dacă prelucrarea datelor are loc pe baza consimțământului persoanelor vizate sau în temeiul excepțiilor de la consimțământ prevăzute de lege.

Prin urmare, s-a precizat că se poate recurge la o prelucrare a datelor biometrice, în temeiul dispoziţiilor legale de mai sus, dar numai dacă această măsură este proporţională cu riscurile cu care se confruntă operatorul şi determină luarea unei asemenea măsuri intruzive în viaţa privată a persoanelor vizate. În acelaşi timp, trebuie să se ţină cont şi de interesele, drepturile şi libertăţile acestora. În funcție de specificul prelucrării, se impune identificarea unei modalități alternative de îndeplinire a scopului propus, prin identificarea altor date, a căror prelucrare nu prezintă riscuri pentru viața privată a persoanei fizice respective.

În măsura în care implementarea unui astfel de sistem afectează drepturile persoanelor vizate în calitate de angajați, în plus faţă de dispoziţiile Legii nr. 677/2001, modificată şi completată, trebuie respectate şi cele prevăzute de Codul muncii sau alte reglementări care vizează statutul acestora. În acest sens, anterior implementării sistemului se impune o justificare temeinică a luării acestei măsuri concomitent cu consultarea sindicatului sau a reprezentanţilor salariaţilor.

În acest context s-a precizat că, în mai multe situații în care angajatorii au implementat, de exemplu, un sistem de efectuare a pontajului pe baza datelor biometrice (amprentele) ale angajaților, fără o justificare temeinică a necesității luării acestei măsuri, aceștia au fost sancționați de către Autoritatea națională de supraveghere, iar instanțele de judecată au menținut măsurile luate de instituția noastră.

f) Cu privire la constituirea și publicarea unei evidențe a anumitor salariați

O persoană fizică a solicitat un punct de vedere cu privire la constituirea unei baze de date cu salariați-problemă conținând nume, prenume, vârsta, fotografie, orașul de domiciliu, funcția ocupată, faptele și orice alte informații considerate utile, ale unor salariați care au creat anumite probleme la locul de muncă, precum și postarea acesteia pe internet.

Potrivit dispoziţiilor art. 5 alin. (1) al Legii nr. 677/2001, modificată şi completată, principiul de bază ce guvernează prelucrarea datelor personale (inclusiv colectarea datelor și dezvăluirea acestora către terți) este consimţământul persoanei vizate, dat în mod expres şi neechivoc.

În mod excepţional însă, datele cu caracter personal pot fi prelucrate de către un operator, fără consimţământul persoanei vizate, în mai multe situaţii de excepţie, de strictă interpretare şi aplicare, reglementate de art. 5 alin. (2) din Legea nr. 677/2001.

Aşadar, datele cu caracter personal la care s-a făcut referire în conținutul adresei transmise (nume, prenume, vârsta, imaginea, orașul de domiciliu, funcția, ocupația - ale unor angajați/foști angajați ai unor entități) nu pot fi dezvăluite de angajatori/foști angajatori (ce au calitatea de operatori de date, potrivit definiției date de Legea nr. 677/2001), decât în situaţia în care există consimţământul persoanei vizate ori, în mod excepțional, numai în condiţiile legale

de excepţie de la consimţământ, de strictă interpretare şi aplicare, cu respectarea principiului proporţionalităţii scopului.

În plus, s-a subliniat că art. 10 din Legea nr. 677/2001 legitimează prelucrarea datelor referitoare la fapte penale sau infracţiuni ori la sancţiuni administrative sau contravenţionale aplicate persoanei vizate, numai de către sau sub controlul autorităţilor publice, în limitele puterilor ce le sunt conferite prin lege şi în condiţiile stabilite de legile speciale care reglementează aceste materii.

Față de cele de mai sus, având în vedere şi:

- considerentul (53) din Directiva 95/46/CE potrivit căruia anumite prelucrări pot să prezinte riscuri specifice pentru drepturile şi libertăţile persoanelor vizate prin însăşi natura lor, domeniul de aplicare sau scopurile lor, cum ar fi excluderea persoanei de la beneficiul unui drept, unei prestaţii sau unui contract;

- opinia unitară a autorităţilor de supraveghere din statele membre exprimată în Documentul de lucru privind listele negre nr. 65 din 3 octombrie 2002 adoptat de Grupul de Lucru Art. 29 pentru protecţia datelor al Comisiei europene, potrivit căreia listele care conţin date ale angajaţilor sau ale candidaţilor la diverse locuri de muncă privind comportamentul profesional reprobabil al acestora pot avea un impact foarte mare asupra intereselor persoanelor vizate aflate pe aceste „liste negre”, motiv pentru care ele necesită o protecţie specială;

- prevederile art. 8 din Convenţia pentru apărarea drepturilor omului şi libertăţilor fundamentale care proclamă respectarea vieţii private şi de familie a oricărei persoane şi cele

ale art. 26 din Constituţie care garantează respectarea dreptului fundamental la viaţă intimă, familială şi privată, drept confirmat şi în Carta Drepturilor Fundamentale a Uniunii Europene;

- necesitatea asigurării unei protecţii eficiente a dreptului la viaţă privată a angajaților și respectarea principiului proporţionalităţii prelucrărilor;

s-a subliniat că prelucrarea datelor personale în scopul menționat, respectiv crearea unei ”liste negre” cu ”salariați-problemă”, este o prelucrare excesivă raportat la scopul urmărit și la prevederile art. 4 din Legea nr. 677/2001.

g) Cu privire la prelucrarea datelor prin sisteme de supraveghere video

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

Autoritatea naţională de supraveghere, în contextul susţinerilor societăţii şi al necesităţii asigurării unei protecţii eficiente a dreptului la viaţă privată al angajaţilor, raportat la caracterul determinat, explicit şi legitim al scopului şi al proporţionalităţii prelucrării, faţă de solicitarea de acordare a avizului în temeiul art. 8 alin. (3) din Decizia nr. 52/2012, a considerat că elementele justificative prezentate nu justifică acordarea avizului.

Astfel, s-a apreciat că nu există argumente pentru efectuarea, prin utilizarea unui sistem de supraveghere video, de prelucrări de date cu caracter personal (imagini) ale angajaților în birourile Societății Profesionale Notariale, raportat la activitatea desfășurată și la obligațiile legale ale acestei societăți.

S-a precizat că, din textul adresei transmise, rezulta că solicitarea de instalare a mijloacelor de înregistrare video se justifica, pentru a preveni eventuale infracțiuni de furt, care s-au înregistrat atât la biroul respectiv, cât și la sediul altor birouri notariale.

Așadar, raportat la necesitatea asigurării unei protecţii eficiente a dreptului la viaţă privată a angajaţilor și la caracterul determinat, explicit şi legitim al scopului şi al proporţionalităţii prelucrării datelor lor cu caracter personal, s-a apreciat că elementele prezentate în adresa transmisă nu îndeplineau condiţiile stipulate de art. 8 din Decizia nr. 52/2012.

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

În anul 2016 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-13/16** privind interpretarea art. 7 lit. f) din Directiva 95/46/CE privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;

- Cauza C-73/16 privind interpretarea art. 7, 8 şi 47 din Carta drepturilor fundamentale a Uniunii Europene, precum şi a art. 1 alin. (1), a art. 7 lit. e), a art. 13 alin. (1) lit. e) şi f) şi a art. 17 alin. (1) din Directiva 95/46/CE;

- Cauza C-434/16 privind interpretarea Hotărârii Digital Rights Ireland and Seitlinger a Curții de Justiție, pronunțată în cauzele conexate C-293/12 și C-594/12 (inclusiv, în special, punctele 60-62 din aceasta).

Secţiunea a 3-a Activitatea de reprezentare în faţa instanţelor de judecată

Având în vedere finalizarea unor acțiuni în instanță în mod favorabil pentru instituția noastră, ca urmare a promovării acestora de către unii operatori sancționați de Autoritatea națională de supraveghere pe parcursul anului 2016, prezentăm mai jos câteva cazuri relevante:

- **Hotârâre pronunţată într-un litigiu privind transmiterea de către o instituție bancară nefinanciară a datelor unor debitori**

Autoritatea națională de supraveghere a fost sesizată de o persoană fizică asupra faptului că, în urma încheierii unui contract de card de credit, figurează cu date negative raportate la SC Biroul de Credit SA de instituția finaciară nebancară, deşi nu a fost înştiinţată în prealabil cu 15 zile înainte de data transmiterii datelor sale la SC Biroul de Credit SA. Persoana a menţionat că

s-a adresat acestei instituții prin mai multe petiţii pe e-mail, solicitând ștergerea datelor sale de la SC Biroul de Credit SA, dar este nemulţumită de răspunsurile primite.

Instituția noastră a demarat o investigație la entitatea respectivă, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001, inclusiv sub aspectul celor semnalate.

Autoritatea națională de supraveghere a emis un proces-verbal de constatare/sancționare prin care s-a constatat săvârşirea de către operatorul controlat a faptei contravenţionale de prelucrare nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 8 alin. (2) din Decizia ANSPDCP nr. 105/2007, precum și a art. 12 din Legea nr. 677/2001. Astfel, instituția financiară nebancară a transmis date negative la SC Biroul de Credit SA, timp de doi ani, fără să prezinte dovezi privind informarea prealabilă a persoanei vizate, cu 15 zile înainte de transmiterea datelor sale, în niciuna din modalităţile prevăzute de art. 8 alin. (2) din Decizia ANSPDCP nr. 105/2007.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat, acesta solicitând anularea procesului-verbal și obligarea instituției noastre la plata cheltuielilor de judecată.

Instanța a respins plângerea operatorului, apreciind că ”agentul constatator a realizat o individualizare corectă a sancțiunii contravenționale prin aplicarea sancțiunii avertismentului.”

Împotriva sentinţei instanței de fond instituția financiară nebancară a declarat apel, respins de instanța superioară, soluţia rămânând definitivă în favoarea Autorității naționale de supraveghere.

Decizia irevocabilă a instanței a confirmat abordarea Autorității naționale de supraveghere de respectare a condițiilor de legitimitate a prelucrării datelor cu caracter personal.

❖ Hotârâre pronunţată într-un litigiu privind prelucrarea nelegală de date cu caracter personal de către o unitate hotelieră

Autoritatea naţională de supraveghere a efectuat o investigaţie la un operator din domeniul hotelier, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 şi ale Legii nr. 506/2004. În urma investigației efectuate s-a constatat faptul că operatorul controlat prelucrează date în scopul oferirii de servicii hoteliere și de turism, precum și în scop de reclamă, marketing şi publicitate.

Autoritatea națională de supraveghere a emis un proces-verbal de constatare/sancționare prin care s-a constatat săvârşirea de către operatorul controlat a următoarelor fapte contravenţionale:

- omisiunea de a notifica şi notificarea cu rea-credinţă, contravenție prevăzută de art. 31 din Legea nr. 677/2001, sub forma omisiunii de a efectua notificarea în condiţiile art. 22 din Legea nr. 677/2001, întrucât nu a notificat prelucrarea datelor cu caracter personal pe care o realizează în scop de servicii hoteliere şi de turism, în scop de reclamă, marketing şi publicitate şi în scop de supraveghere video, deşi avea această obligaţie anterior începerii prelucrării;
- prelucrarea nelegală a datelor cu caracter personal, contravenție prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea prevederilor art. 12 din Legea nr. 677/2001, modificată şi completată, şi ale art. 5 alin. (1) din Legea nr. 677/2001, modificată şi completată, deoarece operatorul, la data întocmirii procesului–verbal, nu a putut prezenta nicio dovadă a informării persoanelor vizate conform art. 12 din Legea nr. 677/2001, pentru prelucrările de date cu caracter personal pe care le efectuează în scop de servicii hoteliere și de turism și în scop de reclamă, marketing şi publicitate;
- neîndeplinirea obligaţiilor privind confidenţialitatea şi aplicarea măsurilor de securitate, contravenție prevăzută de art. 33 din Legea nr. 677/2001, modificată și completată, prin neîndeplinirea obligațiilor privind aplicarea măsurilor de securitate și de păstrare a confidențialității prelucrărilor prevăzute de art. 20 din Legea nr. 677/2001, modificată și completată, deoarece operatorul nu a întocmit și implementat o politică/procedură privind măsurile minime de securitate a prelucrărilor de date cu caracter personal pe care le efectuează, iar angajații cu atribuții referitoare la prelucrarea datelor cu caracter personal nu au fost instruiți cu privire la prevederile Legii nr. 677/2001 și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal;
- nerespectarea condiţiilor prevăzute de art. 4 alin. (5) din Legea nr. 506/2004, modificată şi completată, întrucât operatorul, la nivelul site-ului propriu, pentru informaţiile stocate şi accesate la nivelul echipamentului terminal al utilizatorului nu a îndeplinit în mod cumulativ condiţiile prevăzute de art. 4, alin. (5) lit. a) şi b) din Legea nr. 506/2004, modificată şi completată, respectiv obţinerea acordului utilizatorului în cauză pentru cookie-urile existente la nivelul website-ului şi furnizarea, anterior exprimării acordului, a informaţiilor privind scopul general al procesării informaţiilor

stocate, durata de viaţă, informaţiile stocate şi accesate, precum și permiterea stocării şi/sau accesului unor terţi la informaţiile stocate în echipamentul terminal al utilizatorului, contravenţie prevăzută de art. 13, alin. 1 lit. i) din Legea nr. 506/2004, modificată şi completată.

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

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat sub aspectul contravențiilor reținute în sarcina sa.

Plângerea operatorului a fost respinsă prin hotărâre judecătorească definitivă.

Astfel, instanța de apel a apreciat că ”Faptele săvârșite sunt agravate, întrucât este vorba de un cumul de abateri, iar legiuitorul nu a avut în vedere producerea unui prejudiciu, ci sancționarea unui eventual pericol social (…)”.

Decizia definitivă a instanței de apel confirmă corecta interpretare dată dispozițiilor prevederilor Legii nr. 677/2001 şi ale Legii nr. 506/2004 de către reprezentanții Autorității naționale de supraveghere și, în consecință, corecta individualizare a sancțiunilor reținute în sarcina operatorului sus menționat.

- **Hotârâre pronunţată într-un litigiu privind prelucrarea de date biometrice de către o instituție publică**

Autoritatea națională de supraveghere a efectuat o investigaţie din oficiu la un operator din domeniul public referitor la o situaţie de presă, care menționa că pontajul a sute de funcţionari din cadrul operatorului controlat se realiza pe bază de amprentă.

Ca urmare a controlului efectuat, Autoritatea națională de supraveghere a constatat că accesul în instituţie a unei părți dintre angajaţii operatorului se realiza pe baza amprentei digitale personale.

Anterior procurării şi punerii în funcţiune a sistemului de pontaj electronic operatorul utiliza carduri de acces pentru angajaţi în vederea accesului în instituţie.

Pentru punerea în aplicare a sistemului de pontaj electronic operatorul a colectat datele biometrice (amprente) ale angajaţilor. Astfel că, prin intermediul sistemului de pontaj electronic

erau înregistrate orele de începere şi terminare a programului de lucru, precum şi intrări/ieşiri din instituţie.

La nivelul operatorului investigat, la data controlului, erau angajate aproximativ 500 de persoane, însă doar jumătate dintre aceştia utilizau pentru pontaj cardul de acces.

De asemenea, la data controlului, s-a constatat că erau înregistrate în sistem un număr de 755 de persoane, din care doar 500 erau angajate, iar celelalte figurau ca fiind pensionate şi/sau ca având încetat raportul de muncă cu operatorul. Cu toate acestea sistemul reţinea datele persoanelor (respectiv: numărul unic atribuit atunci când era angajatul operatorului, numele, prenumele, data şi ora intrării, data şi ora ieşirii şi CNP), deşi nu mai aveau raporturi de muncă cu respectivul angajator.

Operatorul investigat nu a prezentat niciun document de aprobare a sistemului de pontaj electronic şi nici de evaluare a necesității implementării acestui sistem.

La data controlului, nu s-a făcut dovada informării în prealabil a angajaţilor asupra sistemului de pontaj electronic, nu s-a făcut dovada obţinerii consimţământului angajaţilor privind implementarea acestui sistem, nu se stabilise o perioadă de stocare a datelor, nu erau adoptate suficiente măsuri de confidențialitate și securitate a datelor prelucrate (date biometrice), astfel că operatorul a încălcat dispoziţiile Legii nr. 677/2001.

Faptele săvârşite de operator au fost sancţionate contravenţional cu amendă, iar procesul-verbal de constatare/sancţionare contravenţională a fost contestat în instanţă.

Instanţa, analizând probatoriul administrat în cauză, a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit, astfel că au fost menţinute sancţiunile contravenţionale aplicate.

Hotărârea a rămas definitivă prin respingerea recursului declarat de operator.

- **Hotârâre pronunţată într-un litigiu privind supravegherea video a angajaților în birouri de către o instituție din domeniul public**

Autoritatea națională de supraveghere a fost sesizată de o persoană fizică asupra faptului că o instituție din domeniul public, în calitate de angajator, i-a prelucrat datele cu

caracter personal, imagini, prin intermediul unui sistem de supraveghere video, instalat inclusiv în spaţiile de lucru (birouri), fără respectarea prevederilor legale.

A fost demarată o investigație la instituția respectivă, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001, inclusiv sub aspectul celor mai sus precizate.

Autoritatea națională de supraveghere a emis un proces-verbal de constatare/sancționare prin care s-a constatat săvârşirea de către operatorul controlat a următoarelor fapte contravenţionale:

- omisiunea de a notifica şi notificarea cu rea-credinţă, prevăzută de art. 31 din Legea nr. 677/2001, sub forma omisiunii de a efectua notificarea în condiţiile art. 22 din această lege;

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, întrucât operatorul nu a realizat informarea persoanelor vizate ale căror imagini sunt prelucrate prin intermediul sistemului de supraveghere video instalat, în conformitate cu prevederile art. 11 din Decizia nr. 52/2012;

- prelucrarea nelegală a datelor cu caracter personal, prevăzută de art. 32 din Legea nr. 677/2001, întrucât operatorul a prelucrat în mod excesiv datele personale, respectiv imaginea angajaţilor săi, prin intermediul camerelor video instalate în 9 birouri şi într-o sală de audienţe, cu încălcarea art. 4 alin. (1) lit. a) şi c) din Legea nr. 677/2001, raportat la art. 8 din Decizia nr. 52/2012.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de instituția din domeniul public sancționată, aceasta solicitând anularea procesului-verbal.

Instanța a respins plângerea, reținând, cu privire la reclamantă, că, pe de o parte la data efectuării controlului, aceasta nu realizase notificarea prealabilă, potrivit art. 22 din Legea nr. 677/2001 iar, pe de altă parte, monitorizarea persoanelor, spațiilor și bunurilor efectuată în cadrul operatorului, chiar dacă ar fi fost realizată doar în scopul asigurării pazei obiectivului, bunurilor și persoanelor și prevenirii unor fapte de genul sustragerii unor bunuri, nu înlătură obligația reclamantei de notificare prevăzută de art. 22 din Legea nr. 677/2001, deoarece această supraveghere comportă riscuri pentru drepturile și libertățile fundamentale ale angajaților, mai ales pentru dreptul la viață privată.

Referitor la cea de a doua contravenție, instanța a constatat că aceasta există și a fost în mod temeinic reținută în sarcina reclamantei de către agentul constatator, în condițiile în care reclamanta a luat decizia de a instala camerele de supraveghere fără a se consulta, în prealabil, cu autoritatea centrală în materie și fără a proceda la consultarea, în mod direct și explicit, a angajaților, ceea ce conduce la concluzia că s-a acționat în afara legislației în materie națională și internațională.

S-a reținut că susținerile reclamantei, în sensul că angajații ar fi cunoscut existența camerelor de supraveghere, deoarece li s-a comunicat, sub semnătură, decizia de instalare a sistemului de supraveghere, nu echivalează cu efectuarea unei informări directe a salariaților cu privire la prelucrarea datelor lor. Instanța a reținut că informarea trebuia realizată într-o manieră completă și clară.

Cât privește cea de a treia contravenție, instanța a constatat că aceasta a fost în mod legal și temeinic reținută în sarcina reclamantei, odată ce angajații sunt monitorizați și supravegheați permanent, având camere de supraveghere instalate în birouri și în sala de audiențe, resimțind astfel o presiune implicită la locul de muncă și o stare de disconfort.

Instanța de fond a considerat că măsura luată de reclamantă, de instalare a acestor camere de supraveghere, este disproporționată față de scopul declarat și anume asigurarea pazei obiectivului, bunurilor și persoanelor și prevenirea unor fapte de genul sustragerii unor bunuri, în raport cu respectarea drepturilor fundamentale ale angajațior acesteia.

Împotriva sentinţei instanței de fond reclamantul a declarat apel, pe care instanța superioară l-a respins, soluţia fiind definitivă în favoarea Autorității naționale de supraveghere.

Secţiunea a 4-a Informare publică

În cursul anului 2016, Autoritatea naţională de supraveghere a continuat activităţile şi modalităţile de comunicare destinate informării publicului larg, cu privire la regulile specifice de prelucrare a datelor cu caracter personal.

Astfel, a fost organizată Ziua Europeană a Protecţiei Datelor, ca în fiecare an, eveniment de prestigiu ce a fost onorat de prezența unor reprezentanți de marcă ai autorităților publice centrale, ai societății civile și ai mediului privat.

Un rol important în activitatea de popularizare a domeniului protecției datelor l-a avut și difuzarea pe postul public de televiziune a unui clip de informare privind datele personale.

Pe tot parcursul anului, instituţia noastră a participat activ la cele mai importante evenimente cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private. La aceste reuniuni, reprezentanții Autorității naționale de supraveghere au clarificat anumite aspecte privind condițiile utilizării datelor, respectarea drepturilor persoanelor vizate şi asigurarea confidenţialităţii prelucrărilor de date cu caracter personal.

Dintre evenimentele semnificative în care instituţia noastră a fost implicată, reliefăm:

- ✓ **Ziua Europeană a Protecţiei Datelor**

În data de 28 ianuarie 2016 s-a marcat aniversarea a 35 de ani de la semnarea, la Strasbourg, în anul 1981, a Convenţiei 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, primul instrument legal adoptat în domeniul protecţiei datelor.

Pentru creșterea gradului de conştientizare a persoanelor fizice de pe întreg cuprinsul Europei asupra importanţei protecţiei datelor cu caracter personal şi a drepturilor specifice, autorităţile naţionale independente de protecţia datelor din statele europene organizează evenimente specifice.

În cinstea Zilei Europene a Protecţiei Datelor, Autoritatea naţională de supraveghere a organizat, la Palatul Parlamentului, un Simpozion care s-a bucurat de participarea prestigioasă a unor înalţi oficiali şi reprezentanţi ai justiţiei, mediului academic şi ai organizaţiilor nonguvernamentale.

Cu acest prilej, s-a prezentat și noul regim de notificare a prelucrărilor de date, stabilit prin Decizia nr. 200/2015 a Autorității naționale de supraveghere.

- ➢ **Conferința Data protection - soluții și responsabilități**

În data de 23 iunie 2016, la Camera de Comerț și Industrie a României, a avut loc Conferința Data protection - soluții si responsabilități, în deschiderea căreia a luat cuvântul ministrul Comunicațiilor și Societății Informaționale.

Cu ocazia acestui eveniment la care au participat numeroși invitați din mediul privat și public, s-au dezbătut implicațiile noului Regulament General privind Protecția Datelor, adoptat de Parlamentul European și Consiliu, iar reprezentanții Autorității naționale de supraveghere au prezentat noutățile aduse de noua reglementare europeană de directă aplicabilitate.

Desfășurată într-o manieră interactivă, această manifestare a evidențiat realul interes al persoanelor juridice pentru alinierea la exigențele noului Regulament (UE) 679/2016 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date, care se va aplica începând cu data de 25 mai 2018.

- **Reuniune în domeniul farmaceutic și medical**

În data de 28 noiembrie 2016, a avut loc un eveniment care a reunit numeroși reprezentanți ai societăților interesate de prelucrarea datelor în domeniul medical și farmaceutic.

În cadrul acestui eveniment, reprezentantul Autorității naționale de supraveghere a susținut o prezentare a principalelor reguli aplicabile în domeniul medical și a noutăților aduse de Regulamentul (UE) 2016/679 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, aplicabil începând cu data de 25 mai 2018.

La această reuniune, reprezentantul Colegiului Farmaciștilor din România a subliniat particularitățile și importanța utilizării datelor personale în domeniul farmaceutic, precum și dificultățile practice existente.

De asemenea, din partea mediului privat au fost subliniate măsurile interne necesare la nivelul fiecărui operator, pentru evaluarea riscurilor și asigurarea confidențialității datelor deținute, și s-au discutat măsurile ce se impun în perspectiva aplicării noului cadru normativ european.

- **Masa Rotundă în domeniul marketingului direct**

Reprezentanţii Autorităţii naţionale de supraveghere au participat la masa rotundă, organizată de Asociaţia Română de Marketing Direct (ARMAD), în data de 14 aprilie 2016.

În cadrul acestui eveniment, s-a abordat problematica prelucrării datelor personale în domeniul marketingului direct, inclusiv din perspectiva implicațiilor adoptării Regulamentului general privind protecția datelor, precum și a securității prelucrării datelor cu caracter personal, în contextul evoluţiei tehnologice actuale, raportat la utilizarea pe scară tot mai largă a internetului pentru comunicări comerciale.

Dincolo de aceste manifestări, pagina de internet a Autorității naționale de supraveghere a continuat să reprezinte un mijloc eficient și util de informare a operatorilor și publicului larg cu privire la evoluțiile din domeniu și la activitatea instituției noastre.

În scopul popularizării activităţii instituţiei şi 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 naţională de supraveghere. De asemenea, prin informaţiile furnizate telefonic şi în cadrul audienţelor acordate la sediul Autorităţii naţionale de supraveghere, s-a realizat informarea rapidă şi eficientă a cetăţenilor şi a operatorilor, în sensul că au fost oferite, într-o manieră directă, informaţii utile privind drepturile persoanelor vizate şi obligaţiile specifice operatorilor, lămuriri referitoare la condiţiile prelucrării datelor şi dezvăluirii acestora către terţi.

Articolele de presă publicate şi reportajele difuzate la principalele posturi de televiziune au reflectat interesul manifestat de mass-media faţă de domeniul protecţiei datelor cu caracter personal.

CAPITOLUL IV

ACTIVITATEA DE CONTROL ȘI DE SOLUȚIONARE A PLÂNGERILOR ȘI SESIZĂRILOR

Secțiunea 1. Prezentare generală

O componentă importantă a activității Autorității naționale de supraveghere o reprezintă monitorizarea și controlul legalității prelucrărilor de date personale, prin intermediul investigațiilor efectuate fie din oficiu, fie în scopul soluționării plângerilor și sesizărilor primite.

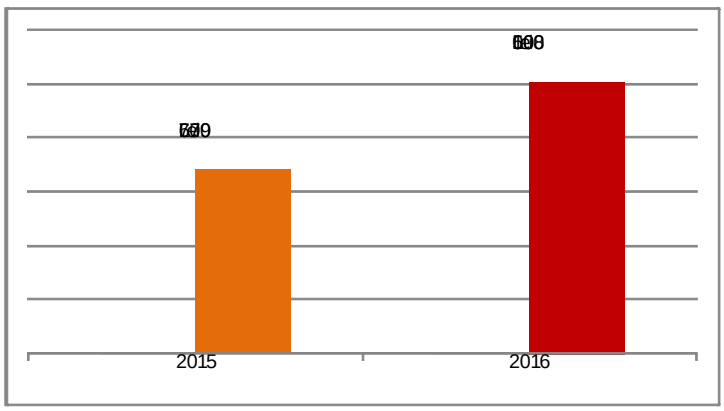
În anul 2016, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile în cadrul prelucrării datelor personale în sisteme de evidență de genul birourilor de credit, al prelucrării datelor biometrice și al prelucrării datelor de către autoritățile publice.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri considerabile a numărului acestora (**2014 plângeri și 188 sesizări**), în anul 2016 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, în cadrul sistemelor ce utilizează mijloace de supraveghere video sau în sectorul comunicațiilor electronice.

Numărul total de investigații efectuate de Autoritatea națională de supraveghere în 2016 este de **632**, în creștere cu peste 57% față de anul anterior.

În urma investigațiilor efectuate, au fost aplicate sancțiuni contravenționale constând în **193 amenzi și respectiv, 357 avertismente**.

Cuantumul total al amenzilor aplicate în 2016 a fost de **1.008.500 lei,** în creștere cu peste 48% față de anul anterior. (figura 1)



Secțiunea a 2-a: Investigații din oficiu

În anul 2016, Autoritatea naţională de supraveghere a întreprins **140 de acțiuni de control din oficiu**, atât în sectorul public cât și în sectorul privat. Astfel au fost aplicate **62 de avertismente**, respectiv **72 de amenzi** în cuantumul total de **648.500 lei.**

I. Respectarea prevederilor Legii nr. 677/2001 și ale Legii nr. 506/2004, referitor la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit (Instituții financiare bancare/nebancare)

Numărul mare de plângeri și sesizări primite, în 2015, de Autoritatea națională de supraveghere privind prelucrările de date cu caracter personal în sisteme de evidență de tipul birourilor de credit, a determinat demararea de investigații din oficiu la instituțiile financiare bancare și nebancare participante la sistemul de evidență al biroului de credit. Au fost supuse controlului un număr de **24 entități** care prelucrează date cu caracter personal în sisteme de evidenţă de tipul birourilor de credit, iar cuantumul total al sancțiunilor aplicate a fost de **382.000 lei**.

Controalele efectuate au vizat verificarea respectării prevederilor Legii nr. 677/2001 și ale Deciziei nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit, în special în ceea ce privește respectarea drepturilor persoanelor vizate.

În cadrul controalelor efectuate au fost solicitate informații referitoare la rapoartele de credit ale clienților care au fost raportați la biroul de credit cu debite restante, notificările (informările) transmise clienţilor cu privire la faptul că aceştia urmează să fie raportaţi, conform Deciziei nr. 105/2007, precum și dovada transmiterii acestor notificări.

Ca urmare a controalelor desfășurate, s-a constatat că majoritatea instituțiilor financiare bancare/nebancare supuse controlului realizează raportări la biroul de credit fără respectarea dispozițiilor legale, fiind sancționate 23 de entități din cele 24 controlate.

Principalele deficiențe constatate în activitatea de prelucrare a datelor cu caracter personal realizată de instituțiile financiare bancare/nebancare în sistemele de evidență de tipul birourilor de credit au fost următoarele:

- transmiterea de date negative cu încălcarea dispozițiilor art. 5 alin. (1) din Decizia nr. 105/2007, care prevede că datele negative se transmit către sistemele de evidență de tipul birourilor de credit după 30 de zile de la data scadenței;

- transmiterea de date negative cu încălcarea dispozițiilor art. 8 alin. (2) din Decizia nr. 105/2007, care prevede că datele negative se transmit către sistemele de evidență de tipul birourilor de credit numai după înștiințarea prealabilă a persoanei vizate, realizată de către participanți cu cel puțin 15 zile calendaristice înainte de data transmiterii;

- notificările (informările) transmise clienţilor cu privire la faptul că aceştia urmează să fie raportaţi cu debite restante nu respectă prevederile art. 9 alin. (1) din Decizia nr. 105/2007.

Față de aspectele constatate în urma controalelor efectuate, s-au recomandat instituțiilor financiare bancare și nebancare verificate următoarele:

- să adopte măsuri necesare în vederea respectării tuturor prevederilor Deciziei nr. 105/2007 pentru prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit;

- să întreprindă măsurile necesare pentru ştergerea informațiilor transmise ca date negative la biroul de credit, fără realizarea informării prealabile potrivit art. 8 alin. (2) din Decizia nr. 105/2007.

II. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal de tipul datelor biometrice

Autoritatea națională de supraveghere a dispus efectuarea de investigații la mai multe entități care prelucrau sau intenționau să prelucreze date cu caracter personal de tipul datelor biometrice. Investigațiile au fost dispuse din oficiu, atât în cadrul investigațiilor tematice, cât și ca urmare a sesizării celorlalte compartimente din cadrul Autorității naționale de supraveghere.

Datele biometrice fac parte din categoria datelor cu caracter personal , referitoare la caracteristicile fiziologice sau comportamentale ale unei persoane fizice, ce permit identificarea unică a acestuia.

Identificarea unei persoane cu ajutorul unui sistem biometric este, de obicei, procesul prin care se compară datele biometrice ale unei persoane (colectate în momentul identificării) cu o serie de modele biometrice stocate într-o bază de date, conform Avizului Grupului de Lucru Art.29 nr. 3/2012 privind progresele înregistrate de tehnologiile biometrice.

Conform aceleiași legislații, în cadrul prelucrărilor de date cu caracter personal, acestea trebuie să fie adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate.

Tehnologiile informatice care au la bază folosirea biometriei se utilizează în special în procesele de acces securizat în incinte prin deblocarea unor uși sau a unor turnicheți, pentru autentificarea accesului la resurse logice într-un sistem informatic, pentru deblocarea unor dispozitive (token-uri, carduri, laptop-uri etc.). Mecanismele de autentificare, identificare presupun realizarea unor operațiuni, cum ar fi înregistrarea și stocarea datelor șablonului, compararea rezultatelor citite la accesare, înregistrarea unor informații suplimentare (de ex. numele, prenumele sau un identificator al persoanei, eventual data și timpul accesării). În cadrul acestor sisteme informatice operațiunile efectuate asupra datelor biometrice trebuie să fie foarte bine securizate.

Tehnologiile biometrice presupun captarea datelor biometrice ale unei persoane, transformarea lor într-un tipar biometric (template/pattern), stocarea acestuia într-o bază de date și, ulterior, verificarea identității acelei persoane prin compararea tiparului biometric (proces de comparare a unei serii de date cu mai multe serii de date) cu caracteristica fiziologică/comportamentală corespunzătoare a individului. În cazul folosirii acestor tehnologii, stocarea și compararea datelor biometrice trebuie să fie foarte bine securizate.

În condițiile extinderii utilizării noilor tehnologii în societatea contemporană, trebuie analizat impactul acestora asupra respectării dreptului la viață privată și a principiilor de prelucrare a datelor cu caracter personal. Astfel, se pune problema caracterului invaziv și inoportun al acestor tehnologii raportat la anumite scopuri sau activități pentru care ar fi folosite. Un alt aspect de analizat este acela al riscului de securitate a bazelor de date care conțin datele biometrice.

Referitor la entitățile controlate, specificăm că majoritatea acestora au implementat sau intenționau să implementeze sisteme biometrice de autentificare, îndeosebi pentru realizarea pontajului sau/și accesului fizic în interiorul entității, bazate în special pe amprente sau recunoaștere facială.

Autoritatea națională de supraveghere a considerat că prelucrarea datelor biometrice este excesivă, raportat la scopurile menționate, aplicând atât amenzi, cât și recomandări privind identificarea unor măsuri mai puțin intruzive în viața persoanelor vizate. Totodată, Autoritatea națională de supraveghere a emis decizii privind încetarea prelucrării datelor biometrice și ştergerea datelor biometrice deja colectate.

A existat și un caz în care se intenționa folosirea unui sistem biometric prin care să se realizeze recunoașterea facială a unor persoane fizice, informație care ulterior ar fi trebuit să fie folosită pentru interzicerea accesului acelor persoane în interiorul entității.

Ca urmare a investigației efectuate, în acest caz, Autoritatea națională de supraveghere a considerat excesivă această prelucrare și a respins înscrierea în Registrul de evidență a prelucrărilor de date cu caracter personal a notificării transmise de către operator.

”În acest context, subliniem că instanțele judecătoreşti au confirmat constant abordarea Autorității naționale de supraveghere în sensul că prelucrarea datelor personale (amprente) ale angajaților nu se poate realiza decât pe baza unei analize temeinice privind necesitatea şi proporţionalitatea unor astfel de măsuri, iar angajatorul trebuie să identifice soluţii alternative care să aibă un impact mai redus asupra vieţii private a salariaţilor.

Raportat la acest aspect, în jurisprudenţa Curţii Europene a Drepturilor Omului referitoare la art. 8 din Convenţia pentru apărarea drepturilor omului şi libertăţilor fundamentale (dreptul la respectarea vieții private și de familie) instanța europeană a statuat faptul că protecţia oferită de acest articol ar fi diminuată în mod inacceptabil dacă folosirea de tehnici ştiinţifice moderne ar fi permisă cu orice preţ şi fără realizarea unui echilibru între beneficiile folosirii extensive a acestor tehnici şi interesele importante legate de viaţa privată (Cauza S. şi M. Marper contra Regatului Unit).” - comunicat de presă ANSPDCP, 08.12.2015**.**

III. Prelucrarea datelor cu caracter personal la nivelul sectorului public - autorități publice locale (consilii județene și primării de municipii)

În anul 2016 a fost efectuat un număr total de 33 acţiuni de control, în cadrul cărora au fost aplicate 15 avertismente și 13 amenzi. Cuantumul total al amenzilor aplicate în cadrul investigațiilor efectuate din oficiu, în cadrul acestei tematici, este de 29.500 lei.

Investigațiile efectuate au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum şi a dispoziţiilor Legii nr. 506/2004.

Obiectivele avute în vedere au fost următoarele:

- îndeplinirea obligaţiei de notificare cu privire la prelucrările efectuate prin mijloace de supraveghere video;
- modalităţile de prelucrare a datelor cu caracter personal în cadrul autorităților publice județene, în temeiul Legii nr. 677/2001;
- asigurarea drepturilor persoanelor vizate;
- îndeplinirea obligaţiei de asigurare a confidențialității și securității prelucrărilor.

Din investigațiile efectuate, s-a constatat că unitățile administrativ - teritoriale reprezentate prin primar sau prin președintele consiliului județean sunt scutite de depunerea formularelor de notificare a prelucrării datelor cu caracter personal, conform Deciziei Președintelui ANSPDCP 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. Conform art. 3 alin. (3) din decizia de mai sus, operatorii au obligația asigurării drepturilor persoanelor vizate, precum și a confidențialității și securității datelor.

Din investigațiile efectuate a reieșit că **unitățile administrativ - teritoriale reprezentate prin primar** prelucrează date cu caracter personal în îndeplinirea obligațiilor legale: resurse umane, soluționarea petițiilor și acordarea de audiențe, taxe și impozite, constatarea și sancționarea contravențiilor, colectare debite/recuperare creanțe, fond funciar, urbanism și amenajarea teritoriului, emitere autorizații, cadastru și publicitate imobiliară, evidența persoanelor, monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor publice/private etc.

De asemenea, a reieșit că **unitățile administrativ - teritoriale reprezentate prin președintele consiliului județean** prelucrează date cu caracter personal în îndeplinirea obligațiilor legale: resurse umane, soluționarea petițiilor și acordarea de audiențe, emitere certificate de urbanism etc. Operatorii au declarat că nu au fost înregistrate cereri pentru exercitarea drepturilor persoanelor vizate în condițiile Legii nr. 677/2001, modificată și completată.

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, în scopul de ”monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor publice/private”,

- 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.

Secţiunea a 3-a Activitatea de soluţionare a plângerilor şi sesizărilor

I. Prezentare generală

Scopul adoptării Legii nr. 677/2001, după cum reiese din art. 1, constă în garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială si privată, în legătură cu prelucrarea datelor personale și cu libera circulație a acestor date. Pentru realizarea acestui deziderat, una dintre principalele atribuții reglementate de lege în competența Autorității naționale de supraveghere este de apărare a acestor drepturi și libertăți ale persoanelor fizice, prin soluționarea plângerilor și a sesizărilor ce vizează încălcarea acestora.

Astfel, persoanele fizice care se consideră lezate prin modul de prelucrare a datelor lor personale de către operatorii de date sau persoanele împuternicite de aceștia pot adresa plângeri Autorităţii naționale de supraveghere. Legiuitorul a reglementat, de asemenea, posibilitatea ca orice persoană să poată sesiza Autoritatea națională de supraveghere în cazul în care constată că anumite prelucrări de date personale ar putea să contravină dispozițiilor legale.

Pentru ca plângerile să fie considerate admisibile, persoanele fizice trebuie să îndeplinească mai multe condiții stipulate în lege: să nu introducă anterior o acţiune în justiţie cu acelaşi obiect şi cu aceleași părți; să înainteze anterior (15 zile) o cerere cu acelaşi conţinut către operatorul de date, la care să nu fi primit un răspuns de la operator sau acesta să fie nesatisfăcător.

Astfel, deși unul dintre motivele de respingere a plângerilor a fost și în anul 2016 legat de neîndeplinirea procedurii legale prealabile de către petenţi, s-a constatat o creștere considerabilă a numărului plângerilor admisibile, ceea ce dovedește o mai bună informare a persoanelor vizate asupra condițiilor pe care trebuie să le îndeplinească o plângere adresată Autorității naționale de supraveghere.

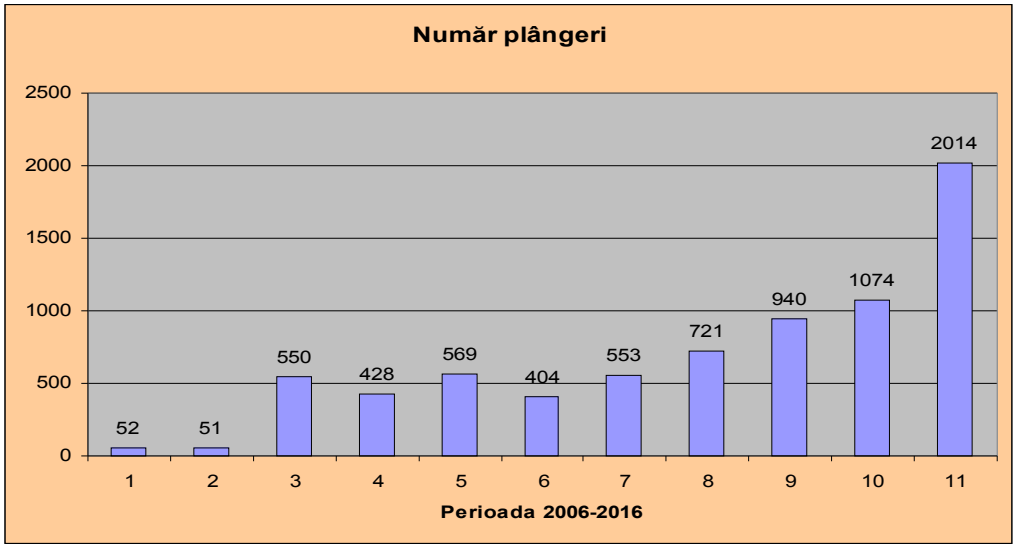
Printre alte considerente pentru care plângerile și sesizările nu au putut fi reținute în vederea efectuării unor demersuri de către autoritate pot fi enumerate: neprezentarea dovezilor în susţinerea aspectelor reclamate sau a calității de reprezentant al persoanei vizate (ex. lipsa împuternicirii avocațiale sau a unui mandat emis conform dispozițiilor legale aplicabile); sesizarea unor fapte în legătură cu care Autoritatea națională de supraveghere nu deține competenţa legală materială (ex. aspecte care țin de aplicarea legislației din domeniul protecției drepturilor consumatorilor sau din domeniul dreptului penal) sau teritorială să intervină (ex. prelucrări efectuate pe teritorul altui stat); imposibilitatea identificării exacte a entității reclamate (ex. neidentificarea certă a expeditorului unei comunicări comerciale electronice nesolicitate sau a deținătorului unui website).

În anul 2016, numărul petițiilor soluționate de compartimentul de specialitate din cadrul Autorității naționale de supraveghere aproape s-a dublat prin raportare la anul 2015. Astfel, au fost primite și soluționate un total de **2302 petiții** (față de 1335 în 2015), din care **2014 plângeri și 188 sesizări**. Din conținutul petițiilor, se poate constata că această creștere considerabilă a numărului petițiilor primite în cursul anului 2016 este rezultatul unei mai bune cunoașteri a atribuţiilor legale ale Autorităţii naționale de supraveghere de către persoanele fizice prin comparație cu perioada anterioară și al creșterii încrederii petiționarilor în acțiunile instituției noastre pentru respectarea drepturilor și libertăților lor.

Având în vedere evoluția exponențială a numărului plângerilor adresate în perioada 2006-2016 (numărul lor a crescut **de peste 38 de ori** față de primul an de activitate), considerăm ca fiind imperios necesară creșterea numărului de personal al Autorității naționale de supraveghere implicat în această activitate, mai ales în perspectiva implementării din 2018 a noului regulament general privind protecția datelor personale în toate statele membre ale Uniunii Europene. Potrivit viitorului cadru legislativ, orice persoană vizată va avea dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care își are

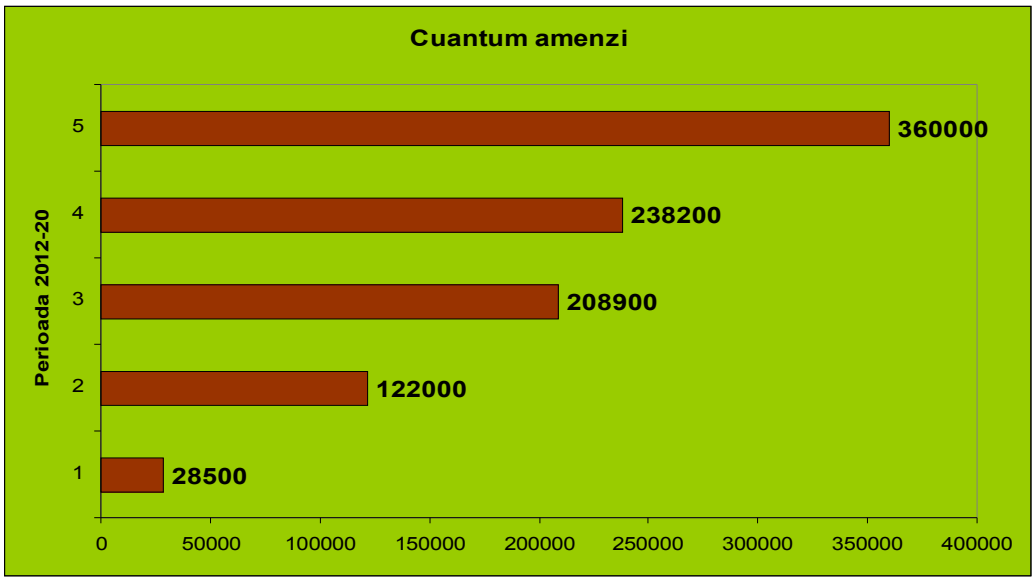
reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare a regulamentului.

Figura 1: Numărul plângerilor în perioada 2006-2016



Pentru soluţionarea plângerilor şi sesizărilor primite, **au fost efectuate 492 de investigații** din care **202 investigații pe teren și 290 de investigații în scris**; **în 85 de cazuri**, investigațiile au fost finalizate prin încheierea la sediul Autorității naționale de supraveghere a unor procese-verbale de constatare/sancționare. Astfel, comparativ cu anul 2015, se poate constata că activitatea de soluționare a plângerilor/sesizărilor **s-a dublat**, iar în cazul investigațiilor în scris, numărul acestora **a crescut de peste 4 ori**. Cu ocazia investigaţiilor efectuate pentru soluționarea plângerilor și sesizărilor, au fost aplicate sancţiuni contravenţionale, cuantumul total al amenzilor aplicate în 2016 fiind de **360.000 lei**.

Figura 2: Cuantumul amenzilor aplicate în activitatea de soluţionare a plângerilor şi sesizărilor în perioada 2012-2016



Totodată, în urma demersurilor de soluţionare a plângerilor şi sesizărilor adresate autorităţii, au fost emise **8 decizii** ale preşedintelui Autorităţii naționale de supraveghere, prin care s-a dispus ştergerea datelor personale sau a anumitor categorii de date. Principalele domenii în care au fost emise aceste decizii sunt legate de raportarea datelor negative către biroul de credit, monitorizarea condominiilor prin mijloace de supraveghere video și marketingul direct.

Plângerile şi sesizările primite în cursul anului 2016 au vizat o gamă largă de domenii, însă, la fel ca și în anii precedenţi, cele mai multe dintre plângeri au avut ca obiect posibile încălcări ale dreptului la protecția datelor personale în legătură cu acordarea de credite, utilizarea sistemelor de supraveghere video, transmiterea de comunicări comerciale prin mijloace de comunicație electronică, dezvăluirea datelor către diverse entități sau diseminarea datelor pe Internet. O problemă care a fost sesizată în anul 2016, în mai multe cazuri comparativ cu perioada anterioară, se referă la utilizarea de cookies pe anumite pagini de Internet, fără respectarea condițiilor legale.

Indiferent de domeniul de activitate al operatorilor, în continuare, multe dintre plângerile primite au avut ca obiect nerespectarea prevederilor legale ce privesc exercitarea drepturilor persoanelor vizate (în special, drepturile de informare, acces, intervenție, opoziție).

Referitor la prelucrarea datelor personale în legătură cu acordarea de credite, s-a constatat în anul 2016 o creştere accentuată a numărului plângerilor formulate împotriva băncilor, instituţiilor financiare nebancare ori a societăților de recuperări creanțe. Principalele motive de nemulţumire a persoanelor vizate au fost determinate, în continuare, de nerespectarea prevederilor Legii nr. 677/2001 și ale Deciziei Autorității naționale de supraveghere nr. 105/2007, care reglementează prelucrarea datelor personale în sistemele de evidenţă de tipul birourilor de credit.

Un număr însemnat de plângeri și sesizări s-au referit în 2016 la prelucrarea datelor personale prin mijloace de supraveghere video, domeniu reglementat de Autoritatea națională de supraveghere prin Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video. Operatorii reclamaţi au fost în principal asociaţiile de proprietari, diverse categorii de angajatori care au instalat un sistem de supraveghere video la locul de muncă, precum și persoane fizice care au montat camere de supraveghere video ce surprind imagini din spațiul public. Au mai fost sesizate și investigate situații de prelucrare a datelor personale prin intermediul sistemelor de supraveghere video instalate la nivelul unităților de învățământ.

În anul 2016 au fost înregistrate, de asemenea, o serie de petiţii având ca obiect dezvăluirea datelor personale pe Internet, fără consimțământul persoanelor vizate sau alt temei legal. Operatorii reclamaţi au fost societăţi care administrează diferite site-uri de socializare, societăți care au preluat și diseminat informații din dosarele aflate pe rolul instanțelor judecătorești, precum și autorități/instituții publice. De asemenea, Autoritatea națională de supraveghere a continuat să primească plângeri în anul 2016 (într-un număr mai redus, însă, prin comparație cu anii anteriori) 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.

O pondere importantă a fost reprezentată de plângerile prin care petiționarii au sesizat Autoritatea națională de supraveghere cu privire la primirea de mesaje comerciale nesolicitate prin mijloace de comunicație electronică. Operatorii reclamați au fost, în principal, societați care

efectuează activități de comerţ on-line sau marketing direct și furnizori de servicii de comunicații electronice.

În urma investigaţiilor realizate în 2016, cu toate că s-a identificat o scădere a numărului cazurilor în care operatorii nu cunosc deloc dispoziţiile legale aplicabile prelucrărilor de date, au fost constatate în continuare încălcari ale acestor prevederi de către operatori, ca urmare a nerespectării sau ignorării obligațiilor care le revin potrivit legii.

În majoritatea cazurilor investigate, operatorii au implementat măsurile dispuse de Autoritatea națională de supraveghere (ex. ștergerea datelor prelucrate ilegal, eliminarea rezultatelor afișate pe Internet, transmiterea unor răspunsuri adecvate persoanelor care și-au exercitat drepturile prevăzute de lege etc.), astfel încât să fie respectate reglementările în vigoare din materia protecției datelor personale.

În scopul informării celor interesați, pe pagina de Internet a Autorității naționale de supraveghere 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.

II. Principalele constatări rezultate din activitatea de soluţionare a plângerilor şi sesizărilor

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

În anul 2016 numărul plângerilor care au avut ca obiect transmiterea datelor personale către biroul de credit a crescut în mod considerabil, ocupând prima poziție ca pondere în numărul total al petițiilor primite de Autoritatea națională de supraveghere. În general, persoanele care au formulat o astfel de plângere au luat la cunoștință despre existența datelor negative (întârzieri la plata ratelor de credit) în sistemul de evidență al biroului de credit cu ocazia solicitării altor produse bancare, uneori trecând mai mulți ani după ce datele lor fuseseră transmise de către participanții la acest sistem. Prin urmare, lipsa informării prealabile, corecte și complete, condiție obligatorie impusă de Decizia nr. 105/2007 pentru a putea fi raportate date negative de către bănci sau instituții financiare nebancare, a constituit principalul motiv pentru care s-a solicitat intervenția instituției noastre.

Numărul ridicat al plângerilor primite în acest domeniu a determinat ca efectuarea investigațiilor să se realizeze în majoritatea cazurilor în scris, solicitându-se clarificarea

circumstanțelor în care au fost transmise date negative către biroul de credit pentru fiecare dintre plângerile particulare primite. În urma investigaţiilor desfăşurate, s-a constatat în multe situații nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul biroului de credit, cu referire la: tipul de informaţii raportate de către bănci și instituțiile financiare nebancare, modalitatea şi termenul de realizare a informării prealabile impuse de Legea nr. 677/2001 şi 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 şi 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 nebancare 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 mai multe petiţii, un petent a sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o bancă, despre care susținea că i-a transmis datele la biroul de credit fără a-l informa în prealabil, în conformitate cu prevederile Deciziei nr. 105/2007.

De asemenea, petentul a susținut și faptul că i-a fost încălcat dreptul de acces, dreptul de intervenție și dreptul de opoziție, prevăzute de Legea nr. 677/2001, deoarece operatorul nu a dat curs cererilor sale de exercitare a drepturilor menționate anterior și nu i-a transmis un răspuns în termen de 15 zile.

Pentru soluționarea petiției, s-a efectuat o investigație la bancă, în urma căreia s-a constatat faptul că, întrucât petentul nu și-a achitat la timp ratele datorate, a fost raportat la biroul de credit cu date negative, însă cu încălcarea dispozițiilor art. 12 din Legea nr. 677/2001

și ale art. 8 din Decizia 105/2007, adică fără a face dovada realizării informării prealabile a petentului anterior raportării. De asemenea, banca i-a transmis petentului un răspuns la cererea sa, fără să respecte însă opțiunea acestuia cu privire la expedierea răspunsului la o anumită adresă de e-mail, încălcând astfel prevederile art. 15 din Legea nr. 677/2001.

În acest context, banca în cauză a fost sancționată contravențional pentru contravențiile prevăzute de art. 32 din Legea nr. 677/2001 raportat la art. 12 și 15 din aceeași lege și la art. 8 din Decizia 105/2007 și i s-a recomandat să șteargă informațiile negative raportate la biroul de credit cu încălcarea dispozițiilor legale.

FIȘĂ DE CAZ

Prin petiţia transmisă, petentul a reclamat că figurează cu date negative raportate la biroul de credit, în legătură cu un contract încheiat cu o instituție financiară nebancară pentru emiterea unei linii de credit, deşi nu a fost înştiinţat în prealabil cu 15 zile înainte de data transmiterii datelor sale.

În cadrul investigaţiei efectuate, reprezentanţii societăţii financiare au precizat faptul că, întrucât petentul nu a realizat plăți lunare în intervalul scadent stabilit prin contract, a acumulat restanțe pe parcursul derulării creditului şi, în consecinţă, a transmis datele sale negative la biroul de credit. Cu toate acestea, instituţia financiară nu a făcut dovada informării prealabile a petentului înainte de transmiterea datelor negative, așa cum prevăd art. 8 și art. 9 din Decizia nr. 105/2007, cu excepţia a două dintre raportările negative evidenţiate la biroul de credit.

Societatea financiară nu a dat curs solicitării petentului de ștergere a datelor sale din baza de date a Biroului de Credit, susţinând că datele negative au fost transmise după înștiințarea cu cel puțin 15 zile calendaristice înainte de raportare, aspect care nu a fost însă dovedit.

În baza acestor constatări, societatea financiară a fost sancţionată contravenţional conform art. 32 din Legea nr. 677/2001 şi Deciziei nr. 105/2007 şi i s-a pus în vedere obligaţia de ștergere a datelor negative transmise la Biroul de Credit, fără informarea prealabilă a petentului în conformitate cu art. 8 și art. 9 din Decizia nr. 105/2007.

FIȘĂ DE CAZ

Prin petiţia transmisă, petentul a sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o instituție financiară nebancară, prin faptul că figurează cu date negative raportate la biroul de credit, deşi nu a fost înştiinţat în prealabil cu 15 zile înainte de data transmiterii acestora cu privire la restanţele înregistrate şi cu privire la posibilitatea raportării acestora la biroul de credit.

În cadrul investigaţiei efectuate, reprezentanţii societăţii financiare au precizat că, întrucât petentul nu şi-a achitat ratele lunare datorate, au transmis datele negative ale acestuia la biroul de credit. Din documentele analizate, a rezultat că nu s-a realizat informarea prealabilă a petentului pentru toate raportările făcute la biroul de credit potrivit art. 8 şi art. 9 din Decizia 105/2007, fiindu-i transmise în mai multe cazuri notificări cu depăşirea termenului de 15 zile prevăzut de lege; de asemenea, înştiinţările prealabile nu conţineau informaţii exacte privind sumele datorate ce urmau să fie raportate la biroul de credit.

În baza acestor constatări, societatea financiară a fost sancţionată contravenţional conform art. 32 din Legea nr. 677/2001 şi Deciziei nr. 105/2007. Totodată, prin decizia președintelui Autorității naționale de supraveghere s-a dispus ștergerea datelor negative transmise la Biroul de Credit fără informarea prealabilă a petentului, aşa cum prevăd art. 8 și art. 9 din Decizia ANSPDCP nr. 105/2007.

2. Prelucrarea datelor personale prin mijloace de supraveghere video

În acest domeniu, petițiile transmise Autorității naționale de supraveghere au fost în continuare într-un număr semnificativ, ca urmare a conștientizării de către persoanele fizice a drepturilor de care beneficiază, dar şi a rolului Autorităţii naționale de supraveghere în apărarea acestora, în contextul în care se constată ca fiind tot mai frecvente situațiile în care diverse persoane juridice sau fizice decid să recurgă la instalarea de sisteme de supraveghere video.

Prelucrarea datelor personale prin utilizarea unor sisteme de supraveghere video se supune atât prevederilor Legii nr. 677/2001, modificată şi completată, celor ale Deciziei

Autorității naționale de supraveghere nr. 52/2012, cât şi celor ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi 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 persoane juridice de drept public și privat care au montat astfel de sisteme la locurile de muncă în scopul monitorizării activității salariaților proprii, dar și al 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. O parte semnificativă a investigațiilor din acest domeniu s-a desfășurat la nivelul asociațiilor de proprietari unde au fost instalate camere de supraveghere video pentru protecția bunurilor din condominii și siguranța persoanelor care locuiesc în respectivele imobile.

În acest context, art. 8 din Decizia nr. 52/2012 stabileşte situaţiile în care prelucrarea datelor personale ale angajaţilor prin mijloace de supraveghere video este permisă, şi anume: pentru îndeplinirea unor obligaţii legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora. Alin. (3) al aceluiaşi articol din Decizia nr. 52/2012 prevede că „nu este permisă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, cu excepţia situaţiilor prevăzute expres de lege sau a avizului Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal”.

Având în vedere dispoziţiile legale de mai sus, Autoritatea națională de supraveghere a apreciat faptul că efectuarea supravegherii video la locul de muncă nu poate fi admisă în situațiile în care există mijloace mult mai puțin intruzive pentru atingerea scopurilor declarate (protecția bunurilor sau a salariaților ori monitorizarea desfășurării activității acestora în condiții de eficiență). În acelaşi timp, trebuie făcută dovada faptului că a fost efectuată în prealabil consultarea sindicatului sau a reprezentanţilor angajaţilor 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), Autoritatea națională de supraveghere a întreprins demersuri de investigare a plângerilor sau sesizărilor primite numai în situația în care s-a considerat ca fiind aplicabilă legislația în materie, respectiv în situațiile în care persoanele fizice operează un sistem de supraveghere video instalat pe proprietatea personală, care surprinde și stochează imagini din spațiul public (potrivit Hotărârii Curții de Justiție a Uniunii Europene din 11 decembrie 2014, pronunțată în cauza František Ryneš împotriva Úřad pro ochranu osobních údajů). În celelalte situații, devine incident art. 2 alin. (6) din Legea nr. 677/2001 care se referă la exceptarea de la aplicarea 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.

În urma investigaţiilor efectuate la mai multe categorii de operatori, în special la asociaţiile de proprietari, s-a constatat că aceştia nu au cunoștință sau nu respectă prevederile Legii nr. 677/2001 şi 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, reprezentanților acestora le-a fost făcut cunoscut 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 pe pagina de Internet).

FIŞĂ DE CAZ (asociaţii de proprietari)

Printr-o petiţie înregistrată la Autoritatea naţională de supraveghere, o persoană fizică a sesizat o posibilă încălcare a dispoziţiilor legale, în sensul că asociaţia de proprietari din imobilul unde locuiește a montat un sistem de supraveghere video în incinta blocului fără respectarea prevederilor legale aplicabile.

Urmare a investigației efectuate, unele dintre aspectele reclamate s-au confirmat, astfel că asociaţia de proprietari a fost sancţionată contravenţional pentru săvârşirea contravenţiilor prevăzute de art. 31 din Legea nr. 677/2001 (pentru omisiunea de a notifica în prealabil prelucrarea la autoritate) și de art. 32 prin raportare la art. 12 şi la art. 4 din aceeași lege (prelucrarea nelegală a datelor personale, întrucât nu se realiza o informare adecvată și completă a persoanelor vizate cu privire la această prelucrare, iar instalarea unor camere în lifturi a fost apreciată ca fiind excesivă prin raportare la scopul declarat).

Totodată, s-a recomandat asociaţiei, printre altele, să înceteze prelucrarea datelor persoanelor vizate (imaginea) prin intermediul camerelor de supraveghere montate în lifturi.

FIŞĂ DE CAZ (primării)

Prin petiţia înregistrată la Autoritatea naţională de supraveghere, o persoană fizică a sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către primăria unei comune, în sensul că aceasta prelucrează datele personale ale angajaților săi, prin intermediul unui sistem de supraveghere video montat în interiorul primăriei, inclusiv în birouri, monitorizând nelegal activitatea acestora.

Urmare a controlului efectuat, unitatea administrativ teritorială (reprezentată prin primarul comunei) a fost sancționată contravențional pentru faptele prevăzute de art. 31 din Legea nr. 677/2001 (omisiunea de a notifica prelucrarea la Autoritatea națională de supraveghere), art. 32 raportat la art. 12 (neasigurarea unei informări corespunzătoare a persoanelor vizate), art. 32 raportat la art. 4 (prelucrarea datelor personale fără respectarea prevederilor legale în vigoare care interzic, de regulă, instalarea camerelor video în birourile angajaților dacă nu există o obligație legală expresă sau un aviz emis în prealabil de către Autoritatea națională de supraveghere).

FIŞĂ DE CAZ (unități de învățământ)

Printr-o plângere adresată Autorității naționale de supraveghere, un petent a sesizat faptul că o școală a încălcat prevederile Legii nr. 677/2001, în sensul că aceasta deține un sistem de supraveghere video care prelucrează ilegal imagini cu elevi sau cadre didactice, în condițiile în care camerele de supraveghere erau instalate inclusiv în interiorul claselor.

În cadrul controlului efectuat pentru soluționarea plângerii, școala a motivat instalarea sistemului de supraveghere video ca fiind o obligație de a asigura supravegherea operațiunilor efectuate în timpul examenelor de evaluare națională, prin intermediul camerelor video instalate în sălile de examen și în birourile unde se multiplică subiectele de examen (biroul directorului).

Cu toate acestea, s-a constatat că, la data efectuării investigației, erau funcționale camerele de supraveghere din sălile de curs și în afara perioadelor examenelor de evaluare națională, sens în care s-a dispus menținerea în funcțiune a camerelor de supraveghere din sălile de curs exclusiv pe perioada examenelor, precum și ștergerea înregistrărilor existente din afara acestei perioade.

La finalul investigației au fost constatate contravențiile prevăzute de art. 31 din Legea nr. 677/2001 (omisiunea de a notifica prelucrarea datelor la Autoritatea națională de supraveghere), de art. 32 cu încălcarea art. 12 (prelucrarea nelegală a datelor personale ca urmare a lipsei unei informări corespunzătoare prevederilor legale), precum și de art. 33 din aceeași lege (neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, întrucât școala nu a adoptat suficiente măsuri de securitate, astfel încât să se prevină accesul sau dezvăluirea neautorizată la imaginile captate prin intermediul sistemului de supraveghere video instalat în școală, care puteau fi accesate inclusiv prin Internet, de la domiciliul directorului școlii).

FIŞĂ DE CAZ

Printr-o plângere adresată Autorității naționale de supraveghere, un fost primar de municipiu a sesizat faptul că ar fi fost dezvăluite către terți imagini cu el și soția sa, surprinse de o cameră de supraveghere instalată în incinta primăriei, imaginile fiind transmise către presă.

În cadrul controlului efectuat, aspectele sesizate au fost confirmate. Astfel, s-a constatat că la nivelul primăriei nu era elaborată și implementată o politică de securitate a datelor prelucrate prin intermediul sistemului de supraveghere video, care să cuprindă cerințele minime de securitate a prelucrărilor de date personale și în care să se regăsească informaţii privind fişierele de acces, instruirea personalului, folosirea computerelor, imprimarea datelor, tipul de

acces, identificarea şi autentificarea utilizatorului etc., potrivit dispozițiilor Ordinului nr. 52/2002, fapt care a condus și la accesul neautorizat și dezvăluirea imaginilor colectate de sistemul de supraveghere. Ca atare, s-a aplicat o sancțiune contravențională în baza art. 33 din Legea nr. 677/2001, întrucât nu au fost adoptate suficiente măsuri de securitate astfel încât să se prevină accesul sau dezvăluirea neautorizată la imaginile captate prin intermediul sistemului de supraveghere video instalat în primărie.

De asemenea, s-a mai constatat că, deși pe fiecare etaj al primăriei erau afișate pictograme, acestea nu cuprindeau toate informațiile potrivit art. 12 din Legea nr. 677/2001, sens în care s-a mai aplicat o sancțiune în temeiul art. 32 din Legea nr. 677/2001. O altă sancțiune aplicată în baza art. 32 a vizat nerespectarea dreptului de acces al petentului, având în vedere că primăria nu a răspuns la cererea sa.

3. Dezvăluirea datelor personale către diverse entităţi

Prin mai multe plângeri adresate Autorităţii naționale de supraveghere, au fost semnalate aspecte referitoare la încălcarea dispoziţiilor legale privind condiţiile în care date personale au fost dezvăluite publicului larg (prin publicarea pe site-uri, blog-uri etc.) sau către diverse entităţi de drept public şi privat, fără să fi fost obţinut 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 2016, Autoritatea națională de supraveghere a înregistrat în continuare o serie de plângeri (deși într-un număr mai redus față de perioada anterioară) 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, operatorul reclamat a fost Google Inc. care 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 sau că ar fi dezvăluite de către o ”agenție guvernamentală”. 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 Curţii de Justiţie a Uniunii Europene privind Google Spania şi INC v. Agencia Española de Proteccion de Datos (AEPD) Mario Costeja Gonzales C-131/12”, adoptat de Grupul de Lucru Art. 29, din care face parte şi Autoritatea națională de supraveghere din România.

FIȘĂ DE CAZ

Un petent a sesizat faptul că datele sale personale (imaginea), asociate cu o serie de informaţii false şi defăimătoare, au fost publicate pe mai multe pagini de internet (presă în format electronic). Informațiile considerate false se refereau la presupuse acuzaţii ce vizau o relaţie din mediul virtual între petent şi o persoană de sex feminin, care a pretins că este studentă şi care ar fi solicitat ajutor privind obţinerea unei diplome false, acuzaţii care ulterior s-au dovedit a fi nereale, petentului fiindu-i recunoscută nevinovăția de către o comisie de etică a universității unde activa în calitate de cadru didactic.

Petentul s-a adresat la Google Inc. cu solicitarea de a i se şterge datele personale, indexate pe Internet cu ajutorul motorului de căutare al acestei companii. Aceasta i-a transmis un răspuns prin care se comunica faptul că, în ceea ce privește unele adrese URL referitoare la numele său, se lucrează la blocarea acestora, iar pentru alte adrese URL, nu s-a dat curs solicitării, pe motiv că acestea includ informații de interes public.

În urma investigației efectuate de Autoritatea națională de supraveghere, adresele URL la care se aflau datele personale ale petentului nu au fost eliminate de Google Inc. din lista de căutări, operatorul solicitând în instanță anularea adresei prin care instituţia noastră i-a cerut ştergerea adreselor URL menţionate de petent.

Ca urmare a respingerii de către instanță a contestației formulate de Google Inc., Autoritatea națională de supraveghere a revenit la operator, cu solicitarea de a da curs cererii de ștergere a adreselor URL. În consecință, Google Inc. a blocat adresele URL menționate de către petent.

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.

Din investigațiile efectuate în anul 2016 s-a constatat faptul că, în anumite cazuri, dezvăluirea ilegală a datelor personale s-a produs ca urmare a neadoptării de către operatori a măsurilor de securitate și confidențialitate necesare pentru a preveni accesul unor persoane neautorizate la date sau diseminarea necontrolată a acestora în spațiul public.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere în legătură cu o posibilă încălcare a dispoziţiilor Legii nr. 677/2001, prin dezvăluirea pe Internet a unor adrese de poștă electronică, la o serie de adrese URL asociate unei pagini de internet.

Din verificarea adreselor URL indicate de petent, a rezultat disponibilitatea pe Internet a mai mult de 200 de adrese de poștă electronică, asociate site-ului deținut de o societate autorizată ca agenție de turism.

Ca urmare a investigației efectuate, s-a constatat faptul că agenția de turism colectează date personale, inclusiv adrese de poștă electronică, prin intermediul unor formulare de contactare și rezervare disponibile pe un site de promovare turistică, completate și trimise de persoanele interesate, precum și prin abonarea la ”newsletter”-ul societății.

În urma verificărilor efectuate în baza de date a societății au fost identificate o parte semnificativă din adresele de poștă electronică dezvăluite pe Internet la adresele URL menționate în sesizarea petentului, operatorul neputând prezenta motive care să justifice dezvăluirea pe site-ul pe care îl administrează a respectivelor adrese de e-mail.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul, în baza art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale), întrucât nu a asigurat o informare completă a persoanelor fizice ale căror date personale sunt colectate pe pagina de Internet a societății, dar și a art. 33 din aceeași lege, întrucât nu a aplicat măsuri tehnice și organizatorice adecvate pentru protejarea datelor personale împotriva dezvăluirii sau accesului neautorizat, în special, în cazul transmisiei de date în cadrul unei rețele, situație care a condus la divulgarea pe Internet a adreselor de poștă electronică ale unor abonați din baza de date a societății. Totodată, s-a dispus înlăturarea din spațiul public (Internet) a adreselor de e-mail ilegal dezvăluite.

FIȘĂ DE CAZ

O petentă a reclamat încălcarea prevederilor legale privitoare la prelucrarea datelor sale personale, provenite din dosarul profesional gestionat de o primărie din mediul rural, a cărei angajată este, prin dezvăluirea acestora (contract de muncă, diplome de absolvire, fișa postului) pe o reţea de socializare (Facebook), în perioada campaniei electorale pentru alegerile locale din anul 2016, în care soțul său a candidat la funcția de primar.

În cadrul investigației a rezultat că, urmare a unor informații defăimătoare publicate pe Facebook de către soțul petentei, primarul de la acea dată, candidat pentru ocuparea în

continuare a acestei funcții, a considerat necesar să contrazică afirmațiile la adresa sa, prin dezvăluirea publică a condițiilor considerate ilegale de ocupare a postului de către petentă, pe baza unor documente apreciate a fi false. În acest sens, a solicitat secretarului comunei dosarul profesional al petentei și a fotografiat cu telefonul personal o serie de documente, pe care ulterior le-a postat pe contul de Facebook al unei cunoștințe.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat comuna, reprezentată prin primar, în baza art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale), pentru nesocotirea dreptului de opoziție al petentei, dar și a art. 33 din aceeași lege, întrucât nu au fost adoptate măsuri de securitate și confidențialitate, astfel încât să se prevină dezvăluirea neautorizată a datelor personale aflate în gestiunea primăriei unde era angajată petenta, situație care a condus la dezvăluirea datelor personale ale acesteia pe Facebook.

Faţă de constatările din cadrul investigaţiei şi având în vedere prevederile Hotărârii Guvernului nr. 432/2004 privind dosarul profesional al funcţionarilor publici, conform cărora Agenţia Naţională a Funcţionarilor Publici are competenţa de a sancţiona fotocopierea şi/sau transmiterea unor fotocopii de pe documentele aflate în dosarul profesional către terţe persoane, Autoritatea națională de supraveghere a sesizat instituția menționată anterior.

FIȘĂ DE CAZ

Un petent ne-a sesizat cu privire la faptul că o instanță (judecătorie) a refuzat să dea curs solicitării ca datele sale personale să nu mai fie publicate pe portalul instanţelor de judecată, întrucât nu ar fi reglementată o procedură în acest sens.

În cadrul investigației desfășurate în acest caz, Autoritatea națională de supraveghere a adus la cunoştinţă operatorului informaţiile furnizate de Ministerul Justiției în legătură cu situaţii similare, potrivit cărora conţinutul paginilor web de tip portal se află în administrarea instanţelor, termenul de arhivare electronică este de 24 luni şi începe să curgă de la data soluţionării dosarului, conform regulilor stabilite în utilizarea sistemului ECRIS (sistemul de gestiune a dosarului în instanță).

Ulterior demersurilor Autorității naționale de supraveghere, dosarul cuprinzând datele personale ale petentului, aparținând instanței reclamate, nu a mai figurat pe portalul instanțelor, ca urmare a arhivării acestuia în sistemul ECRIS.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, pe un cont de Facebook, a fost publicată copia vizibilă a unui certificat de orientare școlară și profesională, emis de un Centru Județean de Resurse și Asistență Educațională, care conținea datele personale (nume, prenume, data nașterii, locul nașterii, adresa de domiciliu și de reședință, codul numeric personal), date privind starea de sănătate (tipul de deficiență/handicap ”somatic”) ale unui minor, precum și numele și prenumele părinților acestuia.

Din verificările întreprinse a rezultat că respectivul document ar fi fost postat de comitetul de părinți al unei clase din școala gimnazială unde minorul în cauză era înmatriculat.

În cadrul investigațiilor întreprinse, Autoritatea națională de supraveghere a sancționat școala gimnazială pentru fapta prevăzută de art. 33 din Legea nr. 677/2001, întrucât nu a adoptat măsuri de securitate și confidențialitate astfel încât să prevină dezvăluirea neautorizată a datelor personale ale unui minor, prin fotocopierea și ulterior dezvăluirea unui document cuprinzând datele acestuia, precum și ale părinților săi, prin postarea unui înscris pe un cont de Facebook, de către președintele comitetului de părinți al clasei în care învăța minorul. Autoritatea națională de supraveghere l-a sancționat inclusiv pe acesta din urmă pentru dezvăluirea datelor minorului pe Facebook cu încălcarea dispozițiilor art. 5 din Legea nr. 677/2001.

FIȘĂ DE CAZ

Un petent a sesizat instituția noastră cu privire la faptul că o autoritate publică a publicat pe site-ul propriu o listă cu persoanele care au depus cereri în baza Legii nr. 544/2001, conţinând nume şi prenume ale mai multor persoane fizice, precum şi liste cu persoane juridice cărora li s-au aplicat sancţiuni contravenționale.

În urma demersurilor efectuate a rezultat că documentele în cauză nu sunt publicate pe pagina de internet a autorității publice reclamate, ci în spaţiul Google Drive, de către un minister căruia îi fuseseră comunicate respectivele informații.

Conform declarațiilor reprezentanților acestui minister, s-a considerat că informațiile respective erau de real interes pentru societatea civilă, fapt pentru care s-a decis publicarea acestora pe pagina de internet a ministerului, având în vedere rolul şi scopul acestuia, de creştere a transparenţei şi a gradului de informare referitor la activitatea instituţiilor statului.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat ministerul în baza art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale), întrucât a dezvăluit, prin publicarea pe Internet, datele personale ale persoanelor care au depus cereri în baza Legii nr. 544/2001 (respectiv nume şi prenume) şi ale persoanelor fizice autorizate cărora le-au fost aplicate măsuri sancţionatorii, fără să dispună transformarea acestor date în date anonime, fără consimțământul și informarea persoanelor ale căror date personale au fost dezvăluite. Urmare a demersurilor Autorității naționale de supraveghere, ministerul a înlăturat datele personale din spațiul public.

4. Prelucrarea nelegală a codului numeric personal

Din practica de soluționare a plângerilor și sesizărilor adresate Autorității naționale de supraveghere în cursul anului 2016, se constată situații diverse de încălcare a prevederilor Legii nr. 677/2001, sub aspectul respectării principiilor legalității și 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.

În privința prelucrării codului numeric personal, s-au constatat situații în care acesta este colectat în mod obligatoriu pentru efectuarea anumitor operațiuni (ex. emiterea de facturi fiscale, returnarea unor produse comercializate), prin invocarea eronată a unor prevederi legale care ar impune această prelucrare. În acest context, Autoritatea națională de supraveghere a urmărit respectarea art. 8 din Legea nr. 677/2001 și a 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.

FIŞĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată printr-o petiție cu privire la condiţionarea colectării codului numeric personal la întocmirea facturilor pentru persoane fizice, respectiv achiziţionarea unui produs.

Urmare a investigației efectuate, s-a constatat că societatea respectivă prelucrează codul numeric personal de la persoanele fizice pentru întocmirea facturilor, deşi în articolul 155 din Codul fiscal, prevedere în vigoare până la data intrării în vigoare a noului Cod fiscal, precum şi în articolul 319 din noul Cod fiscal, această dată cu caracter personal nu este menţionată printre datele obligatorii ce trebuie completate pentru emiterea facturii fiscale pentru persoanele fizice (altele decât persoanele impozabile ori plătitoare de TVA).

Prin urmare, prelucrarea codului numeric personal pentru emiterea facturii nu s-a realizat nici în baza unei prevederi legale, nici pe baza consimţământului liber exprimat al persoanei vizate, nici cu avizul Autorităţii naționale de supraveghere, aşa cum dispun art. 8 din Legea nr. 677/2001 şi art. 2 din Decizia ANSPDCP nr. 132/2011.

În consecință, operatorul a fost sancționat pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, întrucât a prelucrat codul numeric personal al persoanelor vizate, pentru emiterea facturilor fiscale, fără respectarea prevederilor art. 8 din Legea nr. 677/2001 şi ale art. 2 din Decizia ANSPDCP nr. 132/2011; s-a mai recomandat luarea măsurilor care se impun pentru încetarea prelucrării codului numeric personal în scopul emiterii facturilor fiscale.

5. Nerespectarea drepturilor de informare, acces, intervenţie şi opoziţie

Respectarea drepturilor persoanelor vizate reglementate de Legea nr. 677/2001, în special a dreptului la informare (art. 12), a dreptului de acces la date (art. 13), a dreptului de intervenţie asupra datelor (art. 14) şi a dreptului de opoziţie (art. 15), deși reprezintă o obligație esențială a operatorilor de date, a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere și în anul 2016.

Astfel, ca urmare a investigaţiilor efectuate, s-a constatat că operatorii fie nu cunosc obligaţiile care le incumbă potrivit reglementărilor legale susmenţionate, fie le ignoră cu bună-ştiinţă, fie transmit persoanelor vizate răspunsuri incomplete sau/şi fără respectarea termenului de 15 zile prevăzut de lege, fie nu au adoptat măsuri organizatorice suficiente și eficiente pentru gestionarea cererilor adresate de persoanele vizate în baza drepturilor reglementate de Legea nr. 677/2001.

Totodată, s-a înregistrat o creștere a gradului de conștientizare a persoanelor vizate cu privire la drepturile de care beneficiază în baza Legii nr. 677/2001, indiferent de domeniul în care le erau prelucrate datele personale, aspect care s-a concretizat într-o creștere a numărului de petiții având acest obiect.

Asupra importanței pe care operatorii trebuie să o acorde dreptului de informare, indiferent de calitatea lor de persoane de drept public ori privat, reiterăm faptul că aceasta a

fost confirmată prin Hotărârea pronunțată de CJUE la 1 octombrie 2015 în cauza Smaranda Bara şi alţii împotriva Preşedintelui Casei Naţionale de Asigurări de Sănătate, Casei Naţionale de Asigurări de Sănătate şi Agenţiei Naţionale 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

Prin petiția adresată instituției noastre, petentul a reclamat faptul că un operator nu i-a furnizat toate informaţiile solicitate în urma exercitării dreptului de acces prevăzut de art. 13 din Legea nr. 677/2001, informații pe care le-a solicitat în scris de la acest operator, prin mai multe cereri.

În plus, petentul a reclamat şi faptul că trei dintre răspunsurile operatorului i-au fost trimise prin intermediul poştei electronice, cu toate că solicitase în mod expres ca răspunsurile să-i fie comunicate prin intermediul poştei ordinare, indicând adresa la care să-i fie transmise.

În urma verificărilor efectuate în cursul investigației, a reieșit că petentul a încheiat două contracte de prestări de servicii cu acest operator, unul pentru furnizarea de servicii de televiziune și unul pentru furnizarea serviciului de internet, dar că relația contactuală între părți a încetat anterior solicitărilor adresate operatorului.

Din răspunsurile transmise de operator petentului, a rezultat că acestuia nu i-au fost comunicate, conform prevederilor art. 13 din Legea nr. 677/2001, toate informațiile cu privire la prelucrarea datelor sale și că răspunsurile nu i-au fost transmise la adresa indicată de acesta.

Față de constatările rezultate, operatorul a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal) raportat la prevederile art. 13 din lege. De asemenea, s-a recomandat operatorului transmiterea unui nou răspuns către petent, în care să i se comunice acestuia informațiile solicitate, precum și luarea măsurilor care se impun astfel încât, pe viitor, să se răspundă la cererile prin care persoanele își exercită drepturile prevăzute de Legea nr. 677/2001, cu repectarea prevederilor art. 13, 14 și 15 din aceeași lege.

FIȘĂ DE CAZ

În fapt, petentul a sesizat că este nemulțumit de răspunsul comunicat de un inspectorat județean de poliție, căruia i s-a adresat în 2015 cu solicitarea ca datele sale personale, referitoare la o măsură educativă dispusă în 1991 printr-o hotărâre judecătorească (dată la care petentul era minor), să fie şterse din evidenţele de cazier judiciar ale acestei instituții, să nu mai fie dezvăluite ori utilizate, iar terţii cărora le-au fost dezvăluite să fie notificaţi cu privire la măsurile adoptate.

Astfel, petentul a susţinut că datele sale au fost prelucrate şi dezvăluite către terţi fără respectarea legii de către instituția publică reclamată, care în 2012 a depus în cadrul unui proces de contencios administrativ, printre alte documente, şi anumite rapoarte, făcându-se astfel publice detalii din viaţa sa privată, care ar fi influențat luarea unei decizii defavorabile cu

privire la autorizarea desfășurării unei activități. Cu această ocazie, petentul a sesizat că la data respectivă figura în evidenţele operative de cazier judiciar cu o măsură educativă care ar fi trebuit ştearsă, deoarece termenul de stocare a expirat. Mai mult, printr-o adresă din 2012 i se comunicase petentului că măsura educativă care i-a fost aplicată a fost ştearsă din oficiu din 2008, iar din 2011 datele sale au fost şterse inclusiv din ”evidenţele operative”, în baza Dispoziţiei IGPR nr. 18/2011.

În cadrul investigației efectuate, operatorul a recunoscut că datele petentului au fost şterse din evidenţele operative, nu la data intrării în vigoare a Dispoziţiei IGPR nr. 18/2011, ci ulterior, în 2012, când petentul a depus o cerere de emitere a unui certificat de cazier judiciar, iar în 2015 au fost şterse definitiv din toate evidenţele sale.

Totodată, din investigație a rezultat că datele petentului au fost comunicate instanțelor de judecată și structurii centrale în subordinea căreia funcționa operatorul reclamat. De aceea, susținerea operatorului că notificarea către terţii cărora le-au fost dezvăluite datele petentului ar fi imposibilă şi ar presupune un efort disproporţionat faţă de interesul legitim, care ar putea fi lezat, nu era întemeiată.

Față de constatările rezultate, operatorul a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal) raportat la prevederile art. 14 din lege, deoarece nu a notificat terţii cărora le-au fost dezvăluite datele petentului în privinţa ştergerii datelor sale din evidenţele cazierului judiciar şi din evidenţele operative de cazier judiciar şi nici nu a comunicat un răspuns complet la cererea acestuia, conform solicitării formulate prin petiţia din 2015.

De asemenea, s-a recomandat operatorului transmiterea unui răspuns complet către petent, în care să i se comunice acestuia informațiile solicitate, precum și notificarea terţilor cărora le-au fost dezvăluite datele petentului cu privire la măsurile adoptate.

FIȘĂ DE CAZ

Petentul a semnalat că a solicitat unei societăți de telefonie în mai multe rânduri ştergerea datelor sale personale, în condițiile în care nu mai exista un contract încheiat cu operatorul de telefonie, dar că răspunsul comunicat de acesta nu a fost unul mulţumitor.

Din verificările efectuate în cursul investigației, a reieșit că petentul a încheiat cu operatorul un contract în 2005, în scopul furnizării serviciilor de telefonie, iar ulterior, alte două contracte. Deoarece în timpul derulării primului contract a înregistrat restanțe la plata facturilor, datele sale au fost transmise către o societate de recuperări creanțe. Cu toate acestea, din corespondența purtată de petent cu această societate, a rezultat că dosarul întocmit pe numele său figurează închis în evidențele societății din anul 2007, debitul fiind recuperat.

Față de aceste constatări, operatorul a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale) raportat la art. 13 și 14 din lege, întrucât nu i-a furnizat petentului informațiile solicitate prin petițiile adresate și nu a dat curs solicitării de a-i șterge datele pe care le prelucrează, în condițiile în care la data solicitării contractul își încetase efectele, iar debitul fusese recuperat din anul 2007.

De asemenea, s-a recomandat operatorului să transmită un răspuns complet petentului, precum și să şteargă datele acestuia din evidențele sale.

FIȘĂ DE CAZ

Petenta a reclamat faptul că o societate comercială nu i-a şters datele personale care o privesc, respectiv nume, adresă, număr de telefon, care se regăseau pe site-ul societății. De asemenea, a semnalat faptul că această societate comercială nu i-a comunicat un răspuns la cererea prin care solicita ştergerea acestor date și nu a încetat diseminarea lor către terţi, în condiţiile în care a radiat din 2009 de la Registrul Comerțului forma de organizare în care își desfășura activitatea la un moment dat, respectiv PFA (persoană fizică autorizată) și cu care erau asociate informațiile de natură personală publicate pe site.

În cursul investigațiilor efectuate, operatorul nu a dat curs solicitărilor instituției noastre și a refuzat comunicarea tuturor informațiilor referitoare la prelucrarea datelor personale efectuate. În ceea ce privește cererea petentei, operatorul a precizat că nu a identificat această corespondență în evidențele societății, deși petiția fusese trimisă prin poștă cu confirmare de primire semnată de operator, și că nu a identificat vreo informație în evidențele informatice care să se refere la petentă, cu toate că aceste date existau pe site-ul societății.

Întrucât din documentele prezentate a reieşit că petenta și-a exercitat dreptul de intervenție față de prelucrarea datelor, iar operatorul nu a dat curs cererii sale şi nu i-a transmis un răspuns, acesta a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal) raportat la art. 14 din Legea nr. 677/2001.

De asemenea, operatorul a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 34 din Legea nr. 677/2001 (refuzul de a furniza informaţii), deoarece nu a furnizat toate informaţiile sau documentele solicitate de Autoritatea naţională de supraveghere, în exercitarea atribuţiilor de investigare prevăzute la art. 27 din Legea nr. 677/2001.

FIȘĂ DE CAZ

În fapt, petentul a sesizat că a solicitat unei bănci ștergerea datelor sale personale negative raportate la biroul de credit, dar nu a primit un răspuns la solicitarea sa.

Din informaţiile obţinute în cadrul investigaţiei, a rezultat că operatorul a prelucrat datele personale ale petentului ca urmare a contractului de credit încheiat cu acesta. Ulterior, deoarece petentul a înregistrat restanțe la plata ratelor, a fost raportat cu date negative la biroul de credit. Întrucât nu și-a respectat obligațiile prevăzute de Legea nr. 677/2001 și Decizia nr. 105/2007 față de persoana vizată, în sensul că nu a realizat informarea prealabilă a acesteia, operatorul a fost sancţionat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal) raportat la art. 12 din aceeaşi lege şi la art. 9 din Decizia nr. 105/2007. Totodată, Autoritatea naţională de supraveghere a solicitat operatorului să șteargă în cazul petentului datele negative transmise la biroul de credit pentru care nu a putut face dovada informării prealabile.

De asemenea, întrucât din documentele verificate a reieşit că, prin petiția adresată operatorului, petentul și-a exercitat dreptul de opoziție față de prelucrarea datelor sale de către biroul de credit, iar operatorul nu i-a transmis un răspuns în termen de 15 zile de la data primirii cererii, acesta a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor cu caracter personal) raportat la art. 15 din Legea nr. 677/2001.

6. Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

În cursul anului 2016, s-a menținut numărul ridicat de plângeri şi sesizări având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (SMS) sau prin poşta electronică. Majoritatea acestora au privit aspecte legate de protecţia vieţii private în sectorul comunicaţiilor electronice prin primirea de mesaje comerciale nesolicitate prin poşta electronică, fără consimţământul expres şi neechivoc al destinatarului în acest sens.

În vederea soluţionării plângerilor considerate admisibile, Autoritatea națională de supraveghere a efectuat o serie de investigaţii pentru a verifica existenţa consimţământului persoanei vizate de a primi mesaje comerciale pe adresa sa de poştă electronică sau prin SMS. În unele cazuri investigate, s-a constatat că expeditorii mesajelor comerciale nu au respectat prevederile legale sub aspectul obţinerii consimțământului prealabil şi al respectării opţiunii persoanelor vizate de a nu mai primi mesaje comerciale nesolicitate. Astfel, în multe situaţii, s-a constatat faptul că operatorii au continuat să trimită mesaje cu caracter comercial chiar şi după ce persoanele vizate şi-au exercitat dreptul de opoziţie, unul dintre motive fiind legat de nefuncționarea unor mecanisme adecvate de abonare (dublu ”opt-in”) și dezabonare.

FIȘĂ DE CAZ

Prin mai multe petiții, o petentă a susţinut faptul că a primit în repetate rânduri, de la mai multe adrese de e-mail, mesaje comerciale nesolicitate care promovau diverse servicii de turism, deşi nu a solicitat să primească astfel de mesaje. Prin aceeaşi petiţie, petenta a precizat şi faptul că s-a adresat deținătorului adreselor de e-mail, dar nu a primit niciun răspuns. În urma verificărilor făcute, s-a constatat faptul că toate mesajele comerciale primite de petentă proveneau de la același operator.

Ca urmare a investigației efectuate la această societate, s-a constatat faptul că, în perioada în care petenta a primit mesajele comerciale, societatea a desfășurat activități de marketing prin transmiterea de comunicări comerciale către adrese de e-mail colectate prin mai multe modalități (on-line pe site-ul societății, prin formulare completate la târguri de turism, telefonic). În ceea ce privește mesajele comerciale primite de petentă, societatea nu a putut preciza sursa adresei de e-mail aparținând acesteia, neputând așadar face dovada obținerii

consimțământului său expres și prealabil pentru primirea de comunicări comerciale prin mijloace de comunicație electronică.

În timpul investigației, reprezentanții societății au precizat faptul că nu au răspuns la cererile petentei, dar au șters adresa de e-mail a acesteia la data primirii solicitării.

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

FIȘĂ DE CAZ

Un petent a reclamat faptul că a primit pe adresa de e-mail personală un mesaj comercial nesolicitat, care nu conținea datele de identificare ale expeditorului comunicării. Prin aceeaşi petiţie, petentul a precizat şi faptul că s-a adresat deținătorului adresei de e-mail (”Operatorul 1”), menționând că nu a accesat anterior site-ul promovat și nici nu s-a abonat pentru a primi ”newsletter”. Prin mesajul trimis, petentul solicita să i se precizeze sursa adresei sale de e-mail și motivul trimiterii de ”spam”. Petentul a primit un răspuns în care i se menționa că mesajul comercial a fost trimis de o societate comercială de marketing online (”Operatorul 2”). Ulterior, petentul a solicitat să i se precizeze denumirea companiei de marketing care a trimis mesajul, solicitare rămasă însă fără răspuns.

În urma investigațiilor efectuate de Autoritatea naţională de supraveghere la cei doi operatori, a rezultat că Operatorul 2 transmitea mesaje comerciale, utilizând propria infrastructură și bază de date pentru trimiterea de e-mail-uri în scop de marketing în numele Operatorului 1.

Reprezentantul Operatorului 2 nu a putut preciza sursa de colectare a adreselor de e-mail care alcătuiesc baza de date proprie (indicând cu titlu de exemplu cumpărarea unor baze de date, fără alte detalii concrete) și a declarat faptul că nu a obținut consimțământul deținătorilor acestor adrese de e-mail pentru prelucrarea datelor lor și trimiterea de comunicări comerciale prin poșta electronică. Aceste declarații s-au menținut inclusiv cu privire la datele petentului.

Față de cele constatate, Operatorul 2 a fost sancționat contravențional în baza art. 13 raportat la art. 12 din Legea nr. 506/2004. Totodată, i s-a solicitat să șteargă toate datele personale, inclusiv adrese de e-mail, colectate și utilizate fără consimțământul expres prealabil al deținătorilor în scopul trimiterii de comunicări comerciale și să înceteze trimiterea de

comunicări comerciale prin mijloace electronice fără consimţământul expres şi prealabil al deținătorilor adreselor de poștă electronică.

FIȘĂ DE CAZ

Un petent a reclamat primirea de mesaje comerciale pe adresa sa de poștă electronică, de la o agenție de turism, cu toate că nu și-a dat acordul pentru primirea acestor mesaje. Petentul a solicitat operatorului în mai multe rânduri informații privind scopul prelucrării datelor sale, datele prelucrate, destinatarii cărora le sunt sau le-au fost dezvăluite datele, sursa din care au fost colectate datele și mecanismele automate utilizate, drepturile față de datele prelucrate, menționând că nu și-a dat acordul pentru trimiterea de comunicări comerciale și nici pentru prelucrarea datelor sale personale.

Petentul a primit un răspuns de la societate, prin care i se comunica faptul că adresele de e-mail către care societatea trimite oferte de servicii turistice se află în baza de date a agenției „ca urmare a abonării la newsletter sau la un site partener, ca urmare a unei corespondențe anterioare etc.”; s-a mai precizat petentului faptul că singura dată personală deținută este adresa sa de e-mail, precum și faptul că are posibilitatea de dezabonare răspunzând la mesajul primit sau accesând butonul de dezabonare din interiorul mesajului.

În timpul investigației, operatorul nu a putut preciza însă cu exactitate care este sursa de colectare a datelor personale aparținând petentului. În baza de date electronică a societății, adresa de e-mail a petentului figura în lista de contacte, ca fiind dezabonată. Prin urmare, reprezentanții societății nu au prezentat dovezi privind obținerea în prealabil a consimțământului expres al petentului, în vederea transmiterii de comunicări comerciale către adresa sa de poștă electronică, conform art. 12 din Legea nr. 506/2004.

De asemenea, din verificarea site-ului societății, unde se putea realiza abonarea în vederea primirii unui ”newsletter”, nu a rezultat existența unei informări complete privind prelucrarea datelor personale, conform art. 12 din Legea nr. 677/2001, în special, sub aspectul drepturilor persoanelor vizate și al condițiilor de exercitare a acestora.

Față de constatări, operatorului i-au fost aplicate sancțiuni contravenționale în baza Legii nr. 677/2001 (art. 32 raportat la art. 12) și a Legii nr. 506/2004 (art. 13 raportat la art. 12).

FIȘĂ DE CAZ

Prin petițiile înregistrate la Autoritatea naţională de supraveghere, o petentă a sesizat faptul că a primit mai multe mesaje comerciale pe adresa sa personală de e-mail, de la mai multe adrese de e-mail.

Petenta s-a adresat în prealabil deţinătorilor adreselor de la care a primit mesajele comerciale, solicitând informații în legătură cu sursa de unde au obţinut adresa sa de e-mail, scopul în care prelucrează această adresă și dacă există destinatari cărora le-a fost dezvăluită aceasta, însă nu a primit niciun răspuns.

Autoritatea naţională de supraveghere a efectuat inițial demersuri la o societate comercială al cărei obiect de activitate avea legătură, printre altele, cu înregistrarea numelor de domenii implicate în trimiterea mesajelor nesolicitate.

În urma investigației desfăşurate, s-a constatat că domeniile de pe care s-au transmis mesajele comerciale reclamate au fost achiziționate de către această societate, în numele și pentru un alt operator. În consecinţă, s-a continuat investigaţia la operatorul care administra efectiv domeniile reclamate. Reprezentantul acestei societăți a recunoscut faptul că a trimis mesaje prin e-mail către adresa petentei, fără să poată face dovada obținerii acordului său.

În urma investigaţiei efectuate, s-a constatat faptul că societatea nu a obţinut consimţământul petentei pentru transmiterea de mesaje comerciale şi nici nu a formulat şi transmis un răspuns petentei la solicitarea sa.

Faţă de constatări, operatorului reclamat i-au fost aplicate sancţiuni contravenţionale în baza Legii nr. 677/2001 şi a Legii nr. 506/2004.

FIȘĂ DE CAZ

Mai mulţi petenţi au reclamat primirea unor comunicări comerciale prin poșta electronică de la diverse entități, utilizându-se serviciile informatice puse la dispoziție de către o anumită societate comercială.

În urma investigaţiei efectuate, s-a constatat faptul că operatorul punea la dispoziția clienților săi (preponderent societăţi comerciale) o platformă de transmitere a mesajelor comerciale de tip newsletter (e-mail marketing). În consecinţă, în timpul controlului, reprezentanţii Autorităţii naţionale de supraveghere au solicitat furnizarea unor informaţii necesare pentru identificarea clienților și a tuturor circumstanțelor care au vizat trimiterea de mesaje către petiționari.

Întrucât în cadrul investigației operatorul nu a prezentat niciun fel de document, în format fizic sau electronic, în sprijinul declarațiilor sale, și nici nu a permis efectuarea vreunei verificări în sistemele informatice utilizate, care au făcut obiectul investigației, s-a pus în vedere acestuia să transmită informaţiile şi documentele solicitate în termenul stabilit.

Operatorul reclamat nu s-a conformat şi, în consecinţă, a fost sancţionat contravenţional în baza Legii nr. 677/2001, pentru refuzul de a furniza Autorităţii naţionale de supraveghere, informaţiile şi documentele cerute de aceasta în exercitarea atribuţiilor de investigare.

Trebuie precizat faptul că, în lipsa informațiilor pe care le dețin astfel de societăți sau furnizorii de servicii de comunicații electronice, Autoritatea națională de supraveghere se află în unele cazuri în imposibilitatea de a identifica expeditorii comunicărilor comerciale prin mijloace de comunicație electronică și de a le antrena în consecință răspunderea juridică.

7. Încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date

Una dintre obligațiile de bază ale operatorilor de date personale prevăzute de legislația în materie se referă la adoptarea măsurilor de securitate a prelucrărilor și de respectare a regulilor de confidențialitate, prin care să se prevină incidente de genul dezvăluirii ilegale a datelor, accesării datelor de către persoane neautorizate, pierderii sau distrugerii datelor etc.

În anul 2016, o parte din plângerile și sesizările ce au fost adresate Autorității naţionale de supraveghere au avut ca obiect fie dezvăluirea datelor personale către terțe persoane sau pe Internet, fie accesarea neautorizată a datelor personale, fără să existe consimțământul

persoanelor vizate sau un temei legal expres, ca urmare a faptului că operatorii în cauză (autorități publice de la nivel local, furnizori de servicii de telefonie etc.) nu au implementat proceduri interne eficiente, de ordin tehnic sau organizatoric, care să conducă la preîntâmpinarea unor astfel de probleme.

FIȘĂ DE CAZ

O petentă a reclamat faptul că ar fi fost încălcat dreptul la protecția datelor personale ale unui număr de 138 de persoane de către primăria unei comune, care le-a postat pe site-ul propriu. Prin accesarea adresei URL indicate, s-a constatat că sunt publicate mai multe documente ce conţin date personale ale locuitorilor comunei, inclusiv date cu caracter sensibil, respectiv cod numeric personal şi date privind starea de sănătate. De asemenea, erau disponibile anunţuri colective emise în baza art. 44 alin. (3) din Codul de Procedură Fiscală care cuprindeau un număr ridicat de persoane, cu menţionarea numelui, a adresei complete, a numărului şi a datei emiterii somaţiei sau titlului executoriu.

Conform Ordinului ministrului finanţelor publice nr. 94/2006 privind aprobarea modelului şi conţinutului formularelor şi a instrucţiunilor de completare a acestora în vederea îndeplinirii procedurii de comunicare a actelor administrative fiscale prin publicitate, comunicarea prin publicitate se efectuează în situaţia în care actul administrativ fiscal nu a putut fi comunicat prin una dintre modalităţile de comunicare prevăzute la art. 44 alin. (2) - (2^1) din Ordonanţa Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu modificările şi completările ulterioare, acte normative în vigoare la data publicării anunţurilor colective. Comunicarea actului administrativ fiscal prin publicitate se realizează prin afişarea, concomitent, la sediul autorităţii emitente şi pe pagina de Internet a acesteia, a unui anunţ în care se menţionează că a fost emis actul administrativ fiscal pe numele contribuabilului. Anunţul va fi păstrat o perioadă de 15 zile de la data afişării. Modelul anunţului colectiv prevăzut în anexa nr. 1^B la acest ordin cuprinde: nume, prenume, denumire contribuabil, domiciliu fiscal, denumire, nr. şi dată act administrativ fiscal. Acest model nu conţine şi codul numeric personal al contribuabililor.

De asemenea, Curtea Constituţională, în jurisprudenţa sa (deciziile nr. 1288/2008, 667/2009, 536/2011), a apreciat că "Interesul organelor fiscale de aducere la cunoştinţa contribuabilului a existenţei unei obligaţii fiscale al cărei creditor este însuşi statul implică necesitatea comunicării actului administrativ în care aceasta este consemnată prin modalităţi care să asigure aducerea efectivă la cunoştinţa contribuabilului despre existenţa unor obligaţii fiscale în sarcina sa. Aşa fiind, legiuitorul a prevăzut că actele administrative fiscale pot fi comunicate prin publicitate şi în cazul în care domiciliul contribuabilului este cunoscut. În acest caz, însă, trebuie ca, anterior recurgerii la această modalitate, să fi fost respectată cu stricteţe ordinea prevăzută în art. 44 alin. (2) lit. a) - c) din Ordonanţa Guvernului nr. 92/2003, astfel încât comunicarea prin publicitate să reprezinte doar o modalitate ultimă şi subsidiară."

Prin urmare, comunicarea prin publicitate pe Internet reprezintă ultima modalitate subsidiară de comunicare a actului administrativ fiscal, dacă nu au fost posibile celelalte modalităţi prevăzute de Codul de procedură fiscală, respectiv: remiterea acestuia contribuabilului/împuternicitului, dacă se asigură primirea sub semnătură a actului administrativ fiscal sau prin poştă, cu scrisoare recomandată cu confirmare de primire; prin fax, e-mail sau alte mijloace electronice de transmitere la distanţă, dacă se asigură transmiterea textului actului administrativ fiscal şi confirmarea primirii acestuia şi dacă contribuabilul a solicitat expres acest lucru.

În urma consultării paginii de internet a primăriei, au fost identificate şi dispoziţii pentru acordarea/încetarea indemnizaţiei lunare acordate în baza Legii nr. 448/2006 privind protecţia şi promovarea drepturilor persoanelor cu handicap, în cuprinsul cărora sunt menţionate numele şi prenumele, codul numeric personal, adresa de domiciliu, precum şi menţiunea că este o persoană cu handicap.

De asemenea, erau publicate dispoziţii prin care se acorda alocaţie pentru susţinerea familiei, în baza prevederilor art. 23 din Legea nr. 277/2010 privind alocaţia pentru susţinerea familiei, în cuprinsul cărora erau menţionate numele şi prenumele, codul numeric personal şi adresa de domiciliu.

Ca urmare a investigației efectuate, s-a reţinut că dezvăluirea sau publicarea datelor personale, în special a celor precizate expres la art. 8 şi art. 9 din Legea nr. 677/2001, chiar şi în mod accidental sau din eroare tehnică (cum a susținut primăria reclamată), reprezintă o

încălcare a prevederilor art. 20 din Legea nr. 677/2001, prin neasigurarea corespunzătoare a măsurilor tehnice şi organizatorice pentru protejarea datelor personale.

Ca atare, la finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a aplicat comunei în cauză, reprezentată prin primar, o sancțiune contravențională în baza art. 33 din Legea nr. 677/2001, întrucât nu a aplicat măsuri tehnice şi organizatorice adecvate, conform art. 19 şi art. 20 din Legea nr. 677/2001, pentru protejarea datelor personale împotriva dezvăluirii acestora pe Internet.

De asemenea, s-au recomandat operatorului următoarele:

- luarea măsurilor necesare astfel încât să se evite publicarea codului numeric personal și a datelor privind starea de sănătate a unor persoane fizice, în afara cadrului legal aplicabil;

- luarea măsurilor necesare respectării dispoziţiilor prevăzute de Codul de procedură fiscală (contactarea în prealabil a contribuabililor), înainte de a recurge la ultima modalitate reglementată (publicitatea prin Internet);

- ştergerea de pe site-ul instituţiei a documentelor ce conţin numele şi prenumele, codul numeric personal, adresa de domiciliu, precum şi menţiunea că este o persoană cu handicap;

- adoptarea unei politici de securitate a prelucrărilor de date efectuate, conform art. 19 şi art. 20 din Legea nr. 677/2001 şi Ordinului Avocatului Poporului nr. 52/2002, inclusiv adoptarea măsurilor care se impun pentru prevenirea dezvăluirii datelor personale ale persoanelor vizate pe site-ul instituţiei în alte situaţii decât cele expres reglementate.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că a încheiat cu o societate de telefonie un contract de abonament şi, ulterior, i-a fost creat un cont pe site-ul societăţii, fără acordul și informarea sa, cont prin intermediul căruia soția sa a avut acces la informații privind convorbirile telefonice ale petentului.

Pentru a putea crea contul de utilizator, petentul a susținut că soția sa şi-a furnizat adresa personală de e-mail (care nu îi aparține petentului) împreună cu datele personale ale petentului (nume, prenume, CNP, număr contract/număr factură).

În urma investigației efectuate s-a constatat faptul că, în procedura de creare a unui cont de utilizator, era necesară furnizarea mai multor informații personale, pe baza numărului de

contract și/sau a numărului de înregistrare a facturii. Confirmarea creării contului se efectua prin trimiterea unui mesaj către adresa de e-mail furnizată la crearea acestuia.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat societatea de telefonie în baza art. 13, pentru încălcarea art. 3 din Legea nr. 506/2004, modificată și completată, întrucât operatorul nu a luat măsuri tehnice și organizatorice adecvate în vederea asigurării securității prelucrării datelor personale și a asigurării unui nivel de securitate proporțional cu riscul existent, care să garanteze că datele personale ale titularilor contractelor încheiate cu societatea de telefonie pot fi accesate numai de persoane autorizate și să protejeze respectivele date personale împotriva accesării ilicite, pentru a preîntâmpina crearea și accesarea unui cont de utilizator de către o altă persoană decât titularul contractului. Lipsa unor astfel de măsuri a dus la crearea și accesarea unui cont pentru petent de către o altă persoană care nu avea dreptul să utilizeze și să acceseze aceste date.

8. Utilizarea de cookies fără respectarea condițiilor legale

Autoritatea națională de supraveghere a primit în cursul anului 2016 o serie de sesizări prin care s-a solicitat verificarea anumitor pagini de Internet înregistrate în România (site-uri aparținând unor unități hoteliere, agenții de anunțuri publicitare sau de recrutare a forței de muncă), din perspectiva respectării condițiilor legale de utilizare a cookie-urilor. Prin intermediul acestor cookies este posibilă realizarea de profile ale utilizatorului de Internet, pe baza cărora ulterior se adresează acestuia publicitate personalizată.

În cazurile investigate, aspectele sesizate au fost confirmate, constatându-se că, deși foloseau astfel de fișiere prin care se colectează informații de pe echipamentele utilizatorilor, site-urile în cauză nu asigurau o informare adecvată a acestora încă de la momentul primei vizite a site-ului, astfel încât să permită o acordare a consimțământului în cunoștință de cauză, așa cum prevede Legea nr. 506/2004.

FIȘĂ DE CAZ

Printr-o petiţie, Autoritatea naţională de supraveghere a fost sesizată cu privire la faptul că pe site-ul unui hotel se prelucrează date personale în mod ilegal. În fapt, petentul a sesizat că pe site-ul respectiv, deși sunt folosite cookie-uri, nu sunt disponibile informaţii privind utilizarea acestora şi nici informaţii privind prelucrarea datelor personale, în condiţiile în care se colectează nume şi prenume, adresa de e-mail şi număr de telefon, date care sunt obligatoriu de furnizat în momentul în care se solicită o ofertă de preţ sau o rezervare.

Din verificarea site-ului, s-au confirmat aspectele reclamate, site-ul utilizând (la data efectuării demersurilor) 7 cookie-uri de pe site-ul respectiv și 11 din alte site-uri; pe site erau disponibile formulare de contact și rezervare prin care se solicitau obligatoriu nume, adresă e-mail, număr telefon, precum și data sosirii/plecării, mic dejun, tip cameră, cât și un formular pentru abonare la ”newsletter” prin care se colectează adresa de poştă electronică. Cu toate acestea, pe site nu se regăseau informații privind protecția datelor personale şi politica de utilizare de cookie-uri, nici date privind identitatea societății care administrează acest site.

Din verificările efectuate şi din testările realizate la data încheierii procesului-verbal, s-a constatat că, independent de opţiunea vizitatorului de a accepta sau nu cookie-urile, informaţiile cookies erau stocate pe echipamentul terminal al utilizatorului.

Prin urmare, utilizarea acestor module cookies la nivelul site-ului nu respectă în mod cumulativ condițiile prevăzute de art. 4 din Legea nr. 506/2004.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul astfel:

- în baza art. 13 prin raportare la art. 4 din Legea nr. 506/2004, întrucât anumite cookies existente la nivelul site-ului sunt stocate pe echipamentele utilizatorilor urmare a accesării site-ului, fără să fie necesară obţinerea acordului expres şi prealabil al utilizatorilor;

- în baza art. 32 din Legea nr. 677/2001 (prelucrarea nelegală a datelor personale), întrucât pe site nu exista niciun fel de informare cu privire la prelucrarea datelor personale colectate inclusiv prin intermediul formularelor de contact şi de rezervare.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată că pe site-ul unei societăți nu există informații referitoare la politica cookies.

În urma investigaţiei efectuate, s-a constatat că în momentul accesării site-ului nu era afișată vreo avertizare, astfel încât utilizatorii site-ului să fie informați referitor la politica de utilizare de cookies și să își poată exprima în cunoștință de cauză acordul cu privire la stocarea lor, anterior navigării pe site. De asemenea, în cadrul site-ului nu exista vreun document care să conțină informarea persoanelor vizate care accesează site-ul, cu privire la politica de cookies.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat contravențional operatorul în baza art. 13 raportat la art. 4 din Legea nr. 506/2004, întrucât nu s-a realizat pe site informarea persoanelor vizate, respectiv a utilizatorilor acestuia, în conformitate cu prevederile art. 12 din Legea nr. 677/2001.

CAPITOLUL V

ACTIVITATEA ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

Cooperarea atât la nivel european, cât și la nivel internațional reprezintă un aspect strategic ce necesită o implicare în toate inițiativele ce se află în curs de dezvoltare. O astfel de cooperare poate avea loc prin participarea la diferite forumuri, cum ar fi Grupul de Lucru Articolul 29, Conferința Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private și Conferinţa de primăvară a Autorităţilor europene pentru protecţia datelor.

În acest context, în anul 2016, după adoptarea în luna mai a Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și a Directivei (UE) 2016/680 referitoare la protecția datelor personale în cadrul activităților specifice desfășurate de autoritățile de aplicare a legii (Directiva referitoare la activitățile polițienești și judiciare), Autoritatea națională de supraveghere a participat la punerea în aplicare a pachetului legislativ în domeniul protecției datelor cu caracter personal.

În calitate de membru al Grupului de Lucru Articolul 29, Autoritatea națională de supraveghere s-a implicat în pregătirea pentru noul cadru de protecție a datelor care va intra în vigoare pe întreg teritoriul UE începând cu data de 25 mai 2018. Astfel, Autoritatea naţională de supraveghere, reprezentantă de membrii săi, a participat în 2016 la o serie de reuniuni şi diverse grupuri de lucru la nivel european. Printre acestea se numără:

- Grupul de Lucru Articolul 29 (înfiinţat în temeiul art. 29 din Directiva 95/46/CE) care reuneşte toate autorităţile europene, precum şi Autoritatea Europeană pentru Protecţia Datelor,
- Subgrupuri de lucru: BTLE, Cooperare, Enforcement, Financial Matters, Future of Privacy, Key provisions, Tehnologie, Transferuri Internaţionale,
- Comitetul Consultativ al Convenţiei 108 al Consiliului Europei (T-PD),
- Organismul comun de control în domeniul Europol şi domeniul Vamal,

➢Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II şi Grupul de coordonare comună Eurodac,

➢Grupul Internaţional de lucru pe Protecţia Datelor în domeniul Telecomunicaţiilor, dedicat protecţiei datelor cu caracter personal în sectorul comunicaţiilor electronice,

➢Grupul de Lucru pe protecţia datelor în cadrul Convenţiei pentru stabilirea Centrului Sud-Est European de aplicare a legii.

Grupul de Lucru Articolul 29

În cursul anului 2016, Grupul de Lucru Articolul 29 și-a exprimat poziția față de probleme fundamentale, precum reforma cadrului European de reglementare (Regulamentul general privind protecția datelor și Directiva referitoare la activitățile polițienești și judiciare), Scutul de Confidențialitate UE-SUA, publicarea datelor cu caracter personal în scopul asigurării transparenței în sectorul public, directiva ePrivacy, construind astfel o protecție eficientă a datelor cu caracter personal la nivel european.

Astfel, menționăm următoarele documente ce au fost adoptate fie sub formă de avize, fie sub formă de documente de lucru sau declarații:

- planul de acțiune 2016 pentru implementarea Regulamentului general privind protecția datelor – planul de acțiune a fost conceput pentru anul 2016 și își propune să stabilească prioritățile Grupului de Lucru Articolul 29 în ceea ce privește pregătirea pentru trecerea la noul cadru juridic, în special Comitetul European pentru Protecția Datelor (European Data Protection Board – EDPB);
- justificarea interferențelor cu drepturile fundamentale la viață privată și la protecţia datelor prin intermediul unor măsuri de supraveghere în cazul transferului de date cu caracter personal (Garanții esențiale europene – European Essential Guarantees) – Grupul de Lucru Articolul 29 a utilizat jurisprudența pentru a identifica Garanțiile esențiale europene care ar trebui să fie implementate, astfel încât să se asigure că interferențele cu drepturile fundamentale nu depășesc ceea ce este necesar într-o societate democratică. Aceste garanții se bazează în primul rând pe jurisprudența CJUE și a CEDO în cauzele privind aplicarea drepturilor la viață privată și la protecția datelor în Europa. Acest lucru înseamnă că respectivele garanții sunt aplicabile, în primul rând, în statele membre UE și ale Consiliului Europei în momentul aplicării legislației europene sau naționale ce interferează cu aceste drepturi. Grupul de Lucru

Articolul 29 subliniază faptul că aceste garanții au la bază drepturile fundamentale și sunt aplicabile oricărei persoane indiferent de naționalitatea acesteia.

În urma evaluării jurisprudenței, Grupul de Lucru Articolul 29 a ajuns la concluzia că cerințele pot fi rezumate în 4 garanții esențiale europene și anume: a) prelucrarea trebuie efectuată în baza unor reguli clare, precise și accesibile; b) necesitatea și proporționalitatea în ceea ce privește obiectivele legitime urmărite trebuie demonstrate; c) trebuie să existe un mecanism independent de supraveghere; d) persoana fizică trebuie să dispună de căi de atac eficiente;

- scutul de confidențialitate UE-SUA – documentul oferă o analiză a proiectului de decizie a Comisiei Europene și a anexelor sale, ce constituie un nou cadru legal pentru schimbul transatlantic de date cu caracter personal în scopuri comerciale, respectiv Scutul de Confidențialitate UE-SUA care încearcă să înlocuiască Principiile Safe Harbor invalidate de Curtea de Justiție a Uniunii Europene în octombrie 2015, în cauza Schrems. Grupul de Lucru Articolul 29 a identificat anumite îmbunătățiri prin comparație cu mecanismul anterior. În acest context, menționăm creșterea transparenței în ceea ce privește accesul public la datele transferate în temeiul Scutului de Confidențialitate, fie în scop de securitate națională, fie în scop de aplicare a legii. De asemenea, este binevenit faptul că toate transferurile de date către SUA vor beneficia de aceeași protecție; nu există prevederi legale specifice în vigoare care să ofere un avantaj unui anumit instrument. Cu toate acestea, există trei preocupări care, în opinia Grupului de Lucru Articolul 29 trebuie abordate și anume: i) textul proiectului de decizie al Comisiei Europene nu obligă organizațiile să șteargă anumite date în cazul în care acestea nu mai sunt necesare; un element esențial al dreptului UE privind protecția datelor se referă la faptul că datele sunt păstrate pe perioada strict necesară atingerii scopului pentru care au fost colectate; ii) nu este exclusă în totalitate colectarea în masă a datelor; Grupul de Lucru Articolul 29 a susținut în mod constant faptul că o asemenea colectare de date reprezintă o ingerință nejustificată în drepturile fundamentale ale persoanelor fizice; iii) mecanismul Ombudsperson; chiar dacă este salutată crearea unei căi de atac suplimentare și a unui mecanism de supraveghere pentru persoanele fizice, există totuși motive de îngrijorare în ceea ce privește stabilirea faptului dacă Ombudsperson dispune de suficiente competențe

pentru a funcționa eficient; astfel, trebuie clarificate atât competențele, cât și poziția Ombudsperson pentru a se demonstra că este într-adevăr independent și poate oferi o cale de atac eficientă. Grupul de Lucru Articolul 29 salută îmbunătățirile oferite de Scutul de Confidențialitate și îndeamnă, în același timp, Comisia Europeană să rezolve preocupările exprimate, să identifice soluțiile adecvate și să ofere clarificările solicitate de Grupul de Lucru Articolul 29;

- publicarea datelor cu caracter personal în scopul asigurării transparenței în sectorul public – avizul explică modul de aplicare a principiilor de protecție a datelor cu caracter personal în ceea ce privește prelucrarea și publicarea datelor cu caracter personal în scopul asigurării transparenței în sectorul public, în special atunci când este vorba de măsuri de anticorupție și de gestionarea și prevenirea conflictelor de interes. Documentul nu încearcă să sugereze ce informații ar trebui să fie disponibile prin intermediul accesului la documente publice/legislația privind libera informare din statele membre, nu limitează disponibilitatea unor astfel de informații publice în conformitate cu legislația națională și nici nu acoperă implementarea Regulamentului 45/2001 și a Regulamentului 1049/2001 aplicabile instituțiilor și organismelor UE. Obiectivul opiniei este de a oferi îndrumări practice, recomandări și exemple de bune practici pentru legiuitorii și instituțiile competente din statele membre cu privire la modul în care se pot asigura că dreptul la protecția datelor este respectat, asigurându-se, în același timp, un echilibru cu interesul public legitim de a avea acces la informații;
- evaluarea și revizuirea Directivei ePrivacy (2002/58/CE) – evoluţiile de pe piaţa digitală, alături de recenta adoptare a Regulamentului general privind protecţia datelor, impun o revizuire aprofundată a normelor prevăzute în Directiva 2002/58/CE (Directiva ePrivacy). Revizuirea Directivei ePrivacy trebuie să conducă la un sistem de reglementare coerent şi eficient şi să ofere certitudine juridică cu privire la prevederile legale aplicabile în orice situaţie cu un regim special. Directiva ePrivacy a oferit, încă din 2002, un set de măsuri suplimentare de securitate şi confidenţialitate cu un accent special asupra furnizorilor de telefonie şi Internet. Articolul 1(2) din Directiva ePrivacy prevede că aceasta a fost adoptată în vederea particularizării şi completării Directivei privind protecţia datelor 95/46/CE, care va fi abrogată de Regulamentul general privind protecţia datelor, ce va deveni aplicabil începând cu data de 28 mai 2018. În

acest sens, Grupul de Lucru Articolul 29 sprijină recunoaşterea necesităţii de a avea reguli specifice pentru comunicaţiile electronice în UE. Astfel, noul instrument va oferi protecţie suplimentară comunicaţiilor electronice efectuate atât de persoane fizice, cât şi de persoane juridice. Directiva ePrivacy revizuită ar trebui să păstreze substanţa dispoziţiilor existente, dar, în practică, acestea să fie mai eficiente şi mai funcţionale, prin extinderea domeniului de aplicare a regulilor privind geolocalizarea şi datele de trafic pentru toate părţile implicate, introducând în acelaşi timp condiţii mai exacte care să aibă în vedere viaţa privată a utilizatorilor ale căror date sunt prelucrate.

Comitetul Consultativ al Convenţiei 108 al Consiliului Europei

În anul 2016, activitățile desfășurate la nivelul Comitetului Consultativ al Convenţiei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cunoscută sub denumirea de Convenția 108, la care a participat Autoritatea naţională de supraveghere au vizat, în primul rând modernizarea Convenției 108, stabilirea unor criterii în vederea respectării cerințelor de protecție a datelor cu caracter personal în contextul schimbului automat de date cu caracter personal în scopuri fiscale, prelucrarea datelor pasagerilor (datele PNR). Ca urmare a preocupărilor legate de reacțiile atacurilor și amenințărilor teroriste, în cursul anului 2016, Comitetul Consultativ al Convenției 108 a adoptat Opinia referitoare la implicaţiile prelucrării datelor PNR asupra protecţiei datelor. Astfel, având în vedere în special implicaţiile asupra dreptului la protecţia datelor şi a dreptului la protecţia vieţii private pe care măsurile PNR le-ar putea avea, textul documentului subliniază importanța demonstrării și respectării legalității, proporționalității și necesității unui sistem PNR, ţinându-se cont în special de următoarele aspecte:

- demonstrarea în mod transparent a necesităţii şi proporţionalităţii sistemului în funcţie de scopul legitim urmărit;
- existenţa unor definiţii precise şi stricte ale scopului legitim urmărit, prelucrarea datelor PNR fiind permisă doar în scopurile limitate astfel definite (prevenirea, detectarea, cercetarea şi urmărirea infracţiunilor teroriste şi a altor infracţiuni grave sau, în situaţii, excepţionale, prevenirea ameninţărilor grave la adresa publicului);
- publicarea unei liste cu autorităţile publice competente;
- transmiterea datelor prin metoda „push”, stabilindu-se în mod clar perioada iniţială de stocare a datelor şi a măsurilor de securitate corespunzătoare;

➢interzicerea transferului sistematic de date cu caracter special;

➢limitarea minimizării datelor la riscurile predefinite de indicatori;

➢limitări legale şi doar necesare ale drepturilor la informare, de acces, de rectificare şi de ştergere;

➢competenţele autorităţilor pentru protecţia datelor (de a fi consultate şi de a putea evalua sistemul PNR, precum şi de a soluţiona plângerile persoanelor fizice);

➢existenţa căilor de atac administrative şi judiciare eficiente pentru persoanele fizice;

➢monitorizarea şi supravegherea independentă şi externă a sistemului PNR;

➢revizuirea periodică a sistemelor PNR de către autorităţile competente.

Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II şi Grupul de coordonare comună Eurodac

Cadrul legal pentru protecţia datelor din sistemul VIS este constituit din reguli specifice conţinute în actele normative ce guvernează acest sistem, respectiv Regulamentul (CE) 767/2008 din 9 iulie 2008 şi Decizia Consiliului 2008/633/JAI, care completează prevederile Cartei Drepturilor Fundamentale a Uniunii Europene, Directiva 95/46/CE, Regulamentul (CE) 45/2001, Decizia Cadru a Consiliului 2008/977/JAI, Convenţia 108.

Activitatea Grupului de coordonare comună VIS a vizat, printre altele, o analiză a accesului la datele din sistemul VIS şi a drepturilor persoanelor vizate. Astfel, pe baza răspunsurilor la chestionarele transmise autorităților pentru protecția datelor, au fost întocmite rapoarte privind autoritățile desemnate să aibă acces la datele din sistemul VIS, scopurile în care acestea pot utiliza sistemul, respectiv drepturile persoanelor vizate.

Astfel, asigurarea că persoanele vizate își pot exercita, în mod eficient, drepturile specifice conferite de legislația în domeniu este absolut necesară în sectorul acordării vizelor, unde respectarea cadrului legal este esențială.

Urmare analizei, Grupul de coordonare comună VIS a emis recomandări, precum:

➢actualizarea listei consolidate a autorităţilor competente să aibă acces la VIS, publicată de Comisie;

➢elaborarea şi adoptarea formală de către autorităţile naţionale competente a regulilor interne privind accesul şi utilizarea datelor VIS, precum şi a regulilor de protecţie a datelor cu caracter personal;

➢referitor la procedurile instituite pentru a răspunde la cererile de acces, intervenţie sau ştergere a datelor personale stocate în sistem, statele membre sunt încurajate să adopte perioade maxime armonizate de răspuns.

Referitor la activitatea Grupului de coordonare comună SIS II, în anul 2016 a fost finalizat modelul comun de inspecție a alertelor elaborat de subgrupul format din reprezentanţi ai autorităţilor pentru protecţia datelor din Belgia, Franţa, Lituania, Malta şi România.

Documentul se axează pe aspectele de legalitate, completând documentul privind securitatea datelor elaborat de subgrupul format din experții IT, și este structurat în două părți:

i) întrebări specifice referitoare la fiecare alertă; ii) întrebări generale relevante pentru fiecare alertă, spre exemplu, utilizarea abuzivă a identității, calitatea datelor, păstrarea datelor.

În ceea ce privește sistemul Eurodac, acesta a fost înființat prin Regulamentul Consiliului (CE) nr. 2725/2000 din 11 decembrie 2000 (Regulamentul Eurodac) care a fost completat de Regulamentul Consiliului (CE) nr. 407/2002 din 28 februarie 2002. Textele celor 2 regulamente au fost abrogate de Regulamentul (UE) nr. 603/2013 din 26 iunie 2013 (Regulamentul Eurodac Reformă), care a devenit aplicabil din data de 20 iulie 2015.

Având în vedere noul cadru juridic Eurodac, Grupul de coordonare comună Eurodac a stabilit în cadrul reuniunii sale din aprilie 2016, ca parte a programului de lucru 2015-2018, adaptarea Planului comun de inspecții la noile cerințe legale ale Regulamentului Reformă. Revizuirea planului de inspecții din 2012 a fost efectuată de reprezentanţii autorităţilor pentru protecţia datelor din România și Regatul Unit.

Documentul este structurat astfel încât să sprijine autoritățile pentru protecția datelor în îndeplinirea atribuțiilor specifice de supraveghere (în conformitate cu art. 30), precum și în efectuarea auditului anual obligatoriu (în conformitate cu art. 32(2)) și a investigațiilor la sistemul Eurodac. Documentul și structura acestuia oferă o metodologie fiabilă pentru verificarea punctelor de acces naționale Eurodac și, de asemenea, permite o mai bună analiză a rezultatelor verificărilor efectuate de autoritățile naționale pentru protecția datelor.

Organismul comun de control în domeniul Europol (Joint Supervisory Body Europol – JSB Europol)

JSB Europol - format din reprezentanți ai autorităților pentru protecția datelor din statele membre UE, precum și din reprezentanți ai Consiliului Uniunii - reprezintă organismul comun de supraveghere a modului în care autoritățile polițienești respectă prevederile legale referitoare la protecția datelor cu caracter personal, în cadrul activităților specifice de cooperare ale autorităților polițienești desfășurate prin intermediul sistemului informatic pus la dispoziție de Europol.

În data de 11 mai 2016 Parlamentul European și Consiliul au adoptat Regulamentul (UE) 2016/794[1] care reglementează activitățile desfășurate la nivelul Europol și înlocuiește Deciziile adoptate anterior de către Consiliul Uniunii. Prevederile noului Regulament Europol vor fi aplicabile începând cu data de 1 mai 2017.

În acest fel a fost modificat și cadrul în care autoritățile pentru protecția datelor vor putea coopera în acest domeniu. JSB Europol va fi înlocuit, de la data la care vor fi aplicabile prevederile noului Regulament Europol, de un nou organism de supraveghere comună – denumit Consiliu de Cooperare. În cadrul acestui nou organism de cooperare vor participa reprezentanți ai autorităților pentru protecția datelor din statele membre UE, precum și cei ai Autorității Europene pentru Protecția Datelor (European Data Protection Supervisor - EDPS).

Având în vedere modificările aduse cadrului normativ, și în acest an acțiunile organismului comun de supraveghere – JSB Europol s-au axat pe asigurarea unei tranziții cât mai eficiente a activităților către noua formă de cooperare stabilită de art. 45 din Regulamentul European, respectiv Consiliul de Cooperare. Scopul principal este acela de a asigura continuitatea și consistența activității de supraveghere asigurată de autoritățile pentru protecția datelor și AEPD.

Noul organism comun de supraveghere va prelua activitățile aflate în curs la nivelul JSB Europol și va încerca să evite suprapunerea sau ”dublarea” unor exerciții desfășurate în trecut la nivelul JSB Europol.

[1] Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului

Grupul Internaţional de lucru pentru Protecţia Datelor în domeniul Telecomunicaţiilor

Dezbaterile din cadrul reuniunilor Grupului Internaţional de lucru pentru Protecţia Datelor în domeniul Telecomunicaţiilor din anul 2016 au vizat subiecte precum utilizarea datelor biometrice pentru autentificarea electronică, viaţa privată în cadrul reţelelor de socializare, viaţa privată în ceea ce privește „noua generaţie a Serviciului Director de Înregistrare" (RDS – Registration Directory Service) ICANN, viaţa privată şi securitatea în legătură cu Internetul de telefonie (VoIP), viaţa privată în cadrul platformelor de tip e-learning.

Discuțiile s-au concretizat prin adoptarea documentului de lucru privind aspecte de viaţă privată şi securitate în legătură cu Internetul de telefonie (VoIP). Chiar dacă tehnologiile utilizate de companii diferă, riscurile privind confidențialitatea și protecția datelor cu caracter personal sunt similare, iar recomandările sunt aplicabile tuturor tipurilor de servicii multi-media, respectiv:

- furnizorii de servicii VoIP trebuie să informeze clienții cu privire la caracteristicile de confidențialitate și securitate ale serviciilor VoIP pe care le oferă;
- producătorii de hardware și software trebuie să efectueze analize de impact asupra vieții private și, de asemenea, să implementeze măsuri tehnice corespunzătoare;
- furnizorii de VoIP trebuie să ofere clienților posibilitatea de portabilitate a datelor;
- furnizorii, dezvoltatorii de software și hardware ce prelucrează date de trafic trebuie să respecte principiul limitării scopului.

Grupul de Lucru pentru protecţia datelor în cadrul Convenţiei pentru stabilirea Centrului Sud-Est European de aplicare a legii (PCC SEE)

Pe baza concluziilor primei reuniuni a Grupului de Lucru pentru protecţia datelor din cadrul PCC SEE, subgrupul „Friends-of-Chairmanship", format din reprezentații autorităţilor naţionale pentru protecţia datelor şi ai ministerelor de interne din Ungaria, Macedonia, Moldova, România, Muntenegru – care asigura preşedinţia grupului, şi Secretariatul PCC SEE au realizat o analiză comună a răspunsurilor la chestionarul privind aplicarea la nivel naţional a prevederilor referitoare la protecţia datelor în cadrul PCC SEE.

În acest context, subgrupul recomandă ca aplicarea practică a schimbului de informaţii în cadrul PCC SEE să înceapă cât mai curând posibil, astfel încât să fie intensificată abilitatea de a aborda ameninţările care apar la adresa securităţii regionale, dar şi europene. În același timp, subgrupul „Friends-of-Chairmanship" a constatat că este în vigoare un cadru juridic suficient pentru schimbul transfrontalier de informaţii în cadrul PCC SEE.

A 38-a Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private

Prima Conferință Internațională a Comisarilor din domeniul Protecției Datelor și a Vieții Private a avut loc în anul 1979 și reprezintă primul forum mondial al autorităților pentru protecția datelor.

Conferința urmărește să ofere îndrumări și recomandări la nivel internațional în domeniul protecției datelor și a vieții private, prin conectarea autorităților în domeniu din întreaga lume.

În anul 2016, cea de-a 38a Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private a fost organizată de Autoritatea pentru protecţia datelor din Maroc. În cadrul evenimentului au fost adoptate 5 rezoluții privind:

- promovarea unui cadru normativ internaţional privind creșterea gradului de conștientizare în domeniul vieţii private
- setul internațional de instrumente pentru protecția datelor personale și a vieții private a elevilor
- dezvoltarea unor noi standarde în reglementările privind protecţia datelor
- apărătorii dreptului omului
- consolidarea cooperării internaţionale.

Conferinţa de primăvară a autorităţilor europene pentru protecţia datelor

Conferința de primăvară a autorităților europene pentru protecția datelor reprezintă una dintre cele mai importante întâlniri anuale a tuturor comisarilor pentru protecția datelor din statele membre UE și din celelalte state europene.

În cadrul evenimentului din 2016, organizat de autoritatea pentru protecția datelor din Ungaria, temele dezbătute s-au concentrat asupra a trei aspecte importante în contextul european actual, respectiv:

- perspectiva protecției datelor în ceea ce privește supravegherea serviciilor naționale de informații
- reforma cadrului legal european privind protecția datelor, respectiv noile atribuții ale autorităților pentru protecția datelor prevăzute de Regulamentul general privind protecția datelor și Directiva referitoare la activitățile polițienești și judiciare
- modernizarea Convenției 108.

În cadrul conferinței au fost adoptate 2 rezoluții: rezoluția privind noul cadru de cooperare și rezoluția privind transferul de date cu caracter personal.

Misiuni de evaluare Schengen

Un aspect important în activitatea Autorității naționale de supraveghere în plan extern l-a constituit participarea, în anul 2016, la misiunile de evaluare Schengen în domeniul protecţiei datelor din Luxemburg, Italia și Malta.

Misiunile Schengen se referă la evaluarea și monitorizarea aplicării acquis-ului Schengen, respectiv analizarea modului de implementare a regulilor de protecție a datelor cu caracter personal, asigurându-se astfel că statele membre aplică reglementările Schengen în mod eficient și în conformitate cu principiile și normele fundamentale. La finalul fiecarei misiuni de evaluare se întocmește un raport pe baza răspunsurilor transmise de statul evaluat la chestionarul standard[2] și a informațiilor furnizate de autoritățile statului respectiv pe durata vizitei de evaluare. Respectivul document conține, printre altele, constatări și evaluări privind cadrul legislativ, autoritatea pentru protecția datelor, asigurarea drepturilor persoanelor vizate, cooperarea internațională.

Pachetul legislativ referitor la domeniul protecţiei datelor personale

[2] Art. 9 din Regulamentul (UE) NR. 1053/2013 al Consiliului din 7 octombrie 2013 de instituire a unui mecanism de evaluare și monitorizare în vederea verificării aplicării acquis-ului Schengen și de abrogare a Deciziei Comitetului executiv din 16 septembrie 1998 de instituire a Comitetului permanent pentru evaluarea și punerea în aplicare a Acordului Schengen

După o perioadă de mai bine de 4 ani de negocieri, anul 2016 a fost marcat de adoptarea de către Parlamentul European, în data de 14 aprilie 2016, a pachetului legislativ privind protecţia datelor personale la nivelul Uniunii Europene, compus din două instrumente legislative: Regulamentul general privind protecția datelor şi Directiva care stabileşte reguli specifice de protecţie a datelor cu caracter personal aplicabile în activităţile specifice desfăşurate de autorităţile de aplicare a legii. Astfel, Regulamentul general privind protecția datelor va înlocui Directiva 95/46/CE, actualul cadru legal în domeniul protecţiei datelor cu caracter personal, iar prevederile acestuia vor fi direct aplicabile la nivelul tuturor statelor membre ale Uniunii, stabilind astfel un set unic de reguli în întreaga Uniune Europeană.

Regulamentul aduce o serie de modificări necesare regulilor stabilite acum mai bine de două decenii de Directiva 95/46/CE, care au fost, de altfel, principalele obiective urmărite de Comisia Europeană atunci când a propus primul proiect de text în ianuarie 2012:

- **pentru cetățeni** – drepturile vor fi consolidate. Persoanele fizice vor putea obține informații suplimentare cu privire la modul în care datele personale sunt prelucrate, într-o formă clară, accesibilă și ușor de înțeles. Dreptul de a fi uitat este consolidat, iar un nou drept – dreptul la portabilitatea datelor – este introdus, oferind cetățenilor un control mai bun asupra datelor lor personale. De asemenea, este prevăzută o protecție specială pentru viața privată a minorilor;
- **pentru companii** – formalitățile administrative sunt simplificate și există posibilitatea de a avea un „interlocutor" unic pentru toate autoritățile europene pentru protecția datelor. De asemenea, este pus la dispoziție un set de instrumente de conformitate care include, spre exemplu, codul de conduită, mecanismul de certificare, ce pot fi adaptate nivelului de riscuri la adresa drepturilor și libertăților persoanelor vizate (prin consultarea autorităților pentru protecția datelor);
- **pentru autoritățile pentru protecția datelor –** intensificarea atribuțiilor, inclusiv aplicarea de măsuri coercitive și de amenzi administrative de până la 20 milioane de euro sau de până la 4% din cifra de afaceri a unei companii. În același timp, autoritățile pentru protecția datelor pot lua decizii comune, indiferent dacă este vorba

despre emiterea unor recomandări privind respectarea cadrului legal sau aplicarea unei sancțiuni, oferindu-se astfel o protecție mai mare pentru persoanele fizice;

- **cooperarea între autoritățile pentru protecția datelor va fi reorganizată și va include un organism european – Comitetul European pentru Protecția Datelor (European Data Protection Board - EDPB)** va răspunde de medierea dezacordurilor dintre autoritățile pentru protecția datelor, precum și de elaborarea unui set de principii „europene".

Prevederile Regulamentului general privind protecția datelor vor fi aplicabile începând cu data de 25 mai 2018.

Sistemul Intrări/Ieșiri (Entry/Exit System - EES)

În februarie 2013, Comisia Europeană a prezentat un pachet de propunere legislativă privind Frontierele Inteligente în vederea modernizării managementului frontierelor externe ale zonei Schengen. Pachetul era format din 3 propuneri legislative:

- propunere de Regulament privind instituirea sistemului de intrare/ieşire (Entry/Exist System – EES) pentru înregistrarea datelor referitoare la intrarea şi ieşirea resortisanţilor ţărilor terţe care intră în spațiul Schengen,
- propunere de Regulament privind instituirea programului de înregistrare a călătorilor (RTP),
- propunere de regulament de modificare a Codului Frontierelor Schengen[3].

În urma dezbaterilor din cadrul reuniunilor organizate la nivel european, Comisia Europeană a considerat ca fiind necesare îmbunătățirea și simplificarea propunerilor din 2013. Astfel, Comisia Europeană a decis următoarele: revizuirea propunerii din 2013 de regulament pentru stabilirea unui Sistem Intrări/Ieșiri (EES); revizuirea propunerii din 2013 de modificare a Codului Frontierelor Schengen pentru a integra modificările tehnice rezultate din noua propunere de regulament ce stabilește Sistemul Intrări/Ieșiri; retragerea propunerii din 2013 de regulament privind instituirea programului de înregistrare a călătorilor (RTP).

[3] COM(2013) 95 FINAL, COM(2013) 97 FINAL și COM(2013) 96 FINAL.

Domeniul de aplicare a noului Sistem Intrări/Ieșiri include punctele de trecere a frontierei de către toți resortisanții țărilor terțe care vizitează spațiul Schengen pentru o scurtă ședere (perioada maximă de ședere de 90 de zile în orice perioadă de 180 de zile), atât pentru călătorii cu viză, cât și pentru cei scutiți de viză sau, eventual, în baza unei vize de turism.

Membrii de familie ai cetățenilor UE ce se bucură de dreptul la libera circulație sau ai resortisanților țărilor terțe care se bucură de aceleași drepturi de liberă circulație echivalente cu cele ale cetățenilor UE, precum și cetățenii ce nu au încă un permis de ședere ar trebui să fie înregistrați în Sistemul Intrări/Ieșiri, dar nu se supun regulilor de scurtă ședere, iar controalele se efectuează în conformitate cu Directiva 2004/38/CE[4]. Membrii de familie aflați în posesia unui permis de ședere prevăzut în Directiva 2004/38/CE sunt excluși de la Sistemul de Intrări/Ieșiri.

Acest sistem va colecta datele și va înregistra intrările și ieșirile atât în vederea facilitării trecerii frontierei călătorilor bona fide, cât și pentru o mai bună identificare a persoanelor ce depășesc perioada de ședere. De asemenea, sistemul va înregistra refuzurile de intrare a resortisanților țărilor terțe care intră sub incidența domeniului de aplicare a regulamentului.

Sistemul european de informații și de autorizare privind călătoriile (European Travel Information and Authorisation System – ETIAS)

În Comunicarea Comisiei Europene din 14 septembrie 2016, intitulată „Creșterea nivelului de securitate într-o lume a mobilității: îmbunătățirea schimbului de informații în cadrul combaterii terorismului și consolidarea frontierelor externe”[5], Comisia a confirmat necesitatea de a găsi un echilibru între asigurarea mobilității și întărirea securității, facilitând în același timp intrarea legală în spațiul Schengen fără a avea nevoie de viză. Liberalizarea vizelor s-a dovedit un instrument important în dezvoltarea de parteneriate cu țări terțe, inclusiv ca mijloc de asigurare a unor sisteme eficace în materie de returnare și readmisie.

În acest sens, Comisia Europeană a lansat un studiu de fezabilitate[6] referitor la instituirea unui sistem european de informații și de autorizare privind călătoriile (ETIAS).

[4] Directiva 2004/38/CE a Parlamentului European și a Consiliului privind dreptul la liberă circulație și ședere pe teritoriul statelor membre pentru cetățenii Uniunii și membrii familiilor acestora, de modificare a Regulamentului (CEE) nr. 1612/68 și de abrogare a Directivelor 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE și 93/96/CEE.

[5] COM(2016) 602 final

[6] Studiu de fezabilitate referitor la un sistem european de informații și de autorizare privind călătoriile (ETIAS), raport final; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents/docs/20161116/etias_feasability_study_en.pdf.

În acest context, menționăm că ETIAS va fi un sistem automat, înființat pentru identificarea eventualelor riscuri prezentate de un vizitator exonerat de obligația de a deține viză care călătorește în spațiul Schengen și va colecta informații cu privire la acești vizitatori înainte de începerea călătoriei, pentru a permite prelucrarea prealabilă a datelor.

Prin urmare, funcția principală a ETIAS ar consta în verificarea informațiilor transmise de către resortisanții țărilor terțe exonerați de obligația de a deține viză, prin intermediul unei cereri online, înainte de sosirea lor la frontierele externe ale UE, pentru a stabili dacă aceștia prezintă anumite riscuri în materie de migrație neregulamentară, securitate sau sănătate publică.

Scutul de Confidențialitate UE-SUA (Privacy Shield EU-US)

În luna februarie 2016, Comisia Europeană a publicat Comunicarea Comisiei către Parlamentul European și Consiliu „Fluxuri de date transatlantice: restabilirea încrederii prin garanții puternice”[7], un proiect de decizie privind nivelul de protecție adecvat și axele ce constituie noul cadru legal pentru schimbul transatlantic de date cu caracter personal în scopuri comerciale: Scutul de Confidențialitate UE-SUA care înlocuiește Principiile Safe Harbor invalidate de Curtea de Justiție a Uniunii Europene în data de 6 octombrie 2015 în cauza Schrems[8].

Documentația publicată de Comisia Europeană a făcut obiectul analizei autorităților pentru protecția datelor reunite sub egida Grupului de Lucru Articolul 29, care a avut drept finalitate emiterea unui aviz[9]. Astfel, a fost analizată, pe de o parte, activitatea comercială a Scutului de Confidențialitate și, pe de altă parte, garanțiile instituite în legătură cu derogările de la principiile Scutului de Confidențialitate pentru scopurile de securitate națională și interes public.

În luna august a anului 2016 a fost publicată în Jurnalul Oficial al Uniunii Europene Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului privind caracterul adecvat al protecţiei oferite de Scutul de confidenţialitate UE-SUA.

Potrivit acestei decizii, Statele Unite garantează un nivel adecvat de protecţie a datelor cu caracter personal transferate din Uniunea Europeană către organizaţii din Statele Unite în

[7] COM(2016)117 final, 29 februarie 2016
[8] Cauza C-362/14 - Maximilian Schrems v. Data Protection Commissioner, 6 octombrie 2015
[9] Avizul 01/2016 (WP238)

temeiul Scutului de confidenţialitate UE-SUA, cu condiţia ca respectivele entităţi să prelucreze datele cu caracter personal în conformitate cu un set puternic de principii şi garanţii pentru protecţia vieţii private şi a datelor cu caracter personal care sunt echivalente cu cele din Uniunea Europeană.

În același timp, în sprijinul persoanelor fizice, tot în luna august 2016 a fost publicat pe pagina web a Comisiei Europene Ghidul cetăţeanului referitor la Scutul de confidenţialitate UE-SUA[10].

Ghidul cetăţeanului oferă informaţii generale privind Scutul de confidenţialitate UE-SUA, dar, în acelaşi timp, prezintă într-o formă succintă obligaţiile companiilor ce sunt parte la Scutul de confidenţialitate UE-SUA, precum şi drepturile de care beneficiază persoanele vizate cu privire la prelucrarea datelor cu caracter personal: dreptul la informare, dreptul de acces la date, dreptul de intervenţie asupra datelor, precum şi dreptul de a se adresa cu plângere.

Astfel, Ghidul cetăţeanului oferă informaţii în legătură cu modalitatea în care persoana vizată se poate adresa cu plângere împotriva unei companii din SUA ce prelucrează date cu caracter personal în temeiul Scutului de confidenţialitate UE-SUA la următoarele entităţi: compania din SUA, organismul independent de soluţionare alternativă a litigiilor (Alternative dispute resolution Body - ADR), autoritatea naţională pentru protecţia datelor, Departamentul de Comerţ, Comisia Federală pentru Comerţ, Comitetul de Arbitraj al Scutului de confidenţialitate UE-SUA.

[10] http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf

CAPITOLUL VI

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

În anul 2016, Autoritatea națională de supraveghere a soluţionat **7.445** solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări şi cereri prin care se solicita punctul de vedere sau clarificarea unor aspecte ce ţin de prelucrările de date cu caracter personal efectuate de aceştia.

Au fost soluţionate 6930 notificări privind prelucrări de date cu caracter personal, dintre care 5480 efectuate pe teritoriul României şi 1450 transferuri de date în străinătate.

Din cele 1450 notificări cu transferuri de date către entităţi din străinătate, în 1205 au fost declarate transferuri către state din Uniunea Europeană, Zona Economică Europeană și din state terţe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield), precum şi transferuri către state terţe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată şi completată.

Totodată, au fost notificate 245 de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, în baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules).

În urma analizării transferurilor de date în străinătate către state terţe, a fost emis un număr de 37 autorizaţii de transfer.

În acelaşi timp, au fost analizate 515 solicitări ale operatorilor privind aspecte referitoare la dispoziţiile Legii nr. 677/2001, modificată şi completată.

Secţiunea 1 – Activitatea de înregistrare a prelucrărilor de date

Potrivit Legii nr. 677/2001, notificarea reprezintă regula pentru declararea prelucrărilor de date personale. În funcţie de caracterul unor prelucrări şi de riscurile pe care le presupun pentru viaţa privată, Autoritatea naţională de supraveghere poate stabili scutiri de la obligaţia de notificare. Astfel, ţinând cont de faptul că anumite prelucrări sunt recurente în activitatea

unui operator, nu implică prelucrarea unor date sensibile sau sunt prevăzute ca obligaţii legale în baza unor acte normative, preşedintele Autorităţii naţionale de supraveghere a emis Decizia nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum şi pentru modificarea şi abrogarea unor decizii, care a intrat în vigoare la data de 28 decembrie 2015.

Acest act normativ a fost emis în aplicarea prevederilor art. 22 alin. (9) din Legea nr. 677/2001, conform cărora Autoritatea națională de supraveghere poate stabili şi cazuri în care notificarea nu este necesară. Totodată, s-au luat în considerare prevederile Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE referitoare la eliminarea obligaţiei operatorilor de a notifica autorităţile naţionale de supraveghere pentru prelucrările de date efectuate.

Sub incidența prevederilor Deciziei 200/2015, Autoritatea națională de supraveghere a înregistrat în registrul de evidenţă a prelucrărilor de date cu caracter personal, în principal, următoarele prelucrări de date:

- prelucrarea datelor care permit localizarea geografică a persoanelor fizice prin mijloace de comunicații electronice (monitorizarea/securitatea persoanelor şi/sau bunurilor publice/private prin utilizarea GPS-ului);
- prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea şi/sau evaluarea unor aspecte de personalitate, precum competenţa profesională, credibilitatea, comportamentul sau alte asemenea (crearea şi utilizarea de profiluri ale persoanelor vizate în vederea transmiterii unor newsletteruri, semnalarea încălcării codurilor de conduită în mediul privat - whistleblowing);
- prelucrarea datelor cu caracter personal ale minorilor efectuată prin intermediul internetului sau al mesageriei electronice (publicarea rezultatelor la diferite concursuri şcolare şi extraşcolare, postarea unor imagini din tabere școlare);
- prelucrarea datelor efectuată prin mijloace de supraveghere video în scopul monitorizării/securităţii persoanelor, spaţiilor şi/sau bunurilor publice/private.

Referitor la utilizarea sistemului de geolocalizare GPS, Autoritatea națională de supraveghere a apreciat că aceasta 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.

De asemenea, ca şi în anii anteriori, numeroşi operatori, în special din mediu privat, au notificat Autoritatea națională de supraveghere pentru prelucrările efectuate în scopul monitorizării propriilor angajaţi prin mijloace de supraveghere video.

În ceea ce priveşte supravegherea video a angajaţilor, Autoritatea națională de supraveghere a atras atenţia că implementarea unui sistem de videosupraveghere a acestora poate afecta drepturile salariaţilor, astfel că, în plus faţă de dispoziţiile Legii nr. 677/2001, modificată şi completată şi ale art. 8 din Decizia nr. 52/2012, trebuie respectate şi 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 reprezentanţilor salariaţilor.

În plus, entităţi din domeniul imobiliar, hotelier, furnizori de utilități, precum şi entităţi care desfăşoară o activitate independentă, autorizată în baza unei legi speciale (birouri de executori judecătorești, cabinete de mediatori, societăți de avocatură, cabinete medicale individuale) au notificat Autorității naționale de supraveghere prelucrările pe care le efectuează în scopul îndeplinirii atribuţiilor lor legale.

Autoritatea națională de supraveghere a informat aceste entităţi că au calitatea de operator şi implicit obligaţia de a respecta legislaţia din domeniul protecţiei datelor, în special prevederile art. 12, 19 şi 20 din Legea nr. 677/2001, modificată şi completată, însă sunt scutite de obligaţia de a notifica.

Astfel, scutirea de obligaţia de a notifica Autoritatea naţională de supraveghere nu exonerează operatorii de îndeplinirea celorlalte obligaţii care le revin potrivit dispoziţiilor legale aplicabile în domeniul protecţiei datelor cu caracter personal (ex.: informarea persoanelor vizate în condiţiile reglementate de art. 12 din Legea nr. 677/2001 şi adoptarea unor măsuri adecvate pentru asigurarea securităţii prelucrării datelor conform prevederilor art. 20 alin. 1 din acelaşi act normativ şi cerinţelor minime aprobate prin Ordinul nr. 52/2002).

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

- clarificarea condiţiilor în care se realizează prelucrarea datelor minorilor în activităţi specifice scopului "reclamă, marketing şi publicitate";
- verificarea condiţiilor de prelucrare a datelor privind săvârşirea de infracţiuni, condamnări penale/măsuri de siguranţă sau sancţiuni administrative ori contravenţionale în scopul managementului riscului privind reputaţia clienţilor operatorului; prevenirea, respectiv corectarea riscului actual sau viitor de afectare negativă (prin fraudă) a valorii activelor şi a reputaţiei clienţilor operatorului, determinat de percepţia nefavorabilă a contrapartidelor, acţionarilor, investitorilor sau autorităţilor de supraveghere asupra imaginii acestuia;
- controlul condiţiilor de prelucrare a datelor care denotă originea rasială, etnică, convingerile politice, filozofice, apartenenţa sindicală, apartenenţa la un partid politic, datele privind starea de sănătate, datele genetice, datele biometrice, datele

privind viaţa sexuală, datele privind săvârşirea de infracţiuni în scop de organizare casting;

- verificarea condiţiilor de prelucrare a codului numeric personal în activități de marketing;
- verificarea modalității de prelucrare a datelor biometrice (amprente digitale) în scop de resurse umane, respectiv evidenţa pontajului angaţilor;
- clarificarea condiţiilor în care se realizează prelucrarea datelor prin intermediul unui sistem de supraveghere video capabil să realizeze recunoaşterea facială;
- verificarea condiţiilor de prelucrare a datelor cu caracter personal ale persoanelor vizate prin mijloace de supraveghere video, precum şi a echipamentelor de înregistrare a convorbirilor telefonice;
- controlul condițiilor de prelucrare a datelor biometrice şi a datelor privind starea de sănătate ale angajaţilor în scop de cercetare ştiinţifică;
- verificarea condiţiilor în care se prelucrează datele biometrice – recunoaştere facială – ale vizitatorilor.

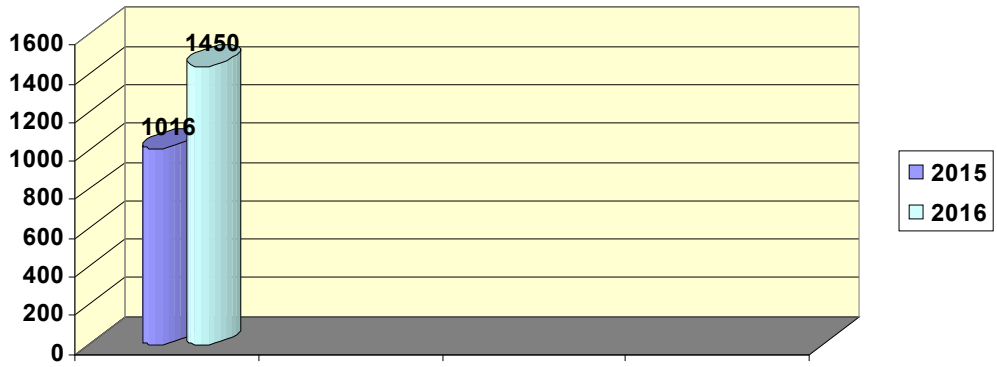
Secţiunea a 2-a – Transferul datelor cu caracter personal în străinătate

Referitor la transferul datelor cu caracter personal în străinătate, menţionăm 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 şi către state cărora Comisia Europeană le-a recunoscut, prin decizie, un nivel de protecţie adecvat.

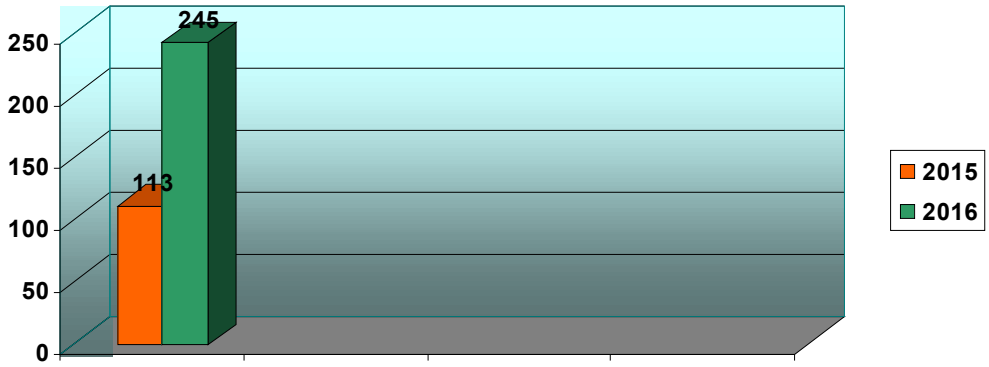
În anul 2016, numărul notificărilor cu transferuri de date către entităţi din străinătate a crescut în mod considerabil față de anii precedenți. Creșterea numărului de notificări cu transferul datelor în străinătate demonstrează faptul că operatorii cunosc mult mai bine obligațiile care le revin în conformitate cu prevederile Legii nr. 677/2001.

Din cele 1450 notificări cu transferuri de date către entităţi din străinătate, în 1205 au fost declarate transferuri către state din Uniunea Europeană, Zona Economică Europeană și din state terţe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield), precum şi

transferuri către state terţe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată şi completată.



Totodată, au fost notificate 245 de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, pe baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules). Comparativ cu anul anterior, constatăm faptul că s-a dublat numărul de transferuri de date cu caracter personal efectuate în baza garanțiilor menționate mai sus.

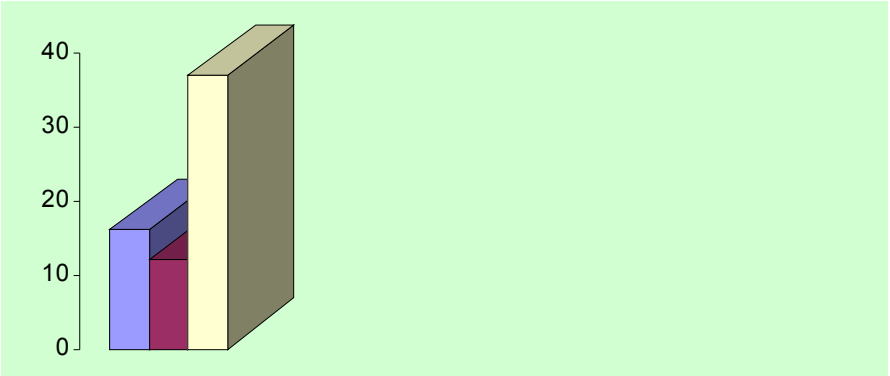


Dintre domeniile care au vizat transferurile de date către state terţe, efectuate în baza prevederilor art. 29 alin. 4 din Legea nr. 677/2001, modificată şi completată, menționăm următoarele:

- gestiune economico-financiară şi administrativă;
- managementul studiilor clinice şi non clinice – procesarea datelor personale ale profesioniştilor din domeniul sănătăţii, consultanţi, colaboratori, liber profesionişti implicaţi în studiile clinice;

- resurse umane şi gestionarea datelor în legătură cu recrutarea, evaluarea şi promovarea personalului;
- soluţionarea sesizărilor de tip compliance formulate de orice persoană interesată cu privire la fapte de încălcare a legii, infracţiuni de corupţie, infracţiuni de serviciu, abateri disciplinare, contravenţii; asigurarea conformităţii respectării legilor în vigoare, a principiilor, a regulamentelor interne; uniformizarea principiilor şi regulamentelor în vederea desfăşurării activităţii potrivit legii la nivelul grupului;
- reclamă, marketing şi publicitate şi asigurare suport IT, externalizat în caz de incidente, suport pentru probleme şi suport IT pentru asigurarea sistemelor IT;
- utilizarea tichetelor electronice, respectiv furnizarea de software specializat pentru a acorda suport cu privire la emiterea cardului şi acceptarea, autorizarea, decontarea şi prelucrarea tranzacţiilor;
- administrarea programelor privind beneficiile şi stimulentele pentru angajaţi;
- sponsorizări, donații și împrumuturi; contribuții la costuri legate de evenimente, inclusiv taxe de înregistrare, cheltuieli de deplasare și cazare;

În urma analizării transferurilor de date în străinătate către state terţe, a fost emis un număr de 37 de autorizaţii de transfer.



Secţiunea a 3-a – Puncte de vedere privind diverse chestiuni de protecţia datelor

În cursul anului 2016, operatorii şi persoanele vizate au solicitat Autorității naționale de supraveghere diverse puncte de vedere cu privire la condiţiile legale de prelucrare a datelor cu caracter personal şi la obligaţia declarării prelucrărilor efectuate, raportat la prevederile Deciziei

nr. 200/2015. Prezentăm mai jos câteva cazuri semnificative supuse analizei Autorităţii naționale de supraveghere:

1) Un reprezentant al unei persoane juridice a solicitat Autorității naționale de supraveghere să i se comunice procedurile necesare notificării pentru implementarea unui sistem de pontaj electronic bazat pe măsurători/scanări ale amprentelor digitale ale angajaților.

În contextul acestei solicitări, s–a comunicat operatorului respectiv faptul că amprentele (datele biometrice) reprezintă date cu caracter personal, întrucât ele privesc caracteristicile fizice/fiziologice ale persoanelor şi pot conduce la identificarea acestora, iar prelucrarea lor intră sub incidența dispoziţiilor Legii nr. 677/2001, modificată și completată.

De asemenea, s-a pus în vedere operatorului faptul că, potrivit art. 4 alin. (1) din legea sus-menționată, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, colectate în scopuri determinate, explicite şi legitime, să fie adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate.

Autoritatea națională de supraveghere a apreciat că angajatorul trebuie să identifice soluţii alternative care să aibă un impact mai redus asupra vieţii private a salariaţilor, considerând prelucrarea datelor biometrice în scop de pontaj excesivă, raportat la scopul urmărit, în contextul necesităţii asigurării unei protecţii eficiente a dreptului la viaţă intimă, familială şi privată .

2) O persoană juridică a solicitat punctul de vedere al Autorităţii naționale de supraveghere cu privire la necesitatea de a notifica prelucrarea datelor în contextul implementării, în cadrul companiilor deţinute de către aceasta, a unui portal prin intermediul căruia să poată fi notificate comportamentele eronate identificate în derularea activităţii angajaților societăţii (precum comportament anticoncurenţial, siguranţa la locul de muncă, siguranţa informaţiilor privitoare la tehnicile de lucru şi know-how-ul societăţii), ca modalitate de raportare subsidiară a neregulilor.

Portalul va permite salariaţilor, partenerilor de afaceri ai societăţii şi părţilor interesate din întreaga lume să notifice abateri grave privind conduita în activitate, încălcări ale dispoziţiilor legale şi ale liniilor directoare interne.

Autoritatea naţională de supraveghere a precizat că prelucrarea pusă în discuţie se încadrează în situaţia reglementată de art. 1 alin. (1) lit. e) din Decizia nr. 200/2015.

Prin urmare, s-a comunicat faptul că, pentru a obţine înregistrarea în Registrul electronic de evidenţă a prelucrărilor de date cu caracter personal, este necesar să se completeze on-line formularul de notificare generală, prevăzut în anexa Deciziei preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 95/2008 privind stabilirea formularului tipizat al notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicată în Monitorul Oficial al României nr. 876 din 24 decembrie 2008.

3) O persoană juridică a solicitat opinia Autorităţii naționale de supraveghere în ceea ce priveşte necesitatea notificării transferului de date către state din Uniunea Europeană, Zona Economică Europeană, precum şi către state cărora Comisia Europeană le-a recunoscut, prin decizie, un nivel de protecţie adecvat.

Astfel, s-a precizat că, potrivit art. 2 alin. (1) din Decizia nr. 200/2015 emisă de preşedintele Autorităţii naționale de supraveghere, „va face obiectul notificării Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal transferul datelor cu caracter personal către statele situate în afara Uniunii Europene, a Zonei Economice Europene, precum şi către statele cărora Comisia Europeană le-a recunoscut, prin decizie, un nivel de protecţie adecvat, inclusiv în cazurile prevăzute la art. 1”.

Prin urmare, s-a comunicat că nu este necesară notificarea transferului de date cu caracter personal către state din Uniunea Europeană, Zona Economică Europeană, precum şi către state cărora Comisia Europeană le-a recunoscut, prin decizie, un nivel de protecţie adecvat.

4) O instituţie publică a solicitat opinia Autorităţii naționale de supraveghere cu privire la necesitatea notificării prelucrărilor de date efectuate în activitatea de eliberare a unor titluri de proprietate, precum şi la condiţiile în care se pot dezvălui datele către autorităţi publice.

Legat de subiectul pus în discuţie, Autoritatea naţională de supraveghere a precizat că, având în vedere faptul că prelucrările la care se face referire se efectuează în baza unor dispoziţii legale, sunt incidente prevederile art. 1 alin. (2) din decizia mai sus menţionată potrivit cărora „notificarea nu este necesară atunci când prelucrarea este prevăzută de lege". În acest context, în situaţia în care nu se prelucrează date de natura celor arătate în dispoziţiile art. 1 ori dacă prelucrarea este prevăzută de lege, nu mai este necesară completarea formularului de notificare.

În ceea ce priveşte dezvăluirea datelor, s-a menţionat că regula instituită de Legea nr. 677/2001, modificată şi completată, este aceea că prelucrarea, inclusiv dezvăluirea datelor cu caracter personal ale persoanei vizate poate fi efectuată de către un operator numai cu consimţământul persoanei în cauză, dat în mod expres şi neechivoc. De asemenea, art. 5 alin. (2) din legea menţionată anterior stabileşte în mod expres şi anumite situaţii de excepţie de la obligativitatea obţinerii consimţământului în cazul prelucrării datelor personale şi, implicit, al dezvăluirii lor prin transmitere, diseminare sau în orice alt mod.

5) Un operator a solicitat punctul de vedere al Autorităţii naționale de supraveghere referitor la necesitatea declarării prelucrării efectuate prin intermediul unei aplicații care permite utilizarea, în procesul de recrutare a personalului, a unui canal video dedicat interviurilor de angajare.

Autoritatea naţională de supraveghere a apreciat că prelucrarea pusă în discuţie se încadrează în situaţia reglementată de art. 1 alin. (1) lit. e) din Decizia nr. 200/2015, fiind necesară declararea prelucrării efectuate prin intermediul aplicației respective.

6) O persoană juridică a solicitat opinia Autorităţii naționale de supraveghere referitoare la condițiile legale care trebuie respectate în cazul supravegherii video a angajaților.

Sub acest aspect, s-a precizat faptul că implementarea unui sistem de videosupraveghere a salariaților poate afecta drepturile acestora, astfel că, în plus faţă de dispoziţiile Legii nr. 677/2001, modificată şi completată, şi ale art. 8 din Decizia nr. 52/2012, trebuie respectate şi 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 reprezentanţilor salariaţilor.

Decizia nr. 52/2012 stabileşte prin art. 8 situaţiile în care prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video este permisă, şi anume: pentru îndeplinirea unor obligaţii legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

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

Totodată, s-a comunicat că, în măsura în care se intenționează extinderea supravegherii video în interiorul birourilor unde salariații își desfăşoară activitatea la locul de muncă, aceasta este permisă doar în situaţiile prevăzute expres de lege sau pe baza avizului Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (art. 8 alin. (3) din Decizia nr. 52/2012).

Ca atare, regula supravegherii video în interiorul birourilor o constituie interzicerea efectuării acestei prelucrări, excepţiile fiind situaţiile expres prevăzute într-un act normativ care obligă angajatorul la instituirea sistemelor de supraveghere video sau cele autorizate de Autoritatea naţională de supraveghere, potrivit art. 8 alin. (3) din Decizia nr. 52/2012, în situaţii temeinic justificate.

De asemenea, s-a comunicat că societatea respectivă are calitatea de operator, sens în care are obligația depunerii notificării.

7) O persoană fizică a solicitat punctul de vedere al Autorităţii naționale de supraveghere cu privire la prelucrarea de date cu caracter personal efectuată prin mijloace de supraveghere video.

S-a comunicat petentului faptul că prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune atât prevederilor Legii nr. 677/2001 pentru protecţia persoanelor cu privire

la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, modificată şi completată, dispoziţiilor Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, cu modificările și completările ulterioare, cât şi celor ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

Cu toate acestea, în conformitate cu prevederile art. 2 alin. (6) din Legea nr. 677/2001, acest act normativ nu se aplică prelucrărilor de date cu caracter personal efectuate de persoane fizice exclusiv pentru uzul lor personal, dacă datele în cauză nu sunt destinate a fi dezvăluite.

Totodată, potrivit art. 17 alin. (2) din Decizia nr. 52/2012, prevederile acestei decizii nu se aplică prelucrărilor de date cu caracter personal, prin mijloace de supraveghere video, efectuate de persoanele fizice exclusiv pentru uzul lor personal, dacă datele în cauză nu sunt destinate a fi dezvăluite.

Aşadar, o persoană fizică nu are calitatea de operator şi nu are obligaţia de notificare a prelucrării datelor (respectiv imagini înregistrate prin mijloace de supraveghere video) către Autoritatea naţională de supraveghere dacă imaginile sunt utilizate de persoana fizică în cauză doar pentru uzul personal şi dezvăluite autorităţilor cu competenţe speciale de anchetă (de exemplu, autorităţilor ce au atribuţii legale în a cerceta săvârşirea de infracţiuni).

Cu toate acestea, în măsura în care o persoană fizică utilizează un sistem de supraveghere video care captează și imagini din spațiul public, aceasta are calitatea de operator de date cu caracter personal și, în consecință, îi revin toate obligațiile acestuia, așa cum sunt stabilite de Legea nr. 677/2001, cu excepția notificării prelucrării către Autoritatea naţională de supraveghere, așa cum se prevede în art. 5 din Decizia nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea, precum şi pentru modificarea şi abrogarea unor decizii.

8) Autorității naționale de supraveghere i s-a solicitat punctul de vedere cu privire la obligaţiile ce revin operatorilor de date cu caracter personal ce transferă date cu caracter personal în Statele Unite ale Americii, în baza certificării Privacy Shield în privinţa notificării, raportat la prevederile Deciziei nr. 200/2015.

În contextul solicitării formulate, s-a comunicat operatorului faptul că, în situaţia în care importatorul a aderat la principiile Privacy Shield, devin incidente prevederile art. 2 alin. (1) din Decizia nr. 200/2015.

În consecință, operatorilor care transferă date cu caracter personal în Statele Unite ale Americii, în baza certificării Privacy Shield, nu le revine obligaţia de a notifica Autoritatea de supraveghere.

9) O instituţie cu atribuţii în constituirea și organizarea colecţiilor de cărţi și a altor documente de bibliotecă a informat Autoritatea naţională de supraveghere cu privire la faptul că acordă abonamente pentru angajaţii unor societăți comerciale. În acest context, instituția menționată mai sus a primit solicitări de la departamentul de resurse umane al companiilor client cu privire la comportamentul şi obişnuinţele de consum ale abonaţilor, angajați ai societăților respective (ce, cât şi când citeşte un abonat, titlul cărţilor, numărul de împrumuturi şi data împrumuturilor).

Autoritatea naţională de supraveghere a apreciat că furnizarea informaţiilor referitoare la monitorizarea comportamentului cititorului reprezintă o prelucrare de date personale care se circumscrie prevederilor art. 1 alin. 1 lit. e) din Decizia nr. 200/2015, impunându-se declararea ei, în măsura în care se realizează prin mijloace electronice, şi obţinerea consimţământului cititorului pentru dezvăluirea datelor referitoare la comportamentul acestuia.

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂŢII

În vederea desfășurării activității, în anul 2016, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal i s-au alocat fonduri prin Legea bugetului de stat nr. 339/2015 și prin Ordonanțele Guvernului nr. 14 și nr. 86/2016 privind rectificarea bugetului de stat pe anul 2016, rezultând un buget final în sumă de 4.851.000 lei, cu următoarea structură:

- mii lei -

Denumire indicator	Cod	Buget iniţial 2016	Buget actualizat la 31.12.2016	Sume cheltuite până la 31.12.2016	Execuţie (%)
Total cheltuieli	51.01	3.256	4.851	4.767	98
Cheltuieli de personal	10	2.485	3.727	3.721	99
Bunuri şi servicii	20	750	765	688	89
Cheltuieli de capital	71	21	359	358	99

Întrucât pe parcursul exercitiului bugetar au avut loc 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 priveşte modul de repartizare al fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorităţii naţionale 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 3.720.823 lei (prin ocuparea unor posturi, temporar, prin detaşare),

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 plăţilor efectuate pentru munca salariată a angajaţilor.

Cheltuielile aferente titlului Bunuri și servicii în anul 2016 au avut o pondere de 15% în bugetul instituției, iar dintre acestea, cheltuielile cu pondere mai importantă au fost:

- 12,95% cheltuielile aferente deplasărilor interne, ca urmare a numărului crescut de plângeri și, implicit a controalelor efectuate la operatorii de date din teritoriu, precum și deplasărilor externe de la grupurile și subgrupurile de lucru europene, în contextul modificărilor legislative la nivel european
- 14% costuri de închiriere și 24% cheltuieli cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI

Trebuie menţionat faptul că Autoritatea Naţională de Supraveghere îşi realizează obiectul principal de activitate prin investigaţii şi controale la operatorii situaţi pe teritoriul României, precum şi la consulatele României.

La nivelul Uniunii Europene, Autoritatea naţională de supraveghere are obligaţia de a participa la lucrările Grupului de Lucru Articolul 29, ale subgrupurilor de lucru din cadrul acestuia, la reuniunile Grupurilor de coordonare comună (SIS II, VIS, Eurodac), precum şi la lucrările Comitetului Consultativ al Convenției 108.

În anul 2016, cheltuielile cu bunuri și servicii au crescut cu 9 % față de anul 2015, avându-se permanent în vedere mai mulți factori – oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice, alăturat unor cerinţe tehnice atent stabilite.

În ceea ce privește cheltuielile de capital, Autoritatea naţională de supraveghere a demarat în anul 2016 un proiect de reînnoire a infrastructurii IT, pentru început fiind achiziționat un nou sistem de servere și un storage, pentru acestea și pentru licențele necesare funcționării serverelor și calculatoarelor din patrimoniul instituției fiind utilizate 63% din sumele alocate cheltuielilor de investiții.

A fost parțial înnoit parcul auto al instituției prin intemediul programului PSIPAN 2016, în acest scop fiind utilizate 47% din fondurile prevăzute în bugetul final al titlului Cheltuieli de capital.

Trebuie menționat că mijloacele fixe înlocuite au fost achiziționate din primul buget alocat după înființarea instituției, în anul 2006.

Politicile contabile utilizate la întocmirea situaţiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare.

Situaţiile financiare anuale oferă o imagine fidelă a realităţii poziţiei financiare a instituţiei, încadrarea în creditele bugetare alocate pe grupe, titluri, articole şi alineate de cheltuieli, aşa cum sunt prevăzute acestea în bugetul autorităţii.

Cheltuielile bugetare s-au efectuat cu respectarea principiilor privind legalitatea, oportunitatea, continuitatea şi eficienţa.

Toate documentele ce intră sub incidenţa controlului financiar preventiv propriu sunt verificate şi vizate.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, putem preciza că acestea au fost utilizate cu maximă eficienţă şi printr-o atentă administrare de către instituţia noastră.