

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

R A P O R T A N U A L

2017



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

București

CUVÂNT ÎNAINTE

*Stimate Domnule Președinte al Senatului,
Stimați Senatori,*

Specificitatea activității instituției noastre în anul 2017 a constat în pregătirea actelor normative naționale de natură să asigure optima aplicare a Regulamentului (UE) 2016/679 privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor), adoptat pe data de 27 aprilie 2016, de către Parlamentul European și Consiliul.

Efectul adoptării acestei reglementări europene constă în uniformizarea principiilor și regulilor de prelucrare a datelor personale în toate statele membre ale Uniunii Europene, în condițiile în care, începând cu data de 25 mai 2018, Regulamentul General privind Protecția Datelor dobândește aplicabilitate directă.

În acest context, reliefaăm consolidarea adusă drepturilor persoanelor fizice și consacrarea unor noi drepturi, cum sunt dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării. În mod corelativ, este de remarcat importanța deosebită acordată responsabilității operatorilor în legătură cu prelucrările efectuate, care au obligația de a demonstra că respectă Regulamentul General privind Protecția Datelor.

Un aspect de noutate, pe care doreș să-l supun atenției dumneavoastră, constă în instituirea obligației instituțiilor publice și, în anumite situații, a entităților private, de a-și desemna o persoană responsabilă cu protecția datelor, în funcție de anumite criterii stabilite expres prin dispozițiile art. 37 din Regulament. Apreciem că aceasta va avea un impact pozitiv în activitatea operatorilor din România și, implicit, efecte benefice în privința respectării drepturilor persoanelor fizice.

Având în vedere că Regulamentul General privind Protecția Datelor conține unele dispoziții care oferă posibilitatea statelor membre de a interveni cu anumite reglementări naționale, s-au realizat în cursul anului 2017, consultări cu ministerele responsabile pentru analiza și pregătirea cadrului național legislativ adecvat.

Astfel, instituția noastră a pregătit proiectul de lege de modificare și completare a Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date. Acest proiect este necesar pentru asigurarea concordanței competențelor și sarcinilor de monitorizare și control ale instituției noastre cu prevederile art. 55-59 din Regulamentul General privind Protecția Datelor.

De asemenea, a fost supus consultărilor interministeriale și un proiect de act normativ destinat stabilirii măsurilor necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 9 alin. (4), art. 37-39, art. 42-43, art. 83 alin. (7), art. 85, art. 87-89 din Regulamentul General privind Protecția Datelor.

În același timp, instituția noastră s-a implicat și în consultările interministeriale referitoare la pregătirea reglementării naționale de transpunere a Directivei 680/2016/EC privind protecția persoanelor fizice față de prelucrările efectuate de către autoritățile competente în scopul prevenirii, cercetării, constatării sau urmăririi penale a infracțiunilor ori executării pedepselor penale și libera circulație a acestor date.

Totodată, în anul 2017, s-a continuat activitatea intensă de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat, alături de acțiunile numeroase de informare a acestora și a publicului larg cu privire la noile condiții aplicabile domeniului protecției datelor cu caracter personal. S-a remarcat creșterea semnificativă a numărului de plângeri și sesizări față de anul anterior, în principal referitoare la prelucrarea datelor personale de către birourile de credit, din cadrul sistemelor ce utilizează mijloace de supraveghere video și din sectorul comunicațiilor electronice.



În considerarea acestor aspecte, apreciem că, în anul 2018, acțiunile Autorității vor urmări în mod special:

- finalizarea adoptării cadrului normativ național în concordanță cu noile reglementări ale Uniunii Europene, prin implicare alături de instituțiile responsabile;
- asigurarea conștientizării publice cu privire la noile reguli de prelucrare a datelor personale;
- consolidarea capacității administrative interne prin luarea măsurilor necesare destinate aplicării noulor acte normative europene și naționale;
- monitorizarea aplicării Regulamentului General privind Protecția Datelor și a celorlalte reglementări aplicabile în domeniu.

Permiteți-mi să mulțumesc pentru sprijinul pe care l-ați acordat până în prezent instituției noastre și să-mi exprim, în același timp, speranța că vom beneficia de încrederea dumneavoastră pentru asigurarea unei efective respectări a dreptului fundamental la viață privată și la protecția datelor cu caracter personal.



CUPRINS

CAPITOLUL I

PREZENTARE GENERALĂ7

CAPITOLUL II

INIȚIATIVE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secțiunea 1 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE9

Secțiunea 2 Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului10

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Elaborarea proiectelor actelor normative de aplicare a RGDP11

Secțiunea a 2-a Avizarea actelor normative12

Secțiunea a 3-a Puncte de vedere privind diverse chestiuni de protecția datelor.....29

Secțiunea a 4-a Aspecte relevante referitoare la aplicarea Regulamentului (UE)2016/679..36

Secțiunea a 5-a Activitatea de reprezentare în fața instanțelor de judecată.....42

Secțiunea a 6-a Informare publică53

**CAPITOLUL IV
ACTIVITATEA DE CONTROL**

Secțiunea 1	Prezentare generală	63
Secțiunea a 2-a	Investigații din oficiu	64
Secțiunea a 3-a	Activitatea de soluționare a plângerilor și sesizărilor	75
ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE.....107		

CAPITOLUL V**CAPITOLUL VI
ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER
PERSONAL**

Secțiunea 1	Activitatea de înregistrare a prelucrărilor de date	128
Secțiunea a 2-a	Transferul în străinătate al datelor cu caracter personal.....	132
Secțiunea a 3-a	Puncte de vedere privind diverse chestiuni de protecția datelor	134

CAPITOLUL VII**MANAGEMENTUL ECONOMIC AL AUTORITĂȚII.....138****CAPITOLUL I
PREZENTARE GENERALĂ**

Raportul de activitate pe anul 2017 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea națională de supraveghere) este structurat pe șapte capitole, după cum urmează:

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

În cuprinsul **Capitolului al II-lea** sunt prezentate aspecte relevante referitoare la pachetul legislativ de reformă în domeniul protecției 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 și la aceea de consultare referitoare la aplicarea regulilor de protecție a datelor personale, inclusiv de clarificare a unor chestiuni semnalate de diverși operatori. Aceasta s-a concretizat în emiterea avizelor asupra unui număr mare de proiecte de acte normative și a unui număr semnificativ de puncte de vedere.

În contextul intrării în vigoare a Regulamentului General privind Protecția Datelor din 25 mai 2018, atât persoanele fizice cât și operatorii de date și-au exprimat interesul pentru noile reglementări aduse în materia protecției datelor de acest act normativ și au solicitat, în special, informații cu privire la aplicabilitatea Regulamentului.

În secțiunea privind reprezentarea în fața instanțelor de judecată, sunt prezentate cele mai semnificative litigii finalizate, în care a fost parte Autoritatea națională de supraveghere, cu evidențierea soluțiilor pronunțate.

Secțiunea privind informarea publică expune principalele modalități de popularizare a Regulamentului General privind Protecția Datelor, utilizate în cursul anului 2017, în limitele resurselor bugetare alocate.

Capitolul al IV-lea constă într-o prezentare a activității de control, în privința investigațiilor din oficiu și a celor efectuate pe baza plângerilor ori sesizărilor primite.



Această activitate constă în verificarea modului de aplicare a dispozițiilor legale în materie.

Investigațiile efectuate din oficiu au vizat verificarea modului de respectare a prevederilor Legii nr. 677/2001, modificată și completată, precum și a dispozițiilor Legii nr. 506/2004, modificată și completată, în cadrul prelucrării datelor cu caracter personal atât în sistemul public, cât și în cel privat.

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri exponențiale a numărului acestora, în anul 2017 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, cu precădere, cele care vizează prelucrarea datelor personale de către birourile de credit, dar și cele din cadrul sistemelor ce utilizează mijloace de supraveghere video sau din sectorul comunicațiilor electronice.

În cadrul investigațiilor efectuate în anul 2017, au fost aplicate sancțiuni contravenționale constând în avertismente și amenzi în cuantum total de 870.500 lei.

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

Capitolul al VI-lea privind activitatea de supraveghere a prelucrărilor de date cu caracter personal cuprinde principalele concluzii rezultate din analiza formulărilor transmise de operatorii de date, persoane fizice și juridice, care au avut obligația depunerii acestora. Au fost înregistrate un număr total de 6115 notificări privind prelucrări de date realizate atât pe teritoriul României, cât și în statele membre, ori transferuri în state terțe.

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



CAPITOLUL II

NOI ACTE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secțiunea 1 - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor)

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

- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE;
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

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.

În primul rând, subliniem consacrarea expresă a „dreptului de a fi uitat”, iar pe de altă parte stabilirea dreptului la portabilitatea datelor și a dreptului la restricționarea prelucrării, de natură să ofere persoanelor fizice un control efectiv asupra datelor lor personale.

Alt element de noutate din Regulament constă în obligativitatea instituțiilor publice și entităților private de a-și desemna un responsabil cu protecția datelor la nivel intern, în funcție de anumite criterii, ceea ce va conduce la o schimbare semnificativă în activitatea operatorilor din România.

În același timp, s-a realizat o reglementare mai detaliată a obligațiilor operatorilor, un accent deosebit fiind pus pe creșterea gradului de responsabilizare a acestora. Consacrarea expresă a principiilor de prelucrare *privacy by design* și *privacy by default* reprezintă un alt element de noutate al acestei reglementări, implicând asigurarea protecției datelor din momentul inițial al stabilirii mijloacelor de prelucrare.

Subliniem că Regulamentul stabilește și un mecanism nou de cooperare între autoritățile naționale de supraveghere care va implica un organism european cu personalitate juridică – Comitetul European pentru Protecția Datelor (European Data Protection Board - EDPB). Acesta va răspunde de medierea pozițiilor între autoritățile naționale de supraveghere, precum și de elaborarea unor ghiduri și recomandări destinate unei aplicări unitare a acestei noi reglementări în spațiul Uniunii Europene.

Mai mult, se prevede o extindere a competențelor și sarcinilor autorităților naționale de supraveghere și, pe cale de consecință, rezultă necesitatea anumitor modificări legislative naționale prin care să se consolideze capacitatea instituțională și administrativă a Autorității 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.

Secțiunea 2 - Directivei (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

Această reglementare distinctă urmează a fi transpusă în plan național prin lege, astfel încât să se asigure o previzibilitate necesară a normelor raportat la specificitatea prelucrărilor de date cu caracter personal efectuate scopul prevenirii, detectării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor.

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ȘI INFORMARE PUBLICĂ

Secțiunea 1 Elaborarea proiectelor actelor normative de aplicare a RGDP

În considerarea faptului că Regulamentul General privind Protecția Datelor conține unele dispoziții care oferă posibilitatea statelor membre de a interveni cu anumite reglementări naționale, în cursul anului 2017, au avut loc mai multe consultări cu ministerele responsabile pentru analiza și pregătirea cadrului național legislativ adecvat.

Instituția noastră a pregătit proiectul de lege de modificare și completare a Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date. Acest proiect este destinat asigurării concordanței competențelor și sarcinilor de monitorizare și control ale instituției noastre cu prevederile art. 55-59 din Regulamentul General privind Protecția Datelor.

Tot în cursul anului 2017 a fost elaborat și supus consultărilor interministeriale și un proiect de act normativ destinat stabilirii măsurilor necesare punerii în aplicare la nivel național, în principal, a prevederilor art. 9 alin. (4), art. 37-39, art. 42-43, art. 83 alin. (7), art. 85, art. 87-89 din Regulamentul General privind Protecția Datelor.

De asemenea, instituția noastră a luat parte activă și în consultările interministeriale referitoare la pregătirea reglementării naționale de transpunere a Directivei 680/2016/EC privind protecția persoanelor fizice față de prelucrările efectuate de către autoritățile competente în scopul prevenirii, cercetării, constatării sau urmării penale a infracțiunilor ori executării pedepselor penale și libera circulație a acestor date.



Secțiunea 2 Avizarea actelor normative

Autoritatea națională de supraveghere a emis, în temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, avize asupra unui număr de 31 de proiecte de acte normative elaborate de instituții și autorități publice, care implicau aspecte complexe privind prelucrarea datelor cu caracter personal.

În condițiile diversității situațiilor reglementate prin actele normative transmise în vederea avizării, în cele mai multe cazuri 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, inclusiv în contextul aplicării Regulamentului general privind protecția datelor începând cu data de 25 mai 2018.

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

- **Consiliul Național pentru Combaterea Discriminării a transmis spre avizare proiectul de "Hotărâre a Guvernului privind aprobarea Strategiei naționale "Egalitate, incluziune, diversitate" pentru perioada 2016-2020 și a Planului operațional privind implementarea Strategiei naționale "Egalitate, incluziune, diversitate" 2016 - 2020"**

Autoritatea națională de supraveghere a formulat următoarele observații și propuneri, în scopul asigurării respectării cerințelor legislației din domeniul protecției datelor cu caracter personal, cu privire la prelucrarea de date cu caracter personal ale persoanelor considerate discriminate pe anumite criterii (gen, vârstă, sex, etnie, stare de sănătate etc.), cu precădere a unor categorii speciale de date (de ex. referitoare la originea rasială sau etnică, date privind starea de sănătate sau viața sexuală), și, în mod particular, cu privire la confidențialitatea și securitatea datelor.



Cu privire la conținutul Cap. IV – Obiective specifice, raportat la atribuțiile Autorității naționale de supraveghere, de monitorizare și control al prelucrărilor de date cu caracter personal efectuate de diverse entități publice sau private, în calitatea acestora de operatori de date (de ex. Ministerul Educației, Institutul Național de Statistică, unități de învățământ) și la cea potrivit căreia Autoritatea națională de supraveghere poate formula recomandări și avize asupra oricărei chestiuni legate de protecția datelor, s-a apreciat ca fiind necesară modificarea unor prevederi referitoare la elaborarea de către CNCD, în parteneriat cu Ministerul Educației și Institutul Național de Statistică, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, a unor instrumente (...).

Referitor la colectarea de date cu privire la discriminare și egalitate (genul, etnia, religia, dizabilitatea, situația familială etc.) în instituții de învățământ superior, s-a subliniat faptul că datele cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenența sindicală, precum și datele cu caracter personal privind starea de sănătate sau viața sexuală, sunt date cu caracter special, protejate de reguli speciale instituite de Legea nr. 677/2001, iar condițiile de prelucrare ale acestora sunt prevăzute în art. 7 și art. 9 din această lege.

Regula instituită de art. 7 alin. (1) din Legea nr. 677/2001 este aceea că astfel de informații sunt interzise de la prelucrare. Însă, prelucrarea acestor date este permisă în anumite cazuri de excepție, expres prevăzute în alin. (2) al art. 7 din Legea nr. 677/2001.

În consecință, prelucrarea datelor sus menționate, inclusiv colectarea acestora, realizată pe scară largă, poate reprezenta o nouă situație de risc pentru protecția datelor cu caracter personal ale persoanelor fizice și, implicit, pentru respectarea și garantarea drepturilor fundamentale ale acestora, în special cel la viață privată și, ca atare, la prelucrarea acestor date este necesară luarea în considerare a tuturor principiilor de prelucrare a datelor, înlocuite de art. 4 alin. (1) din Legea nr. 677/2001.

În același timp s-a subliniat că, la alegerea modalităților de transmitere a datelor sau a documentelor ce conțin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii au obligația de a aplica măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmitii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere prevederile art. 20 din Legea nr. 677/2001.

În contextul Strategiei naționale "Egalitate, incluziune, diversitate" 2016 - 2020, Autoritatea națională de supraveghere a apreciat că este necesară o evaluare a cadrului juridic și, implicit, a actelor normative referitoare la egalitatea de șanse, incluziune și diversitate, astfel încât acesta să prevadă sau să întărească normele referitoare la protecția drepturilor și libertăților persoanelor în ceea ce privește prelucrările de date cu caracter personal.

Cu acest prilej, 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, totodată, că, potrivit principiului responsabilității din Regulamentul (UE) 2016/679, operatorii de date cu caracter personal (precum cel menționat în Strategie) nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrare a datelor ("egalitate, echitate și transparență", "limitări legate de scop", "reducerea la minimum a datelor", "exactitate", "limitări legate de stocare", precum și "integritate și confidențialitate"), dar este necesar ca aceștia să poată demonstra respectarea principiilor menționate.

Autoritatea națională de supraveghere a **avizat cu observații** proiectul de "Hotărâre a Guvernului privind aprobarea Strategiei naționale "Egalitate, incluziune, diversitate" pentru perioada 2016-2020 și a Planului operațional privind implementarea Strategiei naționale "Egalitate, incluziune, diversitate" 2016 - 2020".

> **Autoritatea Națională de Reglementare în Domeniul Energiei a solicitat punctul de vedere cu privire la proiectul de "Ordin privind implementarea la nivel național a sistemelor de măsurare inteligentă a energiei electrice și stabilirea calendarului de implementare"**

Autoritatea națională de supraveghere a formulat observații și propuneri, astfel:

Din analiza textului proiectului a reieșit faptul că, în cadrul activităților ce urmează a fi desfășurate de către operatorii de distribuție a energiei electrice concessionari și furnizorii de energie electrică, în contextul dezvoltării platformei Metering Data Management System în cadrul *Sistemului de măsurare inteligentă a energiei electrice (SMI)*, ar urma să fie prelucrate și

date cu caracter personal ale consumatorilor persoane fizice, în calitatea acestora de beneficiari ai sistemelor de măsurare inteligentă.

În acest context, s-a atras atenția asupra faptului că în proiect nu sunt specificate datele cu caracter personal ce vor fi prelucrate în SMI, fapt pentru care s-a recomandat introducerea unui alineat nou la articolul 11 din proiect, care să clarifice acest aspect.

Totodată, s-a precizat că pentru prelucrarea datelor cu caracter personal din SMI este necesară luarea în considerare a principiilor de protecție a datelor, instituite de art. 4 alin. (1) din Legea nr. 677/2001, în special prin stabilirea garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate și stabilirea persoanelor autorizate care vor avea acces la date, în scopuri legitime.

Întrucât prelucrările de date cu caracter personal pot fi expuse unor serii de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor, s-a recomandat ca, la alegerea modalităților de transmitere a datelor sau a documentelor ce conțin date cu caracter personal, să se aibă în vedere faptul că operatorii au obligația de a aplica măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special în contextul în care prelucrarea de date în SMI comportă transmitii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Sub aspectul celor de mai sus, s-a atras atenția asupra faptului că a fost emis, de către Grupul de lucru Art. 29, *Avizul nr. 12/2011 privind contorizarea inteligentă*, care precizează că serviciile și tehnologiile care se bazează pe prelucrarea datelor cu caracter personal ar trebui proiectate din start astfel încât să respecte viața privată. În acest sens, punerea în aplicare a contorizării inteligente ar trebui să respecte din start viața privată, nu doar în ceea ce privește măsururile de securitate, ci și prin reducerea la minimum a cantității de date cu caracter personal prelucrate.

Mai mult, s-a subliniat că operatorilor de distribuție a energiei electrice concessionari și furnizorilor de energie electrică, în calitate de operatori de date cu caracter personal, le 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 prelucreză, prevăzute de art. 13 - 18, precum și obligațiile de asigurare a confidențialității și securității prelucrării datelor, așa cum sunt prevăzute de Legea nr. 677/2001.



În sensul celor de mai sus, cu privire la informarea și drepturile persoanelor vizate, s-a recomandat introducerea unui alineat nou la art. 11 din proiect.

Având în vedere aspectele de mai sus, **Autoritatea națională de supraveghere a apreciat că proiectul de ordin necesită reanalizare.**

- **Ministerul Muncii și Justiției Sociale a transmis în vederea formulării unui punct de vedere proiectul de "Hotărâre pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 76/2002 privind sistemul asigurărilor pentru șomaj și stimularea ocupării forței de muncă, aprobate prin Hotărârea Guvernului nr. 174/2002, și pentru modificarea și completarea Procedurilor privind accesul la măsurile pentru stimularea ocupării forței de muncă, modalitățile de finanțare și instrucțiunile de implementare a acestora, aprobate prin Hotărârea Guvernului nr. 377/2002"**

Autoritatea națională de supraveghere a formulat observații și propuneri:

În contextul reglementării sistemului asigurărilor pentru șomaj și stimulării ocupării forței de muncă, entități precum Agenția Națională pentru Ocuparea Forței de Muncă și agențiile pentru ocuparea forței de muncă județene sau, după caz, a municipiului București, desfășoară activități ce presupun efectuarea de operațiuni de prelucrare de date.

Raportat la conținutul proiectului de act normativ supus analizei, Autoritatea națională de supraveghere a subliniat necesitatea stabilirii de garanții adecvate pentru respectarea drepturilor persoanelor vizate în ceea ce privește prelucrarea de date cu caracter personal, așa cum se regădesc acestea în art. 12 – 18 din Legea nr. 677/2001 (dreptul la informare, dreptul de acces la date, dreptul de intervenție asupra datelor, dreptul de opoziție, dreptul de a nu fi supus unei decizii individuale, dreptul de a se adresa justiției).

Cât privește comunicarea de informații și date între diversele entități la care face referire *proiectul de Hotărâre* (de ex. art. 1 pct. 6 privind introducerea art. 46³ alin. (5) ce reglementează faptul că informațiile privind veniturile nete realizate "se pun la dispoziția Agenției Naționale pentru Ocuparea Forței de Muncă, de către Casa Națională de Pensii Publice, Agenția Națională pentru Plăți și Inspecție Socială și Agenția Națională de Administrare Fiscală"



ori art. 1 pct. 6 privind introducerea art. 46⁴ alin. (5)), s-a subliniat că o comunicare de acest tip se poate expune la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală a datelor.

S-a mai precizat că la aceleași riscuri ca cele anterior menționate se expune și comunicarea prin poștă, fax ori e-mail (de ex. art. 1 pct. 6 privind introducerea art. 46⁴ alin. (2) din proiect), a documentelor conținând date cu caracter personal între solicitanții primei de instalare sau de relocare și agențiile pentru ocuparea forței de muncă județene sau, după caz, a municipiului București.

În legătură cu transmiterea datelor sau a documentelor (de ex. copii certificate ale actelor de identitate, adeverințe, declarații, formulare etc.) ce conțin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii de date cu caracter personal au obligația de a aplica măsuri tehnice și 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 transmitii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispozițiile art. 17 alin. (1) din Directiva 95/46/CE a Parlamentului European și prevederile art. 20 din Legea nr. 677/2001.

În consecință, s-a recomandat ca, în cuprinsul proiectului de Hotărâre, să se includă un articol distinct, eventual în care să facă referire la faptul că prelucrarea datelor cu caracter personal se va realiza în conformitate cu reglementările legale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Autoritatea națională de supraveghere a apreciat că **proiectul de Hotărâre necesită reanalizare**, sub aspectul observațiilor și propunerilor menționate anterior.

Ulterior, Ministerul Muncii și Justiției Sociale a retransmis Autorității naționale de supraveghere *proiectul de Hotărâre pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 76/2002 privind sistemul asigurărilor pentru șomaj și stimularea ocupării forței de muncă, aprobate prin Hotărârea Guvernului nr. 174/2002, și pentru modificarea și completarea Procedurilor privind accesul la măsurile pentru stimularea ocupării forței de muncă, modalitățile de finanțare și instrucțiunile de implementare a acestora, aprobate prin Hotărârea Guvernului nr. 377/2002*, în vederea avizării.

Întrucât textul proiectului a fost modificat, Autoritatea națională de supraveghere a avizat favorabil proiectul.

➤ **Ministerul Afacerilor Interne a solicitat propuneri și observații cu privire la proiectul de "Lege pentru modificarea și completarea unor acte normative în domeniul ordinii și siguranței publice"**

Autoritatea națională de supraveghere a prezentat următoarele observații:

În ceea ce privește art. II punctul 7 din proiect, referitor la noile prevederi legale introduse la art. 31 alin. (1) lit. q) s-a subliniat că, în contextul utilizării sintagmei "*organe ale administrației de stat*", este necesară reanalizarea textului, în sensul clarificării sintagmei prin restrângerea sferei și stabilirea clară a autorităților ale căror baze electronice de date ar putea fi accesate de poliștii învestit cu exercițiul autorității publice, în realizarea atribuțiilor ce îi revin, potrivit legii, cu respectarea principiului proporționalității, prevăzut de art. 4 din Legea nr. 677/2001 și art. 5 din Legea nr. 238/2009, republicată.

S-a atras atenția asupra necesității reformulării textului anterior menționat în contextul în care dispozițiile Constituției României delimitează clar structura administrației publice din România, în administrație publică centrală de specialitate și administrație publică locală.

În contextul celor de mai sus, a fost evidențiat considerentul (30) din Decizia nr. 440/2014 referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice și ale art. 152 din Codul de procedură penală, care prezintă: "*S-a mai reținut că protecția datelor cu caracter personal, care rezultă din obligația explicită prevăzută la art. 8 alin. (1) din Cartă, prezintă o importanță deosebită pentru dreptul la respectarea vieții private, consacrat la art. 7 din aceeași Cartă (par. 51), motiv pentru care directiva în cauză ar trebui să cuprindă norme clare și precise cu privire la conținutul și aplicarea măsurii reținerii datelor și să prevadă o serie de limitări, așa încât persoanele ale căror date au fost păstrate să beneficieze de garanții suficiente care să asigure o protecție eficientă împotriva abuzurilor și a oricărui acces sau utilizări ilicite (par. 54)."*

De asemenea, cu privire la accesarea sistemelor de supraveghere a spațiului public, Autoritatea națională de supraveghere a solicitat reanalizarea necesității acestor prevederi, raportat la respectarea principiului proporționalității prelucrării datelor și implicațiile accesului nediscriminatoriu și în integralitate la aceste sisteme de evidență.

În sensul celor anterioare, a fost supus atenției inițiatorului considerentul (57) din Decizia nr. 440/2014 care prezintă: "*(...) Legea nu prevede criterii obiective care să limiteze la strictul necesar numărul de persoane care au acces și pot utiliza ulterior datele păstrate, că accesul autorităților naționale la datele stocate nu este condiționat, în toate cazurile, de controlul prealabil efectuat de către o instanță sau de o entitate administrativă independentă, care să limiteze acces și utilizarea lor la ceea ce este strict necesar pentru realizarea obiectivului urmărit. Garanțiile legale privind utilizarea în concret a datelor reținute nu sunt suficiente și adecvate pentru a îndepărta teama că drepturile personale, de natură intimă, sunt violate, așa încât manifestarea acestora să aibă loc într-o manieră acceptabilă."*

Cu privire la reglementarea accesului poliștilor la bazele electronice de date ale "organelor administrației de stat și la sistemele de supraveghere", în baza "unor documente de cooperare încheiate între deținătorii acestora și unitățile competente ale Poliției Române, care vor cuprinde cel puțin măsurile specifice de protecție a datelor cu caracter personal", s-a recomandat reanalizarea acestei prevederi în considerarea hotărârii date de Curtea de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții (C-201/14).

Prin hotărârea pronunțată, instanța Uniunii Europene a constatat că informațiile transmise între autorități publice, precum și modalitățile de efectuare a transmiterii acestora, au fost stabilite nu prin intermediul unei măsuri legislative, ci prin intermediul unui protocol, care nu a făcut obiectul unei publicări oficiale.

În ceea ce privește art. III punctul 3 din proiect, referitor la prevederile art. 27² alin. (3), s-a subliniat necesitatea precizării bazelor electronice de date în care poliștii de frontieră are acces în vederea verificării identității unei persoane și căreia/căror entități aparțin aceste baze.

Autoritatea națională de supraveghere a recomandat **reanalizarea conținutului proiectului de Lege pentru modificarea și completarea unor acte normative în domeniul ordinii și siguranței publice** și prin raportare la prevederile aplicabile domeniului penal ale Directivei (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera



circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului Uniunii Europene.

➤ **Ministerul Muncii și Justiției Sociale a transmis, în vederea avizării, proiectul de "Hotărâre privind aprobarea Regulamentului de organizare și funcționare a Inspecției Muncii"**

Față de conținutul acestui proiect, Autoritatea națională de supraveghere a prezentat următoarele observații:

Referitor la prevederile generale ale art. 12 alin. (1) punctul B, litera i) din Capitolul III, privind efectuarea schimbului de date extrase din registrul general de evidență a salariaților, "pe baza protocoalelor încheiate la nivel național cu alte instituții ale statului", s-a recomandat reanalizarea acestuia, în considerarea hotărârii date de Curtea de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții (C-201/14), precum și pentru asigurarea exigențelor de previzibilitate a actelor normative.

Astfel, prin hotărârea pronunțată, CJUE a constatat că informațiile transmise între autorități publice, precum și modalitățile de efectuare a transmiterii acestora au fost stabilite nu prin intermediul unei măsuri legislative, ci prin intermediul unui protocol, care nu a făcut obiectul unei publicări oficiale.

Curtea de Justiție a Uniunii Europene, prin aceeași hotărâre, 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 transmiterea de date personale unei alte autorități a administrației publice și prelucrarea ulterioară a datelor, 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.

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 persoanelor vizate, respectiv în baza consimțământului expres și liber exprimat al acestora sau în baza unor excepții.

S-a recomandat introducerea unui nou articol, distinct, în cuprinsul Regulamentului, referitor la faptul că prelucrarea tuturor datelor cu caracter personal se va realiza de către Inspecția Muncii în conformitate cu prevederile aplicabile în domeniul protecției datelor.

Corelat cu acest aspect, s-a menționat că nu este suficientă prevederea introdusă la Capitolul III, art. 12 alin. (1) punctul B, litera h) din proiect întrucât, raportat la atribuțiile Inspecției Muncii, aceasta efectuează și alte prelucrări de date cu caracter personal, nu doar cele referitoare la gestionarea bazei de date organizate la nivel național ce conține registrele generale de evidență a salariaților.

Astfel, în contextul celor anterioare, cu titlu de exemplu, s-a menționat că, potrivit lit. e) din același art. 12 alin. (1) pct. B din proiect, Inspecția Muncii "realizează fotografii și înregistrări audio-video" care pot conține și date cu caracter personal (imagine și voce) ale angajaților sau reprezentanților legali ai entităților controlate.

Autoritatea națională de supraveghere a avizat cu observațiile sus menționate proiectul de Hotărâre privind aprobarea Regulamentului de organizare și funcționare a Inspecției Muncii.

Ulterior, **Ministerul Muncii și Justiției Sociale a retransmis proiectul de act normativ modificat conform recomandărilor Autorității naționale de supraveghere, acesta fiind avizat favorabil.**

➤ **Ministerul pentru Relația cu Parlamentul a solicitat punctul de vedere cu privire la propunerea legislativă privind "Codul Administrativ al României" (BP. 649/2017)**

Față de textul propunerii legislative, Autoritatea națională de supraveghere a formulat următoarele observații:

În argumentele cuprinse la punctul E din Expunerea de motive a propunerii legislative nu se regăsește o mențiune cu privire la calitatea de operator a Agenției Naționale a Funcționarilor Publici, în privința Sistemului electronic național de evidență a ocupării în sectorul public, în



concordanță cu atribuțiile acestei instituții, ținând cont de definiția dată de art. 3 lit. e) din Legea nr. 677/2001.

Față de modul de redactare a dispozițiilor art. 421 alin. (2) din acest proiect, s-a apreciat ca fiind necesară reformularea acestuia, în sensul utilizării sintagmei "datele necesare colectate", prin raportare la principiul proporționalității datelor instituit de art. 4 alin. (1) din Legea nr. 677/2001.

Totodată, față de forma actuală a dispozițiilor art. 421 alin. (2) și (5) din propunerea legislativă transmisă, s-a solicitat reanalizarea prevederilor referitoare la încheierea unui protocol de colaborare între Agenția Națională a Funcționarilor Publici și Inspectoratul Muncii, având în vedere că din textul proiectului nu reiese că protocolul ar urma să fie publicat în Monitorul Oficial al României sau că ar urma să fie adus la cunoștința publicului larg, astfel încât să fie respectate exigențele Curții de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții.

Prin urmare, raportat la exigențele informării persoanelor vizate cu privire la schimbul de informații, ținând cont de cele stabilite prin Hotărârea Curții de Justiție a Uniunii Europene sus menționată, propunem ca modalitatea de colaborare să se stabilească prin ordin comun al celor două entități.

Autoritatea națională de supraveghere a recomandat ca textul propunerii legislative să se completeze în concordanță cu observațiile și propunerile formulate.

- **Ministerul Muncii și Justiției Sociale a solicitat un punct de vedere cu privire la proiectul de "Hotărâre pentru aprobarea normelor metodologice privind dețasarea salariaților în cadrul prestării de servicii transnaționale pe teritoriul României"**

Față de proiectul Hotărârii de Guvern transmis, s-au formulat următoarele observații și propuneri:

În contextul reglementării cooperării administrative și a schimbului de informații cu privire la dețasarea transnațională a salariaților pe teritoriul României (inclusiv date cu caracter personal ale salariaților), instituțiile naționale desemnate ca autorități competente (Inspectoratul Muncii, inspectoratele teritoriale de muncă, Casa Națională de Pensii Publice) în calitate de operatori, desfășoară activități ce presupun efectuarea de operațiuni de prelucrare de date, ce pot avea implicații directe asupra drepturilor fundamentale ale persoanelor fizice și pot conduce

22



la grave atingeri aduse dreptului la viață privată al cetățenilor, în ceea ce privește protecția datelor lor cu caracter personal.

Autoritatea națională de supraveghere recomandă introducerea unui nou articol, distinct, în cuprinsul proiectului de Hotărâre, referitor la faptul că prelucrarea datelor cu caracter personal de către instituțiile naționale desemnate ca autorități competente se va realiza în conformitate cu reglementările legale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

S-a subliniat că, în legătură cu transmiterea datelor sau a documentelor (de ex. declarații privind dețasarea salariaților) ce conțin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii de date cu caracter personal au obligația de a aplica măsuri tehnice și 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 transmitii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispozițiile art. 17 alin. (1) din Directiva 95/46/CE a Parlamentului European și a Consiliului și prevederile art. 20 din Legea nr. 677/2001.

De asemenea, s-a propus introducerea în textul proiectului de Hotărâre a unui articol distinct referitor la respectarea drepturilor persoanelor vizate în ceea ce privește prelucrarea de date cu caracter personal (dreptul de informare, de acces, intervenție, de opoziție, de a nu fi supus unei decizii individuale) prevăzute de art. 12 – 18 din Legea nr. 677/2001.

Prin urmare, Autoritatea națională de supraveghere propus reformularea proiectului.

- **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul proiectului de "Lege privind cooperarea autorităților publice române cu Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL)"**

Autoritatea națională de supraveghere a formulat următoarele observații:

S-a propus înlocuirea referinței la Legea nr. 677/2001 cu sintagma „se exercită potrivit reglementărilor aplicabile în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date”, prin raportare la Regulamentul General privind Protecția Datelor aplicabil din 25 mai 2018 și la Directiva (UE) 2016/680.

23



La art. 28 alin. (2) din proiect, s-a recomandat modificarea acestuia, în sensul înlocuirii referinței la art. 38 alin. (8) sau (9) cu art. 37 alin. (8) sau (9) din Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului, secțiunea „Dreptul la rectificare, ștergere și restricționare”.

În contextul menționat, s-a recomandat desemnarea unui responsabil cu protecția datelor în cadrul Uniunii Naționale Europol din cadrul Inspectoratului General al Poliției Române – Centrul de cooperare polițienească internațională, precum și în cadrul celorlalte autorități din domeniu, raportat la dispozițiile Directivei (UE) 2016/680.

Ulterior, Ministerul Afacerilor Interne a transmis spre avizare proiectul modificat al actului normativ.

Autoritatea națională de supraveghere a **avizat favorabil proiectul de „Lege privind cooperarea autorităților publice române cu Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (EUROPOL)”**.

➤ **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul proiectului de Lege pentru modificarea și completarea unor acte normative care cuprind dispoziții privind evidența persoanelor și actele de identitate ale cetățenilor români**

Autoritatea națională de supraveghere a formulat următoarele observații:

În ceea ce privește modificările propuse textului O.U.G. nr. 97/2005, referitoare la propunerea de completare a art. 9 alin. (4) lit. c), s-a apreciat că argumentele prezentate în Expunerea de motive nu includ și menționarea unor garanții privind modalitatea de respectare a drepturilor persoanelor vizate (în special cel de intervenție).

Referitor la propunerea vizată de art. 12¹, respectiv la posibilitatea eliberării opționale a cărții de identitate electronice sub vârsta de 14 ani, întrucât aceasta poate să conțină și datele biometrice ale titularilor (imaginea facială și, de la 12 ani, impresiunile papilare), Autoritatea națională de supraveghere și-a menținut aprecierea potrivit căreia aceste prevederi sunt de natură să afecteze dreptul la viață privată al minorilor lipsiți de capacitate de exercițiu, raportat la colectarea și stocarea datelor biometrice ale acestora.

În acest context, raportat la toate argumentele prezentate în corespondența anterioară, Autoritatea națională de supraveghere și-a menținut rezervele cu privire la propunerea de



emitere a cărții electronice de identitate care conține datele biometrice, pentru minorii aflați sub vârsta de 14 ani.

Totodată, instituția noastră și-a menținut rezervele și în ceea ce privește argumentele referitoare la necesitatea colectării și prelucrării datelor biometrice ale minorilor cu vârsta între 0 și 14 ani și de emitere chiar și a unei cărți de identitate simple pentru minorii între 0 și 14 ani, în lipsa unui act normativ al Uniunii Europene care să oblige la luarea unei astfel de măsuri, a respectării principiului proporționalității și a dispozițiilor constituționale ale art. 49 (Protecția copiilor și a tinerilor) coroborat cu art. 26 (Dreptul la viață intimă, familială și privată).

De asemenea, referitor la propunerea de la art. 12¹, sub aspectul sintagmei “la solicitarea unuia dintre părinți”, Autoritatea națională de supraveghere și-a menținut observația potrivit căreia propunerea se impune a fi reanalizată și prin raportare la dispozițiile Legii nr. 272/2004 privind protecția și promovarea drepturilor copilului, republicată, care stabilește obligația ambilor părinți de a-și exercita drepturile și de a-și îndeplini obligațiile față de copil ținând seama cu prioritate de interesul superior al acestuia.

La art. 13 alin (3) din proiect, s-a apreciat că sintagma “sisteme informatice ale altor instituții publice sau private” se impune a fi completată cu mențiuni adecvate, în vederea unei identificări mai clare a acestora. În acest sens, este necesar a se avea în vedere și coroborarea dispozițiilor art. 13 alin (3) cu cele ale art. 17¹ alin. (1¹) din proiect.

În ceea ce privește modificările propuse la art. 338 alin. (4) și (5) din Legea nr. 95/2006, instituția noastră și-a menținut aprecierile privind faptul că se impun a fi efectuate precizări privind modalitatea de stabilire a autentificării și în sistemul informatic al asigurărilor sociale de sănătate, în vederea instituirii unor garanții privind asigurarea dreptului la viață privată și protecția datelor cu caracter personal, cu atât mai mult cu cât autentificarea se efectuează pentru accesul la un sistem de evidență privind starea de sănătate a titularului cărții de identitate, respectiv date cu caracter sensibil ale acestuia.

Totodată, Autoritatea națională de supraveghere și-a menținut și recomandarea referitoare la propunerea de la alin. (5) al art. 338 privind necesitatea stabilirii unor dispoziții tranzitorii care să reglementeze trecerea de la cardul de sănătate la cartea electronică de identitate, cu atât mai mult cu cât aceasta din urmă se eliberează în mod eșalonat.

Autoritatea națională de supraveghere a **avizat cu observații** proiectul de act normativ supus avizării.

➤ **Ministerul Afacerilor Interne a solicitat propuneri și observații în ceea ce privește textul proiectului de *„Lege privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale***

Autoritatea națională de supraveghere a menținut următoarele observații și propuneri, în contextul în care acestea fuseseră comunicate anterior.

S-au menținut aprecierile, în acord cu opinia Grupului de Lucru Articolul 29, exprimate pe parcursul întregii corespondențe anterioare cu privire la această inițiativă legislativă, raportat la colectarea și prelucrarea datelor cu caracter personal pe scară largă și la necesitatea, legitimitatea și proporționalitatea acestui sistem de evidență.

Așa cum se mai precizase, măsura transmiterii de date poate reprezenta o nouă situație de risc pentru respectarea și garantarea drepturilor fundamentale ale persoanelor fizice, precum și a principiilor statuate în Carta drepturilor fundamentale ale UE, în special în art. 7 privind dreptul la viață privată și familială și art. 8 privind protecția datelor personale, precum și în art. 8 din Convenția pentru apărarea drepturilor și libertăților fundamentale.

Raportat la dispozițiile Directivei (UE) 2016/681, Autoritatea națională de supraveghere și-a exprimat opinia în sensul că scopul proiectului de lege referitor la *„prevenirea și înlăturarea amenințărilor la adresa securității naționale”* nu se regăsește în sfera de reglementare a acestei Directive.

Potrivit art. 1 alin. (2) din Directiva (UE) 2016/681, *„datele PNR pot fi colectate doar în scopul prevenirii, investigării și urmării penale a infracțiunilor de terorism și a infracțiunilor grave, astfel cum este prevăzut la art. 6 alin. 2 lit. a), b) și c)”. În aceste dispoziții nu se regăsește sintagma „înlăturarea amenințărilor la adresa securității naționale”, ele referindu-se la prelucrarea datelor PNR exclusiv în vederea prevenirii activităților teroriste sau a unor infracțiuni grave.*

De asemenea, 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”.

În același timp, Autoritatea națională de supraveghere și-a exprimat opinia în sensul menținerii observațiilor anterioare, referitoare la faptul că 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 IGPF și are calitatea de operator de date cu caracter personal, intrând sub incidența Legii nr. 677/2001, precum și a legii de transpunere a Directivei (UE) 2016/680.

În sensul celor de mai sus, s-a reiterat faptul că este necesară punerea în acord a scopului acestui proiect de lege cu cel stabilit de Directiva (UE) 2016/681, precum și cu dispozițiile acesteia, prin eliminarea din titlul actului normativ a sintagmei *„prevenirea și înlăturarea amenințărilor la adresa securității naționale”*.

Legat de argumentele de mai sus, s-a reiterat necesitatea faptului că se impune și eliminarea pct. 1 din Anexa proiectului de lege care stabilește lista infracțiunilor, referitor la *„infracțiuni contra securității naționale”,* punct care nu se regăsește în Anexa II a Directivei, care cuprinde limitativ lista infracțiunilor grave.

În acest context, raportat la aspectele invocate în expunerea de motive, s-a precizat că, la considerentul 12 din Directiva (UE) 2016/681, se precizează următoarele: *„Definiția infracțiunilor grave ar trebui să cuprindă categoriile de infracțiuni enumerate în anexa II la prezenta directivă.”*

De asemenea, raportat la aplicabilitatea legii inclusiv la zborurile intra-UE, prevăzută la art. 1 alin. (1) lit. a), s-a subliniat faptul că 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 principiului proporționalității și necesității, menționate anterior, cu efecte negative asupra respectării dreptului la viață privată al cetățenilor Uniunii Europene. Totodată, această măsură se impune a fi analizată prin coordonare cu măsurile pe care le preconizează și celelalte state membre, cu prezentarea corespunzătoare a situației din aceste state.

Referitor la prevederile art. 17 din proiect, raportat la faptul că Directiva (UE) 2016/681 prevede că statele membre sunt obligate să asigure că o autoritate de supraveghere națională independentă este responsabilă de consilierea și de monitorizarea privind modul de prelucrare a

datelor PNR, instituția noastră și-a menținut observația potrivit căreia acestea se impun a fi eliminate, întrucât competențele de monitorizare ale UNIP contravin art. 15 din Directivă, reprezentând o suprapunere cu atribuțiile de investigare ale Autorității naționale de supraveghere, o ingerință gravă în competențele acesteia și, implicit, o implementare necorespunzătoare a Directivei (UE) 2016/681.

În ceea ce privește autoritățile competente stabilite la art. 11 alin. (1), astfel cum s-a menționat și în corespondența anterioară, pentru claritatea normei, previzibilitatea și predictibilitatea acesteia, s-a apreciat faptul că 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.

În acest context, s-a apreciat că este necesară menționarea expresă a structurilor competente a Poliției Române (lit. a), raportat la art. 5 din Legea nr. 218/2002, republicată, care se referă inclusiv la instituții de învățământ pentru formarea și pregătirea continuă a personalului, precum și la alte unități necesare pentru îndeplinirea atribuțiilor specifice poliției, înființate potrivit legii.

Aceleași solicitări au fost reiterate 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 unități sau instituții de învățământ, centre de formare profesională, centre, birouri și puncte de contact, precum și alte unități.

În privința art. 42 din proiect referitor la regimul sancționator, au fost menținute observațiile anterioare cu privire la faptul că acesta vine în contradicție cu art. 41, care stabilește competențele exclusive ale Autorității naționale de supraveghere în ceea ce privește monitorizarea prelucrării datelor în sistemul PNR, dar și cu art. 15 din Directiva (UE) 2016/681 (Autoritatea națională de supraveghere) raportat la art. 4-6 (referitoare la unitatea de informații despre pasageri - UIP) din Directiva (UE) 2016/681.

S-a precizat, ca și în corespondența anterioară avută cu Ministerul Afacerilor Interne, faptul că prevederile art. 42 alin. (1) lit. a)-c) se referă la obligații 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 acest sens, s-a solicitat reanalizarea și modificarea art. 42 alin. (4), în concordanță cu prevederile Directivei (UE) 2016/681, astfel încât constatarea și aplicarea sancțiunilor să revină în competența exclusivă a Autorității naționale de supraveghere.

Față de cele de mai sus, ținând cont de necesitatea respectării principiilor de previzibilitate și predictibilitate ale actelor normative, precum și pentru stabilirea garanțiilor necesare pe care statul trebuie să le asigure în exercitarea drepturilor fundamentale ale cetățenilor, raportat la textul proiectului de lege în forma prezentată, Autoritatea națională de supraveghere a **avizat cu observații și propuneri** acest proiect.

Secțiunea a 2-a Puncte de vedere privind diverse chestiuni de protecția datelor

În anul 2017, au fost emise **409 de puncte de vedere**, ca urmare a solicitărilor primite de la persoane fizice, persoane juridice de drept privat și de drept public, referitoare la aplicarea dispozițiilor reglementărilor naționale incidente.

a) Cu privire la prelucrarea datelor în alt scop decât cel pentru care au fost inițial colectate

1. O instituție publică a solicitat punctul de vedere al Autorității naționale de supraveghere în ceea ce privește posibilitatea prelucrării datelor personale ale locatarilor dintr-un cartier rezidențial în alt scop decât cel pentru care au fost inițial colectate.

Față de conținutul acesteia, s-au precizat următoarele:

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

Cazurile de excepție de la obligativitatea obținerii consimțământului sunt reglementate expres de art. 5 alin. (2), astfel:

a) când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;

b) când prelucrarea este necesară în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului;

d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terțul cărui a fi sunt dezvăluite datele;

e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terțului cărui a fi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate;

f) când prelucrarea privește date obținute din documente accesibile publicului, conform legii;

g) când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau științifică, iar datele rămân anonime pe toată durata prelucrării.

Față de textele legale sus menționate, raportat la conținutul adresei transmise din care reieșea că instituția publică dorea să utilizeze numerele de telefon aparținând locatarilor din cartierul rezidențial în scopul transmiterii unor informații administrative către aceștia, Autoritatea națională de supraveghere a subliniat că această operațiune de prelucrare se poate realiza doar cu obținerea, în prealabil, a consimțământului expres și neechivoc al locatarilor, strict pentru scopul sus menționat ("transmiterea de informații administrative privind întrețineri și chiri rezstanțe la plată cât și a altor informații administrative ce vin în sprijinul locatarilor vizati").

S-a mai precizat că prelucrarea datelor cu caracter personal realizată cu încălcarea dispozițiilor art. 5 din Legea nr. 677/2001 întră sub incidența dispozițiilor art. 32 din aceeași lege privind "prelucrarea nelegală a datelor cu caracter personal".

2. O instituție de învățământ a solicitat acordarea avizului pentru prelucrarea datelor cu caracter personal, efectuată prin mijloace de supraveghere video în sălile de clasă, în afara perioadei examenelor naționale.

Legat de această solicitare, așa cum în mod constant Autoritatea națională de supraveghere a subliniat 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.

Prin urmare, ținând cont de necesitatea asigurării unei protecții eficiente a dreptului la viață privată al persoanelor supravegheate prin utilizarea mijloacelor de supraveghere video, raportat la caracterul determinat, explicit și legitim al scopului și la proporționalitatea prelucrării datelor lor cu caracter personal, Autoritatea națională de supraveghere a apreciat că extinderea supravegherii video în afara desfășurării examenelor naționale în sălile de clasă, spații în care își desfășoară activitatea cadrele didactice și elevii, este excesivă raportat la scopul prezentat.

b) Cu privire la prelucrarea de date cu caracter personal având funcție de identificare de către Facebook

O persoană fizică a cerut Autorității naționale de supraveghere informații cu privire la faptul că Facebook l-a solicitat copie după un act de identitate atunci când a încercat să își recupereze parola și conținutul de pe această rețea de socializare.

Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată și completată, stabilește condițiile în care datele cu caracter personal pot fi prelucrate.

Actul normativ sus menționat se aplică, în principal, prelucrărilor de date cu caracter personal efectuate în cadrul activităților desfășurate de operatori stabiliți în România.

Potrivit dispozițiilor art. 5 alin. (1) al legii anterior menționate, principiul de bază ce guvernează prelucrarea datelor personale este consimțământul persoanei vizate, dat în mod expres și neechivoc.

În mod excepțional însă, datele cu caracter personal pot fi prelucrate de către un operator, fără consimțământul persoanei vizate, în mai multe situații de excepție, de strictă interpretare și aplicare, reglementate de art. 5 alin. (2) din Legea nr. 677/2001.

Potrivit art. 8 din Legea nr. 677/2001, prelucrarea datelor cu caracter personal având funcție de identificare, respectiv prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală poate fi efectuată numai dacă persoana vizată și-a dat în mod expres consimțământul sau prelucrarea este prevăzută în mod expres de o dispoziție legală, ori, în alte cazuri, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

În contextul celor de mai sus, s-a precizat că Facebook este un operator de date cu sediul în afara României (Statele Unite ale Americii, respectiv Irlanda pentru prelucrări de date efectuate în statele membre ale Uniunii Europene).

S-a mai menționat că Facebook pune la dispoziție proceduri diverse ce pot fi parcurse de către persoanele interesate (de pildă, pentru schimbarea parolei, raportare de abuzuri etc.), însă parcurgerea acestor proceduri poate presupune furnizarea de informații suplimentare, cerute de Facebook tocmai pentru a putea identifica cu exactitate persoana sau problema la care se face referire.

c) Condiții legale pentru cesionarea unei baze de date

O societate comercială cu activitate principală de selecție și plasare personal a solicitat un punct de vedere, în contextul în care intenționa să preia de la o altă societate o bază de date cu date ale persoanelor fizice, excluzându-le pe cele cu caracter special.

Față de aspectele prezentate, s-au formulat următoarele precizări:

Potrivit art. 4 din Legea nr. 677/2001, modificată și completată, datele cu caracter personal trebuie colectate în scopuri determinate, explicite și legitime.

Deși condiția obținerii consimțământului persoanei vizate este regula instituită de Legea nr. 677/2001, modificată și completată, aceasta stabilește în mod expres și anumite situații de excepție de la obligativitatea obținerii consimțământului în cazul prelucrării datelor personale și, implicit, al dezvăluirii lor prin transmitere, diseminare sau în orice alt mod. Aceste cazuri de excepție, de strictă interpretare, sunt menționate în mod expres la art. 5 alin. (2) din Legea nr. 677/2001 – pentru datele obișnuite – precum și la art. 7, 8, 9 și 10 din aceeași lege, pentru datele cu caracter special.

De asemenea, art. 6 alin. (1) lit. b) din Legea nr. 677/2001, modificată și completată, stabilește faptul că la încheierea operațiunilor de prelucrare a datelor, dacă persoana vizată nu și-a dat în mod expres și neechivoc consimțământul pentru o altă destinație sau pentru o prelucrare ulterioară, operatorul poate transfera datele unui alt operator. Condiția este ca operatorul inițial (cel care transmite datele) să garanteze, prin intermediul unui act juridic (contract), faptul că prelucrările ulterioare au scopuri similare celor în care s-a făcut prelucrarea inițială.

Totodată, în situația în care operatorul obține în mod indirect datele personale ale unei persoane fizice, art. 12 din Legea nr. 677/2001, modificată și completată, stabilește obligația

acestuiua de a furniza anumite informații, printre care identitatea sa, scopul colectării datelor, destinatarii acestora etc. și, dacă este necesar, sursa obținerii datelor. Aceste informații se furnizează la momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu până în momentul primei dezvăluiri.

În consecință, datele personale pot fi transmise unui terț (persoana căreia i se cedează baza de date), fie la consimțământul persoanei vizate, fie în anumite situații de excepție, expres stabilite de lege, de strictă interpretare.

De asemenea, operatorul inițial care a colectat datele, cât și cel care le obține ulterior, sunt obligați să efectueze informarea persoanelor vizate, după cum datele sunt obținute în mod direct sau indirect de la acestea, în conformitate cu Legea nr. 677/2001, modificată și completată.

Obligațiile de mai sus stabilite de lege în sarcina celui care transmite datele și a celui care le primește vor fi stipulate și în contractul (actul) încheiat între cele două entități.

În ceea ce privește aplicarea art. 6 alin. (1) din Legea nr. 677/2001, modificată și completată, aceasta se realizează în momentul încheierii activității societății respective, dacă se bazează pe prelucrări de date cu caracter personal sau la finalizarea unui segment din activitate, cum ar fi vânzarea unei baze de date către o altă persoană, fără ca baza de date să mai fie utilizată de deținătorul inițial care va proceda la ștergerea sau distrugerea datelor, după caz.

d) Stocarea imaginilor pentru o perioadă mai mare de 30 de zile

O societate comercială a solicitat emiterea unui punct de vedere privind condițiile de "stocare a datelor video pe o durată mai mare de 30 de zile".

Autoritatea națională de supraveghere a precizat următoarele:

Potrivit art. 14 alin. (1) din Decizia nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, modificată și completată, "Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video trebuie să fie proporțională cu scopul pentru care se prelucrează datele, *dar nu mai mare de 30 de zile*, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate."

În contextul prevederilor normative sus-menționate, s-a precizat că stocarea datelor (imagini) obținute prin intermediul sistemului de supraveghere video, utilizat și notificat de operator pentru o perioadă mai mare de 30 de zile, nu se poate realiza decât dacă situația



expusă (monitorizarea zilnică a debitului afluent și a debitului de servitute/salubru aval de captare ori a debitelor asigurate în aval de priza și a prizei hidrometrice montate la prizele MHC-urilor) este expres reglementată de lege ori operatorul justifică temeinic necesitatea unei astfel de stocări.

S-a menționat că, potrivit dispozițiilor art. 4 alin. (1) din Legea nr. 677/2001, modificată și completată, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credință și în conformitate cu dispozițiile legale în vigoare, colectate în scopuri determinate, explicite și legitime, să fie adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate, să fie exacte și, dacă este cazul actualizate, să fie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate. Așadar, o stocare a imaginilor pe o perioadă mai mare de 30 de zile trebuie să fie proporțională cu scopul prelucrării datelor.

În contextul prelucrării menționate anterior, s-a comunicat faptul că este necesară luarea în considerare a faptului că vor fi prelucrate și date ale angajaților, așa cum reiese din notificarea deja înregistrată în registrul de evidență a prelucrărilor de date cu caracter personal de către operator.

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

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

Ca atare, Autoritatea națională de supraveghere a precizat că este necesară depunerea unei documentații care să ateste incidența unui caz temeinic justificat, raportat la situația prezentată, în măsura în care nu există o prevedere legală expresă.



✦ **Puncte de vedere privind unele cauze aflate pe rolul
Curții de Justiție a Uniunii Europene**

În anul 2017 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-25/17** privind interpretarea art. 2 lit. b), c), d) și e), 3, 8, 10, 16 și 17 alin. (1) din Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- **Cauza C - 40/17 – Fashion ID** privind interpretarea art. 2 lit. d) și h), 7 lit. a) și f), 10, 22, 23 și 24 din Directiva 95/46/CE;
- **C - 345/17 – Buivids** privind interpretarea art. 2, 3 și 9 din Directiva 95/46/CE;
- **Cauza C - 507/17 – Google** privind interpretarea art. 7 lit. e) și f), 12, 14 raportat la Hotărârea Google Spain SL, Google Inc. împotriva Agencia Española de Protección de Datos (AEPD), Mario Costeja González a Curții de Justiție, pronunțată în cauza C - 131/12 (în special, prin raportare la punctele 53-56 din aceasta);
- **Cauza C - 573/17** privind interpretarea art. 8 alin. (2) și (5), 14, în contextul Hotărârii pronunțate de Curtea de Justiție în cauza C - 131/12;
- **Cauza C - 623/17** privind impactul Hotărârii Curții de Justiție a Uniunii Europene din 21 decembrie 2016, în cauzele conexe **C-203/15 și C-698/15** (Hotărârea Watson), cu precădere prin raportare la punctele 119-125, în cazul activităților legate de securitatea națională, desfășurate de agențiile de securitate și de informații ale unui stat membru.

Secțiunea a 3-a Aspecte relevante referitoare la aplicarea Regulamentului General privind Protecția Datelor

a) Măsuri naționale destinate asigurării aplicării Regulamentului

O persoană fizică a solicitat informații privind măsurile de aplicare a Regulamentului (UE) 2016/679.

Autoritatea națională de supraveghere a precizat că, întrucât Ministerul Afacerilor Interne a condus negocierile în cadrul Reuniunii Comitetului pentru protecția datelor și schimbul de informații – DAPIX de la Consiliul European, cu privire la pachetul legislativ din domeniul protecției datelor personale, acesta a inițiat Memorandumul cu tema: Transpunerea în legislația națională a Directivei (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016, precum și crearea cadrului legal pentru aplicarea Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016.

Prin acest Memorandum, s-a propus constituirea Grupului Interministerial de Lucru pentru asigurarea luării măsurilor privind aplicarea directă a dispozițiilor Regulamentului (UE) 2016/679 și pentru transpunerea Directivei (UE) 2016/680, coordonat de către Ministerul Afacerilor Interne.

În contextul lucrărilor desfășurate în cadrul Grupului, Autoritatea națională de supraveghere a pregătit proiectul de Lege pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum și pentru abrogarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, dar și a Expunerii de motive. Acest proiect de lege vizează punerea în aplicare a unor dispoziții ale regulamentului, respectiv a prevederilor art. 51-55, 57-59, 62, 77, 79, 80 și 82-84.

Prin urmare, la data primirii solicitării, s-a comunicat că proiectul de lege sus-menționat se află în procedurile de avizare prevăzute de Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea și prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea adoptării/aprobării, adoptat prin Hotărârea Guvernului nr. 561/2009.

S-a mai precizat că, în cadrul Grupului Interministerial de Lucru, se află în analiză și un alt proiect de Lege privind unele măsuri de punere în aplicare a Regulamentului (UE) 2016/679.

b) Responsabilul cu protecția datelor - DPO

Mai multe persoane fizice și juridice au solicitat puncte de vedere referitoare la responsabilul cu protecția datelor.

Autoritatea națională de supraveghere a comunicat următoarele:

Referitor la responsabilul cu protecția datelor cu caracter personal menționăm că, potrivit art. 37 alin. (5) din Regulamentul UE 2016/679, acesta trebuie să fie "desemnat pe baza calificărilor profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39."

Responsabilul cu protecția datelor poate fi angajat al operatorului/persoanei împuternicite de operator sau poate să-și îndeplinească sarcinile pe baza unui contract de prestări servicii. S-a menționat că Regulamentul nu impune o formă de organizare sub care poate funcționa responsabilul pentru protecția datelor.

Prin prisma Regulamentului, s-a apreciat că responsabilul cu protecția datelor poate îndeplini și altă funcție în cadrul operatorului sau al unei persoane împuternicite de operator și îi pot fi încredințate și alte sarcini și atribuții, cu condiția ca acestea să nu dea naștere unor conflicte de interese (de ex: nu poate fi, de pildă, director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane ori șeful departamentului IT).

De asemenea, s-a precizat că, în contextul prevederilor din Regulament referitoare la responsabilul cu protecția datelor și al dispozițiilor art. 10 și art. 11 din Legea nr. 514/2003 privind organizarea și exercitarea profesiei de consilier juridic, care stabilesc, în mod expres, atât incompatibilitățile, cât și compatibilitățile cu privire la exercitarea profesiei de consilier juridic, Uniunea Colegiiilor Consilierilor Juridici din România a considerat că nu există impedimente sau restricții legale, deontologice sau procedurale pentru exercițiul simultan al profesiei de consilier juridic și al ocupației de responsabil cu protecția datelor în cadrul aceluiași operator sau distinct la operatori diferiți.

Cu toate acestea, responsabilul trebuie să aibă capacitatea de a îndeplini sarcinile, fiind necesare anumite calități personale (ex: integritate și etică profesională), cunoștințe, dar și o anumită poziție în cadrul organizației.

De asemenea, responsabilul trebuie să aibă anumite calități profesionale, precum: experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere adecvată a RGPD; nivelul necesar de cunoștințe în domeniul protecției datelor în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție necesar pentru datele cu caracter personal prelucrate; să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informății și necesitățile de securitate și protecție a datelor prelucrate de operator; în cazul unei autorități sau instituții publice, responsabilul cu protecția datelor trebuie să dețină, de asemenea, cunoștințe privind reglementările legale referitoare la organizarea și funcționarea acestora, precum și a procedurilor interne administrative ce vizează desfășurarea activității.

S-a subliniat, totodată, faptul că, potrivit art. 37 alin. (7) din Regulament, operatorul sau persoana împuternicită de operator are obligația de a comunica autorității de supraveghere doar datele de contact ale responsabilului cu protecția datelor.

Prin Ordinul nr. 1786/2017 privind modificarea și completarea Clasificării ocupațiilor din România - nivel de ocupație (sase caractere), aprobată prin Ordinul ministrului muncii, familiei și protecției sociale și al președintelui Institutului Național de Statistică nr. 1.832/856/2011, a fost introdusă în COR această nouă ocupație sub denumirea "responsabil cu protecția datelor cu caracter personal" - cod COR 242231.

Pentru mai multe informații Autoritatea națională de supraveghere a recomandat consultarea *Ghidului privind Responsabilul cu protecția datelor (DPO)*, emis de Grupul de Lucru Art. 29, care este format din reprezentanții tuturor autorităților de supraveghere din statele membre ale Uniunii Europene și care, printre altele, elaborează o serie de opinii/ghiduri, privind aplicarea coerentă și unitară a dispozițiilor regulamentului.

c) Conșimțământ în mediul on-line

În ceea ce privește forma conșimțământului, prevederile art. 5 din Legea nr. 677/2001 impun regula potrivit căreia orice prelucrare de date cu caracter personal poate fi efectuată

numai dacă persoana vizată și-a dat conșimțământul în mod expres și neechivoc pentru acea prelucrare.

Prin urmare, acesta trebuie obținut într-o modalitate care să dovedească acordarea sa de către persoana vizată sau de către reprezentantul legal al acesteia, cu subînțelegerea că acordul trebuie obținut în mod expres pentru fiecare dintre scopurile prelucrării (de ex. dacă se intenționează a se realiza și activitatea de reclamă, marketing și publicitate, alături de scopul principal) care trebuie precizate în mod explicit.

Această cerință este în acord și cu art. 7 din Regulamentul (UE) 2016/679, care abrogă Directiva 95/46/CE și, implicit, Legea nr. 677/2001, Regulament ce va fi pus în aplicare începând cu data de 25 mai 2018.

Astfel, potrivit dispozițiilor legale sus-menționate, "în cazul în care prelucrarea se bazează pe conșimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat conșimțământul pentru prelucrarea datelor sale cu caracter personal."

Considerentul 32 din regulamentul sus-menționat stabilește următoarele:
"Conșimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acești ar putea include bifarea unei căsuțe atunci când persoana viztează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un conșimțământ. Conșimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, conșimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care conșimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă conșimțământul."

În măsura în care serviciile operatorului se adresează și minorilor, art. 8 din Regulamentul (UE) 2016/679, intitulat "Condiții aplicabile în ceea ce privește conșimțământul copiilor în legătură cu serviciile societății informaționale" stabilește faptul că: "Operatorul

depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.”

În acest context, este de precizat faptul că, până la 25 mai 2018, potrivit art. 1 alin. (1) lit. h) din Decizia nr. 200/2015 a Președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (publicată în Monitorul Oficial al României, Partea I, nr. 969 din 28 decembrie 2015), notificarea autorității de supraveghere este necesară când prelucrarea datelor cu caracter personal ale minorilor este efectuată prin intermediul internetului sau al mesageriei electronice.

Astfel, în măsura în care un operator prelucrează datele minorilor prin intermediul internetului sau al mesageriei electronice, se impune fie depunerea unei notificări, fie completarea unei notificări existente.

În ceea ce privește tipul de date care trebuie prelucrate, Legea nr. 677/2001, modificată și completată, stabilește, la art. 4 alin. (1) lit. c), faptul că acestea trebuie să fie “adevate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate”, cu alte cuvinte, cele strict necesare îndeplinirii scopului.

În același timp, este de subliniat faptul că prelucrările de date efectuate vor fi precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 12 din Legea nr. 677/2001, care obligă operatorul să furnizeze persoanei vizate o serie de informații.

În acest context, este de precizat faptul că art. 25 din Regulamentul (UE) 2016/679 stabilește, ca obligații generale ale operatorului, următoarele:

“(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentului regulament și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date

colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.”

În cadrul prelucrărilor menționate operatorii vor avea în vedere și prevederile Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

d) Incidente de securitate și notificare

O persoană fizică a solicitat un punct de vedere referitor la notificarea prelucrărilor de date cu caracter personal efectuate după 25 mai 2018.

Autoritatea națională de supraveghere a precizat următoarele:

De la data aplicării Regulamentului (UE) 2016/679, își va înceta aplicabilitatea Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Ca atare, după data de 25 mai 2018, operatorii nu vor mai avea obligația de notificare a prelucrărilor de date, obligație instituită de prevederile art. 22 din Legea nr. 677/2001. De asemenea, operatorii nu vor mai avea nici obligația obținerii numărului de operator.

Pe de altă parte, art. 33 din Regulamentul (UE) 2016/679 prevede că operatorul are obligația de a *notifica autoritatea de supraveghere în situația în care are loc o încălcare a securității datelor cu caracter personal*. Alin. (3) al acestui articol stabilește ce trebuie să vizeze notificarea autorității de supraveghere.

Referitor la stabilirea unui formular de notificare, în prezent există stabilit un astfel de formular, pentru îndeplinirea obligației operatorilor - furnizorii de servicii publice de rețele sau servicii de comunicații electronice, potrivit Deciziei Autorității nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice (a se vedea informațiile postate pe pagina <http://www.dataprotection.ro/servlet/ViewDocument?id=1100>).

Prin urmare, Autoritatea națională de supraveghere va avea în vedere punerea la dispoziția operatorilor a posibilității de îndeplinire a obligației de notificare a autorității, în temeiul art. 33 din Regulamentul (UE) 2016/679.

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

În anul 2017, s-a înregistrat o creștere semnificativă a acțiunilor prin care s-au contestat actele Autorității naționale de supraveghere care au ajuns la 221, spre deosebire de anul 2016 când s-au primit 112 cereri de chemare în judecată.

Având în vedere finalizarea în mod favorabil pentru instituția noastră a multor acțiuni în instanță, pe parcursul anului 2017, prezentăm mai jos câteva cazuri relevante:

❖ Hotărâre pronunțată într-un litigiu privind neîndeplinirea obligațiilor privind informarea persoanelor vizate

În exercitarea atribuțiilor de control, Autoritatea națională de supraveghere a efectuat o investigație din oficiu la un operator de date cu caracter personal, instituție publică centrală.

Investigația sus-menționată a avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, a măsurilor de securitate, precum și a dispozițiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Prin procesul-verbal de constatare/sancționare s-a constatat săvârșirea următoarei fapte:

“Prelucrarea nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, prin încălcarea art. 12 din această lege, întrucât instituția publică în cauză nu a realizat informarea persoanelor vizate ale căror date personale au fost prelucrate ca urmare a protocoloalelor încheiate având ca obiect schimburi de informații în niciuna din modalitățile prevăzute de lege, conform constatărilor din acest proces-verbal. Pentru această faptă s-a acordat sancțiunea amenzii în cuantum de 6000 lei.

Din investigație a rezultat faptul că instituția publică realizează schimburi de informații referitoare la prelucrarea de date cu caracter personal atât cu instituții publice, cât și cu altele entități din domeniul privat, în baza unor protocoale încheiate cu acestea. Prin aceste

protocoale sunt stabilite, printre altele, obiectul protocolului, obligațiile părților și modalitatea de realizare a schimbului de informații.

În ceea ce privește informarea persoanelor vizate ale căror date cu caracter personal sunt prelucrate și dezvăluite de către instituția publică, la data efectuării controlului, aceasta nu a prezentat dovada informării persoanelor vizate, individual sau în altă modalitate, în concordanță cu art. 12 din Legea nr. 677/2001, pentru nicio situație în care a realizat schimburi de informații referitoare la date cu caracter personal.

Pe site-ul instituției publice respective era postată o notă de informare a persoanelor vizate cu privire la prelucrarea datelor cu caracter personal realizată de instituție conform atribuțiilor legale, dar care nu cuprindea mențiuni cu privire la prelucrarea datelor personale și dezvăluirea acestora în scopul realizării schimburilor de informații în baza protocoloalelor respective și nu respecta pe deplin cerințele art. 12 din Legea nr. 677/2001.

Fiind vorba de o prelucrare nouă, specifică, efectuată în baza unor protocoale al căror conținut nu era cunoscut de persoanele fizice în cauză, prin mijloace electronice, prin intermediul unei aplicații care viza un număr mare de persoane fizice, instituția publică avea obligația informării persoanei vizate așa cum stabilesc dispozițiile art. 12 alin. (1) din Legea nr. 677/2001, cu atât mai mult cu cât colecta datele direct de la persoana fizică.

Chiar și dispozițiile legale care reglementează activitatea acestei instituții fac trimitere la respectarea Legii nr. 677/2001, deci implicit și la art. 12 din lege.

Prin urmare, instituția publică are obligația să asigure informarea persoanei vizate într-un mod dar și exact, astfel încât aceasta să cunoască detaliile prelucrării datelor sale, precum și drepturile de care beneficiază.

Astfel, în măsura în care, ulterior momentului colectării datelor de la persoanele fizice, în relația cu instituția publică, apar scopuri noi (atribuții noi ale operatorului, în speță instituția publică) pentru care se prelucreează datele, precum și destinatarii noi, necunoscuți la momentul obținerii datelor personale (în speță, încheierea protocoloalelor cu entitățile respective și dezvăluirea datelor către acestea), informațiile vizate de art. 12 din Legea nr. 677/2001 trebuie completate cu toate elementele nou-apărute, pentru a se asigura prelucrarea datelor cu bună-credință și în conformitate cu legea (principiul statuat de art. 4 alin. 1 lit. a) din Legea nr. 677/2001).

Prin urmare, conținutul informării sumare identificate pe site-ul instituției publice, la data efectuării controlului, nu respecta exigențele acestor principii, respectiv al caracteristicilor

“determinat” și “explicit” ale scopului, precum și al prelucrării datelor cu bună-credință și în conformitate cu legea.

În acest context, Autoritatea națională de supraveghere a apreciat că nu se poate admite faptul că persoana vizată ar cunoaște toate aceste informații, încă de la începutul raporturilor sale cu instituția publică, astfel încât să nu mai fie necesară informarea sa pe întreg parcursul acestei relații, în cadrul activității de prelucrare a datelor personale.

Curtea de Apel București a menținut procesul-verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere, ca legal și temeinic.

Pentru a hotărî astfel, instanța de apel a reținut că legiuitorul a permis ca informarea să se realizeze în funcție de circumstanțele prelucrării, pentru a acoperi toate ipotezele care s-ar ivi în practică. Prin urmare, instituția publică a nesocotit dispozițiile art. 32 din Legea nr. 677/2001, întrucât nu a luat o minimă măsură de informare colectivă, informare care putea fi expusă pe site-ul propriu, adresată tuturor persoanelor fizice aflate în relație cu instituția publică, iar nu în mod obligatoriu individual.

Totodată, Curtea de Apel București a reamintit că, prin hotărârea preliminară pronunțată în Cauza C-201/14 Bara și alții împotriva Președintelui Casei Naționale de Asigurări de Sănătate, Casei Naționale de Asigurări de Sănătate și Agenției Naționale de Administrare Fiscală, CJUE a statuat faptul că “articolele 10, 11 și 13 din Directiva 95/46/CE trebuie interpretate în sensul că se opun unor măsuri naționale precum cele în discuție în litigiul principal, care permit unei autorități a administrației publice a unui stat membru să transmită date personale unei alte autorități a administrației publice și prelucrarea lor ulterioară, fără ca persoanele vizate să fi fost informate despre această transmitere sau despre această prelucrare”.

De asemenea, instanța de apel a subliniat aspectele reținute de Curtea de Justiție a Uniunii Europene, potrivit cărora “această cerință a informării persoanelor vizate de prelucrarea datelor lor cu caracter personal este cu atât mai importantă cu cât este o condiție necesară exercitării de către aceste persoane a dreptului lor de acces și de rectificare a datelor prelucrate, definit în articolul 12 din Directiva 95/46/CE, și a dreptului de opoziție al acestora față de prelucrarea datelor respective, vizat în articolul 14 din această directivă.”

În concluzie, Autoritatea națională de supraveghere subliniază că obstrucționarea sau negarea dreptului de informare este o practică inacceptabilă care aduce atingere principiului transparenței prelucrărilor de date efectuate de către instituțiile publice care, cu atât mai mult, au obligația legală pozitivă de a asigura respectarea drepturilor și libertăților fundamentale ale

cetățenilor aflați pe o poziție de inegalitate, întrucât prelucrarea nu se efectuează pe baza consimțământului lor, iar nu doar o obligație negativă de a nu aduce atingere acestora.

Hotărârea pronunțată de instanță în favoarea instituției noastre a rămas definitivă.

❖ **Hotărâre pronunțată într-un litigiu privind nerespectarea dreptului de acces al persoanei vizate**

O persoană fizică s-a adresat Autorității naționale de supraveghere și a reclamat faptul că o societate din domeniul privat care furnizează servicii de comunicații electronice nu i-a furnizat toate informațiile solicitate în urma exercitării dreptului de acces prevăzut de art. 13 alin. (1) din Legea nr. 677/2001, informații pe care le-a solicitat, de la acest operator, în scris, în mai multe rânduri.

În plus, petentul reclama și faptul că trei dintre răspunsurile societății i-au fost trimise prin intermediul poștei electronice, cu toate că solicitase în mod expres ca răspunsurile să-i fie comunicate prin intermediul Poștei Române, indicând adresa la care să-i fie transmise.

Urmare a investigației efectuate de Autoritatea națională de supraveghere s-a constatat săvârșirea faptei de “Prelucrare nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 13 din Legea nr. 677/2001, întrucât operatorul nu a comunicat persoanei fizice vizate toate informațiile solicitate de către aceasta prin cererile sale și nici nu i-a transmis răspunsurile la adresa indicată în cereri. Operatorului i s-a aplicat amendă în cuantum de 1500 lei, iar acesta a contestat în instanță sancțiunea aplicată.

Așa cum s-a putut constata din investigație, răspunsurile operatorului au fost formulate generic, fără furnizarea tuturor informațiilor pe care Legea nr. 677/2001 le stabilește în art. 13, deși persoana fizică în cauză are dreptul la comunicarea informațiilor privind scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele, precum și la comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării.

De asemenea, s-a constatat că operatorul nu desfășura efectiv activitățile prevăzute la art. 2 alin. (5) din Legea nr. 677/2001, respectiv dintre cele din domeniul ordinii publice sau al dreptului penal, nefiind o autoritate publică ce face aplicarea excepțiilor art. 16 din Legea nr. 677/2001.

Totodată, în timpul investigației, operatorul nu a făcut dovada faptului că ar fi fost o solicitare din partea autorităților publice de acces la datele petentului înregistrate în evidențele sale, pentru a justifica faptul că nu avea posibilitatea de a asigura exercitarea dreptului de acces al acestuia, la data formulării cererilor petentului.

În consecință, nefiind îndeplinite prevederile art. 16 din Legea nr. 677/2001 coroborate cu art. 3¹ din Legea nr. 506/2004, dreptul de acces la date, astfel cum este prevăzut de art. 13 din Legea nr. 677/2001, trebuia asigurat de către operator petentului.

Art. 3¹ intitulat "Proceduri de accesare" din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, modificată și completată, stabilește faptul că: "Furnizorii au obligația de a stabili proceduri interne pentru a răspunde solicitărilor de accesare a datelor cu caracter personal ale utilizatorilor. La cerere, aceștia oferă Autorității naționale de supraveghere informații despre procedurile respective, numărul de solicitări primite, justificarea legală invocată în solicitare și răspunsul oferit solicitanților."

Prin urmare, operatorul nu poate stabili, în mod arbitrar și subiectiv, o altă procedură de asigurare a exercitării drepturilor persoanelor vizate, care excede dispozițiilor art. 13 din Legea nr. 677/2001.

Instanța de fond a respins acțiunea operatorului și a menținut procesul-verbal de constatare/sanționare încheiat de Autoritatea națională de supraveghere, ca temeinic și legal.

Prin hotărârea sa, instanța de fond a reținut că:

"...reclamanta nu a comunicat petiționarului niciuna din informațiile solicitate și nici nu a uzat de calea indicată pentru transmiterea acestora. Mai mult, reclamanta a recunoscut faptul că în procesul de verificare nu a putut identifica cu certitudine dezvăluri către terți ale datelor personale ale petentului.

Răspunsurile reclamantei au fost generice, emise într-un vădit dezinteres față de drepturile subiective ale petiționarului.

Situația de excepție invocată de reclamantă, de la furnizarea datelor solicitate de petent nu o poate exonera de răspundere întrucât nu s-a făcut dovada incidenței sale, respectiv a premisei reglementate de art. 2 alin. (5) din Legea nr. 677/2001. Reclamanta nu a făcut dovada faptului că ar fi existat o solicitare din partea autorităților publice cu competență în urmărirea activității infracționale, cu privire la datele personale ale petentului, pentru a justifica abordarea sa în relația cu acesta.

Reclamanta nu a furnizat niciun motiv care ar fi împiedicat-o să respecte modalitatea concretă de transmitere a informațiilor, respectiv calea poștei clasice și nu cea electronică."

De asemenea, instanța a reținut în mod corect faptul că *"...față de atitudinea reclamantei Tribunalul consideră că în speță nu se impune înlocuirea sancțiunii amenzi cu avertisment, gradul de pericol social al faptei comise fiind unul ridicat, omisiunea reclamantei creând un sentiment de insecuritate și arbitrar petentului ale cărui drepturi era obligată să le respecte."* Totodată, instanța a mai reținut și faptul că *"reclamanta se face vinovată de o dublă încălcare a drepturilor petentului, respectiv atât de necomunicarea informațiilor solicitate cât și de ignorarea modalității de comunicare a acestora."*

Hotărârea instanței a rămas definitivă.

❖ Hotărâre pronunțată într-un litigiu privind neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate

Autoritatea națională de supraveghere a demarat o investigație din oficiu la o societate care are ca domeniu de activitate servicii de transport în regim taxi, în vederea verificării modului de respectare a prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date și a măsurilor de securitate și a Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

În urma investigației efectuate, s-a constatat săvârșirea de către entitatea controlată a următoarelor fapte contravenționale:

I. Omisiunea de a notifica și notificarea cu rea-credință, contravenție prevăzută de art. 31 din Legea nr. 677/2001, sub forma omisiunii de a efectua notificarea în condițiile art. 22 din Legea nr. 677/2001, întrucât societatea nu a notificat prelucrarea datelor cu caracter personal pe care o efectuează prin intermediul aplicației utilizate în scopul preluării/plasării comenzilor de taxi, pentru care s-a aplicat amendă în cuantum de 1000 lei.

II. Neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate, prevăzută de art. 33 din Legea nr. 677/2001, întrucât societatea, până la data procesului-verbal de constatare/sanționare nu a adoptat măsuri de confidențialitate și securitate a datelor cu caracter personal prelucrate, conform art. 19 și 20 din Legea nr. 677/2001, sub aspectul elaborării/implementării unei politici de securitate, a stabilirii unor

instrucțiuni precise pentru persoana care are acces la datele personale sau instrucțiuni pentru persoanele împuternicite, pentru care s-a aplicat amendă în cuantum de 3000 de lei.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat, acesta solicitând anularea procesului-verbal.

Instanța a respins plângerea, apreciind că *"petenta nu a invocat critici concrete de nelegalitate și netemeinicie a procesului-verbal de contravenție, susținând că individualizarea sancțiunilor aplicate a fost realizată cu nerespectarea dispozițiilor art. 5 alin. 5 din Ordonanța Guvernului nr. 2/2001."*

Împotriva sentinței instanței de fond societatea a declarat apel, iar instanța superioară a respins apelul formulat, soluția fiind definitivă în favoarea instituției noastre.

Decizia definitivă a instanței a confirmat abordarea Autorității naționale de supraveghere de respectare a condițiilor de legitimitate a prelucrării datelor cu caracter personal, așa cum sunt acestea prevăzute de Legea nr. 677/2001 și Legea nr. 506/2004.

În contextul dat, atragem atenția asupra faptului că prelucrarea de date cu caracter personal, în cadrul activității derulate de societățile care au ca domeniu de activitate servicii de transport în regim taxi, intră sub incidența legislației privind protecția datelor personale, astfel de societăți fiind ținute, în calitate de operatori de date, de respectarea tuturor obligațiilor stabilite de lege în sarcina acestora.

❖ **Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală a datelor cu caracter personal, de către o casă de asigurări de sănătate**

Autoritatea națională de supraveghere a demarat o investigație din oficiu la o casă de asigurări de sănătate, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum și a dispozițiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Investigația s-a declanșat ca urmare a unei sesizări a mass-media privind publicarea pe Internet, pe pagina proprie a casei de asigurări de sănătate, a unei liste conținând un număr total de 18.607 persoane fizice (nume, prenume, adresă completă). Astfel, din verificările efectuate, s-a constatat că această listă denumită "Situația cardurilor returnate la sediul instituției de către Poșta Română" era publicată pe internet.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat săvârșirea de către casa de asigurări de sănătate a faptei contravenționale de prelucrarea nelegală a datelor cu caracter personal, contravenție prevăzută de art. 32 din Legea nr. 677/2001, prin încălcarea art. 4 alin. (1) lit. a) și art. 5 alin. (1) din aceeași lege, întrucât începând cu perioada iulie-august 2015, casa de asigurări de sănătate a publicat pe Internet, pe pagina proprie, o listă accesibilă oricărei persoane care accesează pagina de Internet în cauză, conținând datele personale a 18.607 persoane fizice (nume, prenume, adresă completă) privind situația cardurilor returnate la sediul instituției, pentru care s-a aplicat sancțiunea amenzii în cuantum de 8000 lei.

Procesul-verbal de constatare/sancționare a fost contestat în instanță de operatorul sancționat, acesta solicitând anularea procesului-verbal.

Instanța a analizat actul contestat de reclamantă, respectiv procesul-verbal de contravenție, acesta fiind verificat din perspectiva legalității și a temeiniciei, inclusiv sub aspectul motivelor invocate de ambele părți din dosar.

Astfel, în mod corect instanța a constatat că *"Situația de fapt reținută de agentul constator nu este contestată de reclamantă"*.

În consecință, instanța a reținut că respectiva casă de asigurări de sănătate, în calitate de operator, a prelucrat și dezvăluit pe Internet date cu caracter personal a 18.607 asigurați.

Împotriva sentinței instanței de fond casa de asigurări de sănătate a declarat apel, dar instanța superioară a respins apelul formulat, soluția rămânând definitivă în favoarea instituției noastre.

❖ **Hotărâre pronunțată într-un litigiu privind securitatea datelor și supravegherea angajaților**

Autoritatea națională de supraveghere a efectuat o investigație la un operator, ca urmare a unei plângeri prin care se sesiza faptul că au fost găsite pe stradă documente aparținând operatorului, care conțineau date personale ale angajaților operatorului și ale proprietarilor apartamentelor din imobilul administrat de acesta.

De asemenea, a mai fost sesizat aspectul că operatorul are montate camere de supraveghere în birouri și nu a adoptat măsurile legale ce se impun pentru securitatea și protecția datelor personale.

Ca urmare a controlului efectuat, Autoritatea națională de supraveghere a constatat că operatorul deține un sistem de supraveghere video, începând cu luna august 2015, alcătuit din 8 camere de supraveghere video, montate atât în exteriorul clădirii, cât și în interiorul acesteia (în birouri). Operatorul nu a putut face dovada notificării prelucrării datelor prin sistemul de supraveghere video și nici a informării persoanelor vizate cu privire la acest sistem.

De asemenea, operatorul nu a putut face dovada obținerii consimțământului expres și neechivoc al salariaților, a acordului sindicatului anterior montării camerelor sau a unui aviz din partea Autorității naționale de supraveghere consultate în acest sens.

S-a mai constatat că operatorul nu a făcut dovada existenței măsurilor de securitate a prelucrării datelor personale.

Faptele săvârșite de operator au fost sancționate contravențional, atât cu avertisment cât și cu amendă, iar procesul-verbal de constatare/sancționare a fost contestat în instanță.

Instanța, analizând probatoriul administrat în cauză, a constatat că procesul-verbal de constatare/sancționare emis de Autoritatea națională de supraveghere este legal întocmit, astfel că au fost menținute sancțiunile contravenționale aplicate.

Hotărârea a fost contestată de operator, însă soluția instanței care a judecat cauza de atac a fost aceeași, prin respingerea recursului declarat de operator.

❖ **Hotărâre pronunțată într-un litigiu privind transmiterea de mesaje comerciale nesolicitate**

Autoritatea națională de supraveghere a efectuat o investigație la un operator, ca urmare a unei plângeri prin care se sesiza o încălcare a prelucrării datelor prin transmiterea de mesaje comerciale nesolicitate, respectiv fără acordul prealabil al persoanei vizate.

La momentul controlului, operatorul a declarat că adresele de e-mail folosite pentru trimiterea de newslettere provin din mai multe surse: importarea listei din CSV, abonare la newsletter pe site-ul operatorului, completare de pliante denumite "Fișe impresii" de către clienții societății, din pagina de facebook a societății, din completarea formularului de "Cerere ofertă" de pe site-ul societății.

În cadrul investigației s-au efectuat mai multe teste privind modalitatea de abonare și dezabonare, constatându-se astfel că la acel moment funcționa mecanismul de abonare "dublu opt-in", implementat odată cu utilizarea unei aplicații.

De asemenea, operatorul a mai declarat că în anul 2016 a derulat și o campanie de trimitere de mesaje către utilizatorii adreselor de e-mail din baza de date, cu solicitarea de a confirma expres dacă se dorește sau nu primirea în continuare de newsletter. Dintre utilizatorii contactați astfel au răspuns 1071, dintre care 142 au declarat că nu doresc să mai primească newsletter.

Din verificarea site-ului operatorului în timpul controlului a rezultat că nu exista o informare completă 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. De asemenea, pe "Fișele de impresii" nu era inclus un acord expres al persoanelor cu privire la utilizarea adresei de e-mail sau a numărului de telefon în scopul trimiterii de comunicații comerciale prin mijloace de comunicații electronice, așa cum prevede art. 12 alin. (1) din Legea nr. 506/2004.

S-a constatat că operatorul nu a putut face dovada privind obținerea în prealabil a consimțământului expres al petentului care a sesizat posibila încălcare a prelucrării datelor cu caracter personal.

Faptele săvârșite de operator au fost sancționate contravențional atât cu avertisment cât și cu amendă, iar procesul-verbal de constatare/sancționare a fost contestat în instanță.

Analizând probatoriul administrat în cauză, instanța a constatat că procesul-verbal de constatare/sancționare emis de Autoritatea națională de supraveghere este legal întocmit, astfel fiind menținute sancțiunile contravenționale aplicate.

Hotărârea instanței a rămas definitivă.

❖ **Hotărâre pronunțată într-un litigiu privind prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit**

Autoritatea națională de supraveghere a efectuat o investigație, din oficiu, la un operator, având ca obiect prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit.

În acest sens, Autoritatea națională de supraveghere a solicitat operatorului printr-o adresă rapoartele de credit, precizarea datei scadenței (ziua) privind obligația de plată pentru zece clienți precizați, notificările (informările) clienților cu privire la faptul că aceștia urmează să fie raportați la Biroul de Credit cu debite restante, conform Deciziei nr. 105/2007, dar nu mai vechi de 6 luni, precum și dovada notificărilor transmise către clienți.

Operatorul a răspuns adresei Autorității naționale de supraveghere transmițând documentele pe care le deținea raportat la solicitarea autorității.

Din documentele puse la dispoziție, s-a constatat, pentru unii dintre clienți, că operatorul nu a realizat o înștiințare prealabilă a persoanei vizate la fiecare obligație de plată (în scris), așa cum prevede art. 8 alin. (2) din Decizia nr. 105/2007. În cazul altor clienți, deși a transmis o înștiințare prealabilă cu 15 zile înainte de raportare, operatorul nu a furnizat acestora informațiile prevăzute de art. 9 din Decizia nr. 105/2007.

De asemenea, din documentele puse la dispoziție de operator și din situația de transmitere de date la Biroul de Credit, a reieșit că, pentru anumiți clienți, operatorul a transmis date negative la Biroul de Credit înainte de împlinirea termenului de 30 de zile de la data scadenței, contrar prevederilor art. 5 alin. (1) din Decizia nr. 105/2007.

Totodată, s-a constatat că operatorul prelucrează date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit în mod neunitar la nivel național, astfel că în majoritatea situațiilor nu respectă prevederile Deciziei nr. 105/2007.

Operatorul investigat nu a putut pune la dispoziția Autorității naționale de supraveghere documente și dovezi privind informarea prealabilă transmisă persoanelor vizate cu 15 zile înainte de a raporta datele negative la Biroul de Credit, în conformitate cu art. 8 alin. (2) și art. 9 alin. (1) din Decizia nr. 105/2007 coroborat cu art. 12 din Legea nr. 677/2001, astfel că raportarea nu a respectat termenul de 30 de zile de la scadență.

În consecință, operatorul a fost sancționat cu amendă la cuantumul maxim prevăzut de lege, iar procesul-verbal de constatare/sancționare a fost contestat la instanță.

Instanța, analizând probatoriul administrat în cauză, a constatat că procesul-verbal de constatare/sancționare emis de Autoritatea națională de supraveghere este legal întocmit, fapt pentru care au fost menținute sancțiunile contravenționale aplicate.

Hotărârea a devenit definitivă prin respingerea apelului declarat de operator.

Secțiunea a 5-a Informare publică

În cursul anului 2017, Autoritatea națională de supraveghere a continuat activitățile și modalitățile de comunicare destinate informării publicului larg, cu privire la regulile specifice de prelucrare a datelor cu caracter personal, cu precădere în contextul Regulamentului (UE) 2016/679.

Astfel, a fost organizată Ziua Europeană a Protecției 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, instituția noastră a participat activ la cele mai importante evenimente cu incidentță 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 și asigurarea confidențialității prelucrărilor de date cu caracter personal.

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

➤ Ziua Europeană a Protecției Datelor

Pe data de 28 ianuarie 2017, s-a aniversat Ziua Europeană a Protecției Datelor, care a marcat împlinirea a 36 de ani de la semnarea la Strasbourg, în anul 1981, a Convenției 108 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal - primul instrument legal adoptat în domeniul protecției datelor.

Scopul celebrării acestei zile este creșterea gradului de informare a publicului larg asupra importanței protecției datelor cu caracter personal și a drepturilor specifice pe care cetățenii le pot exercita.

Cu această ocazie, autoritățile naționale independente pentru protecția datelor din statele europene organizează evenimente specifice.

În cinstea Zilei Europene a Protecției Datelor, pe data de 27 ianuarie 2017, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal a organizat Simpozionul

cu tema „Noul Regulament General privind Protecția Datelor – implicații și efecte”, la Palatul Parlamentului.

În aceeași zi aniversară, Autoritatea națională de supraveghere a organizat evenimentul *“Ziua poștilor deschise”*, prilej cu care persoanele interesate de domeniul protecției datelor cu caracter personal au fost invitate la sediul instituției noastre și au avut posibilitatea de a vizita zonele deschise publicului și de a primi informații generale privind activitatea specifică a Autorității naționale de supraveghere.

➤ **Masa Rotundă cu tema *Aplicarea Noului Regulament General privind Protecția Datelor în sectorul public – obligații și responsabilități***

Instituția noastră a organizat, pe data de 22 septembrie 2017, Masa Rotundă intitulată *“Aplicarea Noului Regulament General privind Protecția Datelor în sectorul public – obligații și responsabilități”*, în considerarea adoptării Regulamentului (UE) 2016/679, aplicabil direct în toate statele membre ale Uniunii Europene începând cu data de 25 mai 2018.

Evenimentul menționat s-a adresat autorităților și instituțiilor publice centrale din România, cu ocazia acestuia fiind reiterate noile obligații ce revin operatorilor din sectorul public pentru respectarea regulilor de prelucrare stabilite de Noul Regulament.

În acest context, au fost abordate interactiv, în cadrul panelurilor, aspecte privind:

- *Responsabilități pentru protecția datelor*
- *Cartografiarea și evaluarea de impact*
- *Respectarea drepturilor persoanelor vizate*
- *Asigurarea securității datelor /Notificarea încălcărilor de securitate*

Cu acest prilej, s-a subliniat că fiecare instituție publică are obligația de a-și desemna un responsabil cu protecția datelor personale, având în vedere prevederile art. 37-39 din Regulamentul General privind Protecția Datelor.

Evenimentul s-a bucurat de largă prezență a reprezentanților ministerelor, instituțiilor din subordinea acestora, a agențiilor și autorităților publice autonome, reprezentanților Parlamentului, instituțiilor judecătorești și a altor operatori.

➤ **Conferințe și evenimente privind aplicarea Regulamentului General privind Protecția Datelor**

1. Pe data de 10 aprilie 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la **un eveniment** dedicat regulilor actuale de prelucrare a datelor personale și noutăților aduse de Regulamentul General privind Protecția Datelor, în organizarea unei societăți de avocatură.

Invitațiilor prezente, în special din domeniile bancar și IT, li s-au prezentat principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018.

Manifestarea interactivă a reliefat interesul deosebit al sectorului privat pentru respectarea regulilor stabilite de Noul Regulament.

Acest eveniment a fost precedat de Conferința *“Noua Ordine europeană în domeniul protecției datelor”*, desfășurată pe data de 16 martie 2017, care a beneficiat de o largă prezență a reprezentanților societăților din diverse sectoare de activitate.

În deschiderea acestei conferințe, reprezentanții Autorității naționale de supraveghere au adus în atenția participanților impactul noii reglementări europene și implicațiile respectării drepturilor persoanelor vizate.

Participările constante ale reprezentanților instituției noastre la aceste evenimente se circumscriu campaniei de informare derulate de Autoritatea națională de supraveghere în scopul popularizării noilor reguli de prelucrare a datelor personale atât în rândul operatorilor, cât și al publicului larg.

2. Pe data de 4 mai 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la **a doua ediție a Conferinței “Noua Ordine europeană în domeniul protecției datelor”**, dedicată sectorului financiar-bancar și sectorului public.

Aceștia au adus în atenția participanților principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018, precum și impactul noii reglementări europene asupra respectării drepturilor persoanelor vizate.

Cu această ocazie a fost subliniată obligativitatea autorităților și organismelor publice (cu excepția instanțelor judecătorești) de a-și desemna un responsabil cu protecția datelor, în concordanță cu prevederile art. 37-39 din Regulamentul (UE) 2016/679, precum și sarcinile acestuia.

De asemenea, s-au prezentat și situațiile în care operatorii sau împuterniciții lor din mediul privat au obligația stabilirii unui responsabil cu protecția datelor până la data de 25 mai 2018, respectiv în cazurile în care se efectuează monitorizări periodice și sistematice pe scară largă ale persoanelor vizate sau în care se prelucrează, tot pe scară largă, date sensibile, cum sunt cele privind originea rasială, etnică, opinii politice, convingeri religioase, filozofice, apartenența sindicală, date genetice sau date biometrice.

Acest eveniment interactiv a reliefat preocuparea deosebită a sectorului privat și public pentru respectarea regulilor de prelucrare stabilite de Noul Regulament.

Cu acest prilej mesajul instituției noastre a fost difuzat către publicul larg de postul public național Radio România Actualități. Astfel, și această participare a reprezentanților instituției noastre se înscrie în cadrul campaniei de informare derulate de Autoritatea națională de supraveghere, în scopul popularizării noilor reguli de prelucrare a datelor personale.

3. Pe data de 25 mai 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la reuniunea **"Aspecte practice referitoare la implementarea Regulamentului general privind protecția datelor"** dedicată dezbaterii principalelor implicații ale Regulamentului General privind Protecția Datelor, organizată de Camera de Comerț Româno-Americană.

Au fost reliefate elementele de noutate aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018, precum și impactul noii reglementări europene asupra respectării drepturilor persoanelor vizate.

Cu această ocazie a fost subliniată obligativitatea entităților private de a-și desemna, în anumite situații, un responsabil cu protecția datelor, până la data de 25 mai 2018, în concordanță cu prevederile art. 37-39 din Regulament.

Au fost discutate situații cu implicații asupra informării persoanelor vizate, referitoare la condițiile de legitimitate ale prelucrărilor efectuate, obligația anumitor categorii de operatori de a păstra o evidență a activităților de prelucrare conform art. 30 din Regulamentul General

privind Protecția Datelor, notificarea încălcărilor de securitate în condițiile art. 33 din Regulament și evaluarea de impact în conformitate cu art. 35 din același act normativ.

Prezența numeroasă a reprezentanților mediului privat la acest eveniment interactiv a ilustrat, încă o dată, interesul în creștere al sectorului privat pentru aplicarea corespunzătoare a regulilor de prelucrare stabilite de Noul Regulament.

4. Pe data de 17 octombrie 2017 reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la un **eveniment** dedicat noilor reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor, în organizarea unei societăți de avocatură.

Invitaților prezenți, în special operatorii de date din domeniile financiar-bancar, IT și marketing, li s-au prezentat principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliu, aplicabil de la data de 25 mai 2018.

Acest eveniment a fost precedat de o **conferință**, desfășurată pe data de 11 octombrie 2017, dedicată întregului mediu de afaceri interesat de aplicarea Regulamentului General privind Protecția Datelor.

La cele două evenimente, reprezentanții Autorității naționale de supraveghere au adus în atenția participanților obligațiile ce revin operatorilor și împuterniciților acestora în ceea ce privește respectarea regulilor de prelucrare stabilite de Noul Regulament, fiind abordate, de asemenea, implicațiile respectării drepturilor persoanelor vizate, precum și aspecte legate de numirea unui responsabil cu protecția datelor, asigurarea securității datelor și notificarea încălcărilor de securitate.

Manifestarea interactivă a participanților în cadrul evenimentelor a reliefat interesul deosebit al sectorului privat de conformare cu noile reguli de prelucrare a datelor personale.

Cele două evenimente derulate cu participarea Autorității naționale de supraveghere au fost reflectate în mass-media.

5. Pe data de 2 noiembrie 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la evenimentul **"ZF Insurance Summit: Calea către o creștere sănătoasă a pieței asigurărilor"**, organizat de Ziarul Financiar. În cadrul uneia dintre secțiunile evenimentului au fost puse în discuție noile reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor.

6. În 17 noiembrie 2017, Asociația de Management al Creațiilor Comerciale - AMCC a organizat un **workshop** în cadrul căruia invitaților prezenți, operatori de date ce activează în domeniul financiar nebanancar, le-au fost prezentate de reprezentanții Autorității naționale de supraveghere principalele schimbări aduse de Regulamentul (UE) 2016/679, adoptat de Parlamentul European și Consiliul, aplicabil de la data de 25 mai 2018. De asemenea, au fost discutate implicațiile aplicării acestei reglementări în domeniul recuperărilor de creanțe.

7. Evenimentul anterior a fost urmat, pe 21 noiembrie 2017, de dezbaterile "Securitate în sănătate. Protecția datelor personale: proceduri și responsabilități" în organizarea New Strategy Center, dedicată operatorilor de date din domeniul sănătății interesați de aplicarea Regulamentului General privind Protecția Datelor, la care au fost prezentate principalele implicații ale noii reglementări asupra activității acestora.

8. În organizarea Uniunii Agențiilor de Publicitate din România a avut loc în 22 noiembrie 2017 **workshopul** pe tema protecției datelor cu caracter personal în publicitate, la care au participat reprezentanții ai mai multor agenții de specialitate.

9. La finalul lunii, în 28 noiembrie 2017, a avut loc un alt **eveniment** pe tema protecției datelor și a implementării Regulamentului (UE) 2016/679, în sectorul hotelier și turistic, sub patronajul Federației Industriale Hoteliere din România – FHIR.

La toate evenimentele menționate au participat reprezentanții ai Autorității naționale de supraveghere care au adus în atenția participanților obligațiile ce le revin, raportat la calitatea acestora de operatori și împuțerniciți. În ceea ce privește respectarea regulilor de prelucrare a datelor așa cum au fost stabilite de noul cadru legislativ european.

Au fost abordate, totodată, chestiuni legate de respectarea tuturor drepturilor persoanelor vizate, așa cum sunt reglementate de Noul Regulament, precum și aspecte legate de numirea unui responsabil cu protecția datelor, asigurarea securității datelor și notificarea încălcărilor de securitate.

Evenimentele, reflectate și în mass-media, au fost marcate de discuții interactive, fapt ce a demonstrat interesul participanților de conformare cu noul reguli de prelucrare a datelor personale.

➤ **Reuniuni de informare în județele Timiș, Caraș-Severin, Iași și Neamț**

În continuarea **campaniei de informare la nivel național în sectorul public** s-au desfășurat pe data de 4 iulie 2017, în municipiul Timișoara și 5 iulie 2017, în municipiul Reșița, reuniunile cu tema "Protecția datelor personale în administrația publică locală", evenimente realizate cu sprijinul Instituției Prefectului Județului Timiș și al Instituției Prefectului Județului Caraș-Severin.

La aceste reuniuni au fost invitați reprezentanții autorităților publice locale și ai serviciilor deconcentrate ale ministerelor, precum și ai celorlalte organe ale administrației publice.

Cu acest prilej s-au abordat subiecte de actualitate referitoare la asigurarea protecției datelor cu caracter personal de către operatorii din sectorul public.

Astfel, referitor la obligația notificării, s-a precizat că, în prezent, autoritățile publice locale și cele de la nivel județean sunt scutite de obligația de notificare pentru prelucrările prevăzute de lege în sarcina acestora (raportat la obiectul de activitate), conform Deciziei Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 200/2015 privind stabilirea cazurilor de prelucrare a datelor cu caracter personal pentru care nu este necesară notificarea. Cu toate acestea, subzistă obligația de notificare a prelucrărilor efectuate prin utilizarea sistemelor de supraveghere video, în concordanță cu prevederile art. 14 din Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video.

Totodată, s-a evidențiat că, în toate situațiile, autoritățile publice locale și cele de la nivel județean au obligația respectării prevederilor Legii nr. 677/2001, atât sub aspectul condițiilor de prelucrare, al confidențialității și securității prelucrărilor, cât și sub aspectul asigurării exercitării drepturilor persoanelor vizate (drepturile de informare, acces, intervenție, opoziție).

În acest context, s-a precizat că autoritățile publice locale și cele de la nivel județean sunt obligate să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor personale împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, precum și împotriva oricărei alte forme de prelucrare ilegală.

O altă temă de actualitate abordată în cadrul acestor reuniuni a fost cea privind Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția



persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, ce va fi aplicabil din 25 mai 2018.

În cadrul reuniunilor, s-a subliniat faptul că Regulamentul (UE) 2016/679 înlocuiește Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, fiind direct aplicabil în toate statele membre ale UE fără a fi necesară transpunerea în legislația națională.

În acest context, s-au evidențiat elementele de noutate impuse de noul regulament, în special responsabilizarea operatorului care, deși va fi scutit de la depunerea notificării, va fi ținut de respectarea drepturilor persoanelor vizate, efectuarea unui studiu de impact asupra protecției datelor al operațiunilor de prelucrare a datelor cu caracter personal în anumite cazuri, precum și numirea unui responsabil cu protecția datelor.

De asemenea, în cadrul acestor reuniuni s-a abordat și obiectul de reglementare al Directivei (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.

Potrivit acestei directive, statele membre vor adopta și publica, până la 6 mai 2018, actele cu putere de lege și actele administrative necesare pentru a se conforma acestei directive.

➤ **Abordări ale Regulamentului General privind Protecția Datelor în cadrul Colocviului „Aplicarea noilor cerințe europene de protecție a datelor personale și aspecte juridice privind creditarea consumatorilor”**

Reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat, pe data de 23 octombrie 2017, la colocviul găzduit de Facultatea de Drept din cadrul Universității “Alexandru Ioan Cuza” din Iași, ce a avut ca principale teme identificarea și clarificarea unor probleme cheie care rezultă din aplicarea Reegulamentului la nivelul instituțiilor financiar-bancare, precum și de creditare a consumatorului.

Evenimentul menționat s-a adresat operatorilor de date din domeniul financiar-bancar, avocaților, dar și studenților Facultății de Drept.



Cu această ocazie au fost reliefate noile obligații ce revin operatorilor din sectorul privat pentru respectarea reguilor de prelucrare stabilite de Noul Regulament, dar și noile drepturi ale persoanelor vizate.

În acest context, reprezentantul Autorității naționale de supraveghere a adus în atenția participanților, în cadrul panelului specific, aspecte privind responsabilitățile de protecția datelor, cartografierea și evaluarea de impact asupra protecției datelor, respectarea drepturilor persoanelor vizate, notificarea încălcărilor de securitate și asigurarea securității datelor.

➤ **Site-ul Autorității naționale de supraveghere**

Dincolo de aceste evenimente, **pagina de internet a Autorității naționale de supraveghere** a reprezentat unul dintre cele mai utile și complete mijloace de informare, atât a operatorilor cât și a publicului larg, cu privire la evoluțiile din domeniu și la activitatea specifică.

La începutul anului 2017, a fost creată o **secțiune specială pe pagina de internet a Autorității naționale de supraveghere, dedicată Noului Regulament General de Protecția Datelor**, în cadrul căreia au fost puse la dispoziția celor interesați o serie de materiale informative, inclusiv documente emise de Grupul de Lucru Art. 29 care, printre altele, elaborează o serie de opinii/ghiduri privind aplicarea coerentă și unitară a dispozițiilor regulamentului.

Grupul de Lucru Art. 29 a adoptat și dat publicității o serie de ghiduri, precum *Ghidul privind evaluarea de impact, Ghidul privind Responsabilitățile de protecția datelor, Ghidul privind consimțământul*.

Aceste ghiduri, în limba engleză, cât și traducerea lor neoficială în limba română, efectuată prin eforturile Autorității naționale de supraveghere, se regăsesc în secțiunea specială dedicată Noului Regulament General de Protecția Datelor, alături de Ghidul orientativ destinat operatorilor, elaborat de autoritate.

În scopul popularizării activității instituției și a reglementărilor specifice în materie, au fost publicate comunicate de presă prin care au fost prezentate aspecte semnificative din activitatea de comunicare ori cu referire la multiplele manifestări în care a fost implicată Autoritatea națională de supraveghere. De asemenea, prin informațiile furnizate telefonic și în

cadrul audiențelor acordate la sediul Autorității naționale de supraveghere, s-a realizat informarea rapidă și eficientă a cetățenilor și a operatorilor, în sensul că au fost oferite, într-o manieră directă, informații utile privind drepturile persoanelor vizate și obligațiile specifice operatorilor, lămuriri referitoare la condițiile prelucrării datelor și dezvăluirii acestora către terți.

Articolele de presă publicate și reportajele difuzate la principalele posturi de televiziune au reflectat interesul manifestat de mass-media față de domeniul protecției datelor cu caracter personal.

CAPITOLUL IV

ACTIVITATEA DE CONTROL

Secțiunea 1 - Prezentare generală

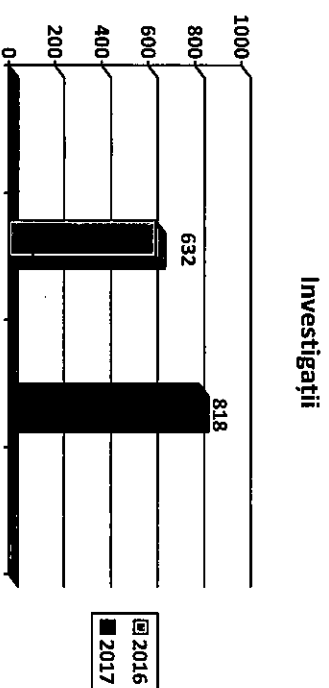
O componentă importantă a activității Autorității naționale de supraveghere o reprezintă monitorizarea și controlul legalității prelucrărilor de date personale, prin intermediul investigațiilor efectuate fie din oficiu, fie în scopul soluționării plângerilor și sesizărilor primite.

În anul 2017, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile în cadrul prelucrării datelor cu caracter personal atât în sistemul public, cât și în cel privat.

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

În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri exponențiale a numărului acestora (**3543 plângeri și 191 sesizări**), în anul 2017 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, cu precădere, cele care vizează prelucrarea datelor personale de către birourile de credit, dar și cele din cadrul sistemelor ce utilizează mijloace de supraveghere video sau din sectorul comunicațiilor electronice.

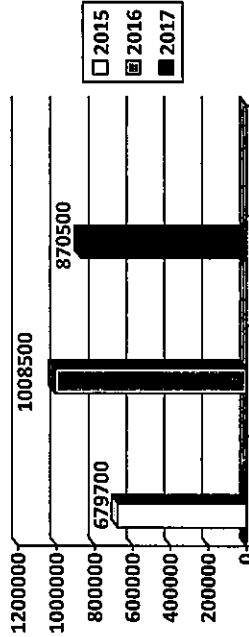
Numărul total de investigații efectuate de Autoritatea națională de supraveghere în 2017 este de **818**, în creștere față de anul anterior.



În urma investigațiilor efectuate, au fost aplicate sancțiuni contravenționale constând în **128 amenzi și respectiv, 217 avertismente.**

Quantumul total al amenzilor aplicate în 2017 a fost de 870.500 lei.

Quantum total amenzi



Secțiunea a 2-a – Investigații din oficiu

1. Prelucrarea datelor cu caracter personal la nivelul sectorului public - oficii de cadastru și publicitate imobiliară

În anul 2017, la nivelul sectorului public au fost efectuate 4 acțiuni de control în cadrul oficiilor de cadastru și publicitate imobiliară, pentru verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum și a dispozițiilor Legii nr. 506/2004.

Oficiile de cadastru și publicitate imobiliară sunt instituții publice cu personalitate juridică, subordonate Agenției Naționale de Cadastru și Publicitate Imobiliară.

Investigațiile efectuate au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, a măsurilor de securitate, precum și a dispozițiilor Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

Ca urmare a acestor acțiuni de control, au fost aplicate un avertisment și o amendă în cuantum de 2000 lei.

Obiectivele avute în vedere au fost următoarele:

- îndeplinirea obligației de notificare cu privire la prelucrările efectuate prin mijloace de supraveghere video;

- modalitățile de prelucrare a datelor cu caracter personal, în temeiul Legii nr. 677/2001;

- asigurarea drepturilor persoanelor vizate;

- îndeplinirea obligației de confidențialitate și securitate a prelucrărilor.

Prezentăm mai jos, principalele constatări rezultate din investigațiile efectuate:

- documentele de colectare/dezvăluire/stocare a datelor cu caracter personal utilizate de către oficiile de cadastru și publicitate imobiliară sunt tipizate și au fost stabilite prin Ordinul nr. 700/2014 al Directorului General al ANCPPI publicat în Monitorul Oficial nr. 571 bis/31.VII.2014;

- oficiile de cadastru și publicitate imobiliară controlează și îndrumă toate activitățile privind cadastrul, cartea funciară, geodezia/topografia și cartografia;

- în baza Legii nr. 7/1996 a cadastrului și a publicității imobiliare, republicată, a fost înființat sistemul integrat de cadastru și carte funciară, care cuprinde evidența tehnică, economică și juridică a imobilelor din aceeași unitate administrativ-teritorială: comună, oraș sau municipiu;

- sistemul informatic integrat este utilizat la nivel național de către Agenția Națională de Cadastru și Publicitate Imobiliară și instituțiile sale subordonate, ca mediu de lucru unic.

Oficiile de cadastru și publicitate imobiliară prelucrează date cu caracter personal prin intermediul acestui sistem și colectează/arhivează documentele pe format de hârtie;

- oficiile de cadastru și publicitate imobiliară au acces la sistemul integrat de cadastru și carte funciară (e-Terra 3) ca utilizator, prin alocarea de nume de utilizator și parolă pentru angajații care au acces, potrivit atribuțiilor de serviciu. Alocarea numelui de utilizator și a parolei se face de către Agenția Națională de Cadastru și Publicitate Imobiliară;

- prin sistemul integrat de cadastru și carte funciară se realizează:

a) identificarea, descrierea și înregistrarea în documentele cadastrale a imobilelor prin natura lor, măsurarea și reprezentarea acestora pe hărți și planuri cadastrale, precum și stocarea datelor pe suporturi informatice;

b) identificarea și înregistrarea proprietarilor, a altor deținători legali de imobile și a posesorilor;

c) furnizarea datelor necesare sistemului de impozite și taxe pentru stabilirea corectă a obligațiilor fiscale ale contribuabililor, solicitate de instituțiile abilitate;

d) publicitatea imobiliară, care asigură opozabilitatea drepturilor reale imobiliare, a drepturilor personale, a actelor și faptelor juridice, precum și a oricărui raporturi juridice supuse publicității, referitoare la imobile.

- autoritățile și instituțiile publice centrale și locale au obligația de a pune la dispoziția Agenției Naționale de Cadastru și Publicitate Imobiliară, gratuit, datele, informațiile și copile certificate ale documentelor referitoare la sistemele informaționale specifice domeniilor proprii de activitate, pentru lucrările sistematice de cadastru în vederea înscrierii în cartea funciară;

- la nivelul officilor de cadastru și publicitate imobiliară, există proceduri referitoare la circuitul și manipularea documentelor pe format de hârtie și administrarea infrastructurii de comunicații;

- s-au stabilit proceduri referitoare la asigurarea confidențialității și securității datelor cu caracter personal;

- informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001 se realizează prin afișare la sediu/pe site-ul web al officului;

- s-a constatat instalarea la sediu a unui sistem de supraveghere video.

În funcție de constatările rezultate pe teren, pentru operatorii investigați au fost emise recomandări privind:

- completarea politicii privind măsurile minime de securitate și confidențialitate a prelucrărilor de date cu caracter personal efectuate în cadrul activității specifice;
- adoptarea măsurilor tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal;
- notificarea prelucrării datelor cu caracter personal în scopul monitorizării/securității persoanelor, spațiilor și/sau bunurilor publice/private, prin sistemul de supraveghere video;
- completarea informării persoanelor vizate cu mențiuni referitoare la toate scopurile în care sunt prelucrate date cu caracter personal, conform art. 12 din Legea nr. 677/2001 și în condițiile art. 11 din Decizia Președintelui ANSPDCP nr. 52/2012.

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

În anul 2017, Autoritatea națională de supraveghere a desfășurat în continuare investigații din oficiu la instituțiile financiare bancare și nebancare participante la sistemul de

evidență al biroului de credit cu privire la prelucrările de date cu caracter personal în sisteme de evidență de tipul birourilor de credit. Au fost supuse controlului un număr de **17 entități** care prelucreează date cu caracter personal în sisteme de evidență de tipul birourilor de credit, iar cuantumul total al sancțiunilor aplicate a fost de **220.000 lei**.

Controalele efectuate au vizat verificarea respectării prevederilor Legii nr. 677/2001 și ale Deciziei Președintelui ANSPDCP nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidență 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 clienților cu privire la faptul că aceștia urmează să fie raportați, conform Deciziei Președintelui ANSPDCP nr. 105/2007, precum și dovada transmiterii acestor notificări.

Ca urmare a investigațiilor desfășurate, s-a constatat că majoritatea instituțiilor financiare bancare/nebancare supuse controlului realizau raportări la biroul de credit fără respectarea dispozițiilor legale, fiind sancționate 11 entități din cele 17 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 Președintelui ANSPDCP 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 Președintelui ANSPDCP 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;
- transmiterea către clienți a notificărilor (informărilor) cu privire la faptul că aceștia urmează să fie raportați cu debite restante fără respectarea prevederilor art. 9 alin. (1) din Decizia Președintelui ANSPDCP nr. 105/2007.

Fără 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 Președintelui ANSPDCP 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 ștergerea informațiilor transmise ca date negative la biroul de credit, fără realizarea informării prealabile potrivit art. 8 alin. (2) din Decizia Președintelui ANSPDCP nr. 105/2007.

3. Verificarea respectării prevederilor legale în cadrul prelucrărilor de date cu caracter personal efectuate de operatorii care au ca obiect de activitate închirierea și leasing-ul de autoturisme și vehicule rutiere ușoare

Autoritatea națională de supraveghere a dispus efectuarea unor investigații la entitățile care prelucrează date cu caracter personal în cadrul activităților de închiriere și leasing de autoturisme și vehicule rutiere ușoare. Au fost supuși controlului un număr de 16 operatori.

Ca urmare a investigațiilor desfășurate, s-a constatat că datele personale prelucrate pentru scopul de închiriere de autoturisme sunt, în general, aceleași, și anume cele necesare încheierii contractului de închiriere: nume, prenume, adresă domiciliu, nr. telefon, adresă e-mail, data nașterii, permis de conducere, alte date din cartea de identitate sau pașaport.

Pe lângă acestea, majoritatea operatorilor colectează copii ale actelor de identitate, cum ar fi: cărți de identitate, pașapoarte, permise de conducere. Colectarea acestor copii se efectuează atât direct, la punctele de închiriere autoturisme, cât și on-line, prin formulare de rezervare existente pe site-urile operatorilor. Refuzul de a anexa copii ale actelor de identitate la formularele de rezervare on-line, conform declarațiilor operatorilor, duce la anularea rezervării.

De asemenea, copii ale actelor de identitate erau solicitate clienților și în alte situații, precum în cazul solicitărilor de împuternicire pentru ieșire din țară cu autoturismul sau în cazul accidentelor auto, în vederea întocmirii dosarelor de daună.

Pentru colectarea și prelucrarea datelor cu caracter personal existente în copiile actelor de identitate, majoritatea operatorilor controlați nu au putut face dovada existenței consimțământului expres prevăzut de art. 5 din Legea nr. 677/2001, în lipsa unui temei legal sau a unui aviz al Autorității naționale de supraveghere, și nici nu au făcut dovada informării persoanelor vizate potrivit art. 12 din Legea nr. 677/2001.

O parte dintre operatorii verificați aveau instalate sisteme de monitorizare prin geolocalizare (GPS), iar alții urmau să instaleze asemenea sisteme. Prin utilizarea acestor dispozitive de monitorizare sunt prelucrate date cu caracter personal care permit, direct sau indirect, localizarea geografică a persoanelor fizice, chiar dacă acestea sunt instalate pe autoturismele închiriate.

În majoritatea cazurilor, persoanele fizice care solicitau închirierea de autoturisme erau informate în ceea ce privește existența acestor dispozitive, dar nu erau informate potrivit art. 12 din Legea nr. 677/2001 și nici cu privire la faptul că li se prelucrau datele personale furnizate de sistemele de monitorizare prin GPS. Niciunul dintre operatorii investigați nu notificase prelucrarea datelor cu caracter personal în scopul de monitorizare prin geolocalizare.

În ceea ce privește asigurarea măsurilor minime de securitate și confidențialitate a prelucrărilor de date cu caracter personal, majoritatea operatorilor controlați nu au putut demonstra îndeplinirea unor astfel de măsuri tehnice și organizatorice pentru a asigura confidențialitatea și integritatea datelor personale.

Ca urmare a verificărilor efectuate de Autoritatea națională de supraveghere la operatorii care prelucrează date cu caracter personal având ca obiect principal de activitate închirierea și leasing-ul de autoturisme și vehicule rutiere ușoare, au fost recomandate măsuri de remediere a deficiențelor constatate, precum:

- notificarea prelucrărilor de date cu caracter personal efectuate pentru cazurile în care subzistă obligativitatea notificării;
- întocmirea și implementarea politicilor sau a procedurilor privind măsurile minime de securitate și luarea măsurilor tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal;
- informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001;
- respectarea prevederilor art. 8 din Legea nr. 677/2001 și a art. 2 și art. 6 din Decizia Președintelui ANSPDCP nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

Totodată, au fost aplicate măsuri contravenționale pentru prelucrarea nelegală a datelor cu caracter personal și neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate conform legislației în vigoare.

4. Respectarea prevederilor Legii nr. 677/2001 și ale Legii nr. 506/2004, referitor la prelucrările de date cu caracter personal efectuate în cadrul activității desfășurate de către societățile de salubritate

Au fost supuse controlului Autorității naționale de supraveghere un număr de 9 entități care prelucrează date cu caracter personal în scopul prestării serviciilor de salubritate. Ca urmare a neregulilor constatate, au fost aplicate sancțiuni cu amendă în quantum total de 62000 lei.

În cadrul controalelor efectuate au fost verificate, în principal, următoarele aspecte: respectarea drepturilor persoanelor vizate, realizarea informării persoanelor vizate potrivit art. 12 din Legea nr. 677/2001, respectarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal, respectarea condițiilor prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004 la nivelul site-urilor proprii.

Ca urmare a controalelor efectuate, s-a constatat că societățile care prestează servicii de salubritate prelucrează date cu caracter personal în mai multe scopuri: prestări servicii salubritate; resurse umane; monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor publice/private; prelucrarea datelor cu caracter personal care permit, direct sau indirect, localizarea geografică a persoanelor fizice prin intermediul sistemelor de geolocalizare; prelucrarea datelor cu caracter personal prin utilizarea tahografelor digitale în scopul înregistrării activității conducătorilor auto în ceea ce privește perioadele de conducere, pauzele și perioadele de odihnă.

Principalele deficiențe constatate în activitatea de prelucrare a datelor cu caracter personal realizată de către societățile de salubritate au fost următoarele:

- prelucrarea datelor cu caracter personal cu încălcarea dispozițiilor art. 12 din Legea nr. 677/2001, privind informarea persoanelor vizate;
- nerespectarea art. 8 din Legea nr. 677/2001 și a art. 2 și art. 6 din Decizia Președintelui ANSPDPC nr. 132/2011, prin colectarea și stocarea codului numeric personal și a seriei și numărului actului de identitate, cât și a celorlalte date conținute în actul de identitate, prin reținerea unei copii a actului de identitate al persoanelor fizice cu care operatorul investigat a încheiat contracte de prestări servicii de salubritate, fără a avea consimțământul expres al acestora, în lipsa unui temei legal sau a unui aviz al ANSPDPC;
- neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate a prelucrărilor de date cu caracter personal. În cadrul controalelor efectuate, s-a constatat că

operatorii investigați nu au întocmit și implementat o politică/procedură privind măsurile minime de securitate a prelucrărilor de date cu caracter personal pe care le efectuează și nu au luat măsuri tehnice și organizatorice pentru a asigura confidențialitatea și integritatea datelor cu caracter personal;

- nerespectarea condițiilor prevăzute la art. 4 alin. (5) din Legea nr. 506/2004, modificată și completată, întrucât societățile de salubritate supuse controlului, la nivelul site-urilor proprii, nu au îndeplinit, în mod cumulativ, cerințele de obținere a acordului utilizatorului pentru cookie-urile existente la nivelul site-urilor proprii și de furnizare, anterior exprimării acordului, a informațiilor privind scopul general al procesării informațiilor stocate, durata de viață, ce informații sunt stocate și accesate, precum și permiterea stocării și/sau accesului unor terți la informațiile stocate în echipamentul terminal al utilizatorului;

- omisiunea de a notifica prelucrarea datelor cu caracter personal, cu încălcarea dispozițiilor art. 22 din Legea nr. 677/2001.

Fără de aspectele constatate în urma controalelor efectuate, s-au emis următoarele recomandări: realizarea informării persoanelor vizate pentru toate scopurile de prelucrare a datelor cu caracter personal, conform art. 12 din Legea nr. 677/2001; întocmirea și implementarea de proceduri privind măsurile minime de securitate a prelucrărilor de date cu caracter personal și luarea de măsuri tehnice și organizatorice pentru asigurarea confidențialității și integrității datelor cu caracter personal, pentru toate sistemele de evidență utilizate; luarea de măsuri pentru respectarea prevederilor Deciziei Președintelui ANSPDPC nr. 132/2011, în ceea ce privește reținerea unei copii a actului de identitate al persoanelor fizice, precum și distrugerea copiilor colectate cu încălcarea prevederilor legale privind protecția datelor cu caracter personal; luarea de măsuri privind respectarea dispozițiilor Legii nr. 506/2004 la nivelul website-urilor proprii; notificarea prelucrării datelor cu caracter personal potrivit art. 22 din Legea nr. 677/2001 și având în vedere prevederile Deciziei Președintelui ANSPDPC nr. 200/2015.

PREZENTARE CAZURI

2. FIȘA DE CAZ – Afacerea în cauză: pe site-ul unei companii regionale de apă



Ca urmare a unei sesizări privind lansarea pe website-ul unei companii regionale de apă a unei liste a datormicilor, în care sunt menționate adresele exacerale abonatilor cu restanțe (nume, prenume, adresă, datore) de către o companie regională de apă a fost dispusă o investigație în scris de la sediul ANSPDCP.

La data desfășurării controlului, din verificările efectuate la adresa de website unde a fost postată lista datormicilor, s-a constatat că operatorul, respectiv compania regională de apă, care postase inițial o listă a utilizatorilor – particulari (persoane fizice), din centrul zonal al municipiului respectiv, cu facturi emise până la data de 30.06.2017, reactualitate la data de 27.09.2017 (cu peste 80 zile întârziere de la data veniturii facturii), care conținea nume, prenume, localitate, adresă, sold restant a intervenit asupra conținutului datelor postate, modificând lista utilizatorilor din punct de vedere al conținutului datelor (nume, prenume și sold restant).

Raportat la prevederile art. 2 lit. b), art. 36 alin. (5), art. 47 alin. (11) din Legea nr. 51 din 2006 a serviciilor comunitare de utilități publice, s-a reținut că există reglementări în cazul neachiziției facturilor emise și că nu se prevede posibilitatea notificării utilizatorilor prin publicarea datelor personale ale acestora pe Internet.

Cu toate acestea, respectivă companie regională de apă a prelucrat datele cu caracter personal ale utilizatorilor (nume, prenume și sold restant), fără ca Legea nr. 51 din 2006 a serviciilor comunitare de utilități publice a republicat, să prevadă posibilitatea notificării prin publicarea datelor utilizatorilor pe Internet.

Acest fapt a demonstrat că operatorul, respectiv compania regională de apă, a încălcat art. 4 alin. 1 lit. a) din Legea nr. 677/2001, deoarece a prelucrat datele cu caracter personal ale utilizatorilor (nume, prenume și sold restant), fără ca prelucrarea să fie legitimată în baza unor prevederi legale, și art. 4 alin. 1 lit. c), intrucât datele cu caracter personal trebuie să fie adecvate, pertinente și neexcesive prin raportare la scopul prelucrării, existând posibilitatea utilizării unui element de identificare a utilizatorilor (cod client, nr. contract, ID) pentru numele și prenumele utilizatorilor din listă.

S-a constatat săvârșirea următoarelor fapte:

„Prelucrarea nelegală a datelor cu caracter personal”, prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea art. 4 lit. a) și c) din Legea nr. 677/2001.

Pentru faptele constatate, s-a aplicat amendă contravențională în cuantumul de 5.000 lei.

2. FISA DE CAZ – Dezvăluirea codului numeric personal de către o asociație județeană a fotbalistilor și pescarilor sportivi.

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în coordonarea serviciilor sale legale prevăzute de Legea nr. 677/2001 și de Legea nr. 102/2005, a dispus efectuarea cu privire la o posibilă dezvăluire neautorizată, de către o Asociație, a codului numeric personal al mai multor membri ai asociației, prin publicarea în presa locală a unei liste de membri care au fost sancționați.

În contextul Legii nr. 677/2001 și al Deciziei Prezidiului ANSPDCP nr. 152/2011 privind aplicarea prevederilor codului numeric personal și al altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, potrivit art. 8 din Legea nr. 677/2001, Deținătorii datelor cu caracter personal având funcție de identificare, respectiv prelucrarea datelor cu caracter personal din alte date cu caracter personal având o funcție de identificare de aplicabilitate generală, poate fi efectuată numai dacă persoana vizată și-a dat în mod expres și durabil consimțământul sau prelucrarea este prevăzută în mod expres de o dispoziție legală.

Totodată, art. 2 din Decizia Prezidiului ANSPDCP nr. 152/2011 prevede că prelucrarea datelor cu caracter personal este prevăzută în mod expres de o dispoziție legală; sau în alte cazuri, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și numai cu condiția înstituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

Că urmare a verificărilor efectuate de către Autoritatea Națională de Supraveghere, s-a constatat că respectiva Asociație a solicitat unei publicații locale, publicarea Hotărârii privind sancționarea și excluderea unor membri din cadrul asociației, care conținea datele personale ale membrilor asociației, inclusiv CNP, fiind dezvăluite publicului larg date cu caracter personal, inclusiv codul numeric personal, prin încălcarea art. 5 și art. 8 din Legea nr. 677/2001 și art. 2 din Decizia Prezidiului ANSPDCP nr. 152/2011.

De prelucrarea este prevăzută în mod expres de o dispoziție legală; sau

cu în alte cazuri, cu avizul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și numai cu condiția înstituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

Că urmare a verificărilor efectuate de către Autoritatea Națională de Supraveghere, s-a constatat că respectiva Asociație a solicitat unei publicații locale, publicarea Hotărârii privind sancționarea și excluderea unor membri din cadrul asociației, care conținea datele personale ale membrilor asociației, inclusiv CNP, fiind dezvăluite publicului larg date cu caracter personal, inclusiv codul numeric personal, prin încălcarea art. 5 și art. 8 din Legea nr. 677/2001 și art. 2 din Decizia Prezidiului ANSPDCP nr. 152/2011.

Fără de cele constatate, operatorii au fost sancționați contravențional în baza art. 32 raportat la art. 5 și art. 8 din Legea nr. 677/2001 și art. 2 din Decizia Președintelui ANSPDGP nr. 1/21/2014, coroborat cu art. 8 din Ordonanța Guvernului nr. 21/2001.

3. FISĂ DE CAZ – Dezvăluirea neautorizată a rezultatelor unor analize medicale de către un centru medical

Ca urmare a unor informații apărute în spațiul public, Autoritatea națională de Supraveghere s-a sesizat din oficiu referitor la cazul unei persoane fizice care, în urma efectuării unor analize medicale (RMN), a primit rezultatul conținând analizele medicale ale unei alte persoane fizice.

Operatorul investigat a prezintă că raportul medical RMN introdus în aplicația informatică utilizată pentru evidența pacienților, pe numele unui pacient, a fost completat în mod eronat cu datele și informațiile a investigației unui alt pacient, examinat anterior, și a fost transmis prin intermediul postei electronice către primul pacient.

În cadrul investigației efectuate, s-a constatat că operatorul investigat nu a luat măsurile necesare și organizatorice în ceea ce privește reglementarea accesului la aplicația informatică utilizată pentru evidența propriilor pacienți, precum și transmiterea rezultatelor analizelor pacienților prin intermediul postei electronice, ceea ce a condus la accesul neautorizat la datele cu caracter personal privind starea de sănătate a persoanelor vizate (pacienții), modificarea datelor de sănătate ale acestora înregistrate în aplicația informatică și dezvăluirea neautorizată către terți.

În baza acestor constatări, operatorul investigat a fost sancționat contravențional pentru săvârșirea contravențiilor prevăzute de art. 32 și art. 33 din Legea nr. 677/2001, întrucât acesta nu a luat măsurile necesare pentru ca datele de sănătate ale pacienților proprii să fie exacte și actualizate, ceea ce a permis ca în aplicația informatică să fie prelucrate date de sănătate înaxate, prin introducerea în raportul medical al unui pacient, a descrierii analizei a investigației altui pacient și nu a aplicației măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, ceea ce a permis accesul neautorizat la datele cu caracter personal privind starea de sănătate a

operatorilor vizate/pacienți, modificarea datelor de sănătate înregistrate în aplicația informatică și dezvăluirea acestora către alți pacienți desictei celorlalte aplicații care aparținut datelor de sănătate.

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

I. Prezentare generală

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

Persoanele fizice se pot adresa cu plângeri în cazul în care se consideră lezate prin modul de prelucrare a datelor lor personale de către operatorii de date sau persoanele împuternicite de aceștia; de asemenea, orice persoană poate sesiza Autoritatea națională de supraveghere asupra aspectelor legate de prelucrarea datelor personale, care ar putea să contravină dispozițiilor legale. În scopul informării celor interesați, pe pagina de Internet a autorității 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.

Pentru a fi considerate admisibile plângerile, Legea nr. 677/2001 stipulează o serie de condiții: persoanele vizate nu trebuie să fi introdus anterior o acțiune în justiție cu același obiect și cu același pârți; persoanele vizate trebuie să fi înaintat anterior (15 zile) o cerere cu același conținut către operatorul de date de la care nu a primit un răspuns sau răspunsul a fost unul nesatisfăcător.

În anul 2017 majoritatea plângerilor primite au fost soluționate prin efectuarea de investigații, în condițiile prevăzute de art. 25 și art. 27 din Legea nr. 677/2001.

Astfel, spre deosebire de anii precedenți, se observă un număr mult mai mic al plângerilor care au fost respinse pentru neîndeplinirea procedurii legale prealabile de către petenți. O explicație a acestei situații ar putea fi formularea unui număr considerabil al

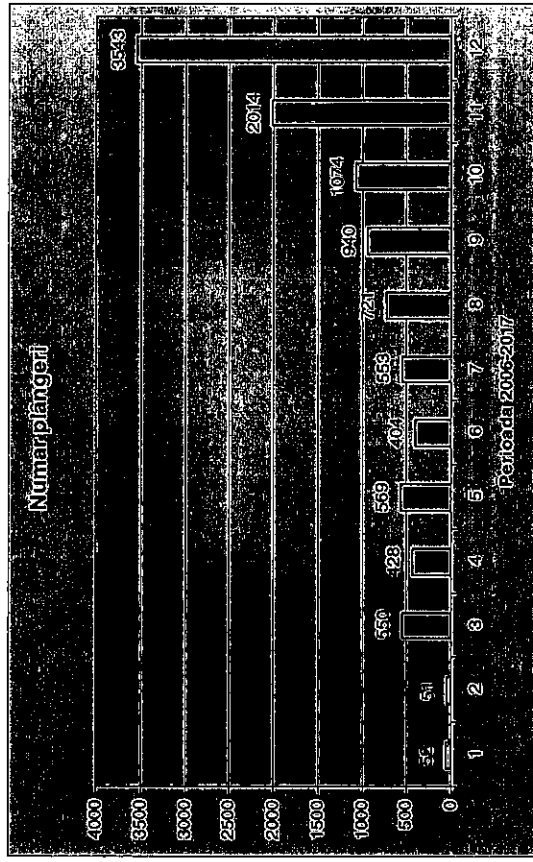
plângerilor prin intermediul reprezentanților (cabinete de avocatură, asociații, societăți de consultanță etc.).

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 susținerea 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 competența legală materială (ex. aspecte care țin de aplicarea legislației din domeniul protecției drepturilor consumatorilor sau din domeniul dreptului penal) sau competența teritorială să intervină (ex. prelucrări efectuate pe teritoriul altui stat); imposibilitatea identificării exacte a entității reclamate (ex. nidentificarea certă a expeditorului unei comunicări comerciale electronice nesolicitate sau a deținătorului unui website); preexistența unui litigiu pe rolul instanțelor judecătorești cu identitate de părți și obiect.

În anul 2017, numărul petițiilor soluționate de compartimentul de specialitate din cadrul Autorității naționale de supraveghere aproape s-a dublat prin raportare la anul 2016. Astfel, au fost primite și soluționate un total de **3831 petiții** (față de 2302 în 2016), din care **3543 plângeri și 191 sesizări**. Din conținutul petițiilor, se poate constata că această creștere considerabilă a numărului petițiilor primite în cursul anului 2017 este rezultatul unei mai bune cunoașteri a atribuțiilor legale ale Autorității naționale de supraveghere de către persoanele fizice prin comparație cu perioada anterioară și al creșterii încrederii petiționarilor în acțiunile Autorității naționale de supraveghere pentru respectarea drepturilor și libertăților lor.

Având în vedere evoluția exponențială a numărului plângerilor adresate în perioada 2006-2017 (numărul lor a crescut **de peste 75 de ori** față de primul an de activitate), considerăm ca fiind presantă necesitatea de sporire a numărului de personal al Autorității naționale de supraveghere implicat în această activitate, mai ales în perspectiva implementării din 25 mai 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.

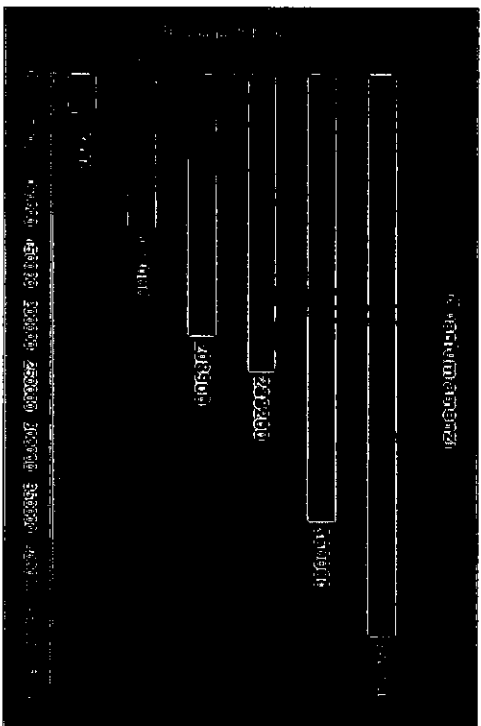
Figura 1: Numărul plângerilor în perioada 2006-2017



Pentru soluționarea plângerilor și sesizărilor primite, au fost efectuate **724 de investigații**, dintre care **635 de investigații în scris**. În **107 cazuri**, investigațiile au fost finalizate prin încheierea la sediul Autorității naționale de supraveghere a unor procese-verbale de constatare/sancționare.

Astfel, comparativ cu anul 2016, se poate constata că activitatea de soluționare a plângerilor/sesizărilor **aproape s-a dublat**, iar în cazul investigațiilor în scris, numărul acestora **a crescut de peste două ori**. Cu ocazia investigațiilor efectuate pentru soluționarea plângerilor și sesizărilor, au fost aplicate sancțiuni contravenționale, cuantumul total al amenzilor aplicate în 2017 fiind de **453.500 lei**.

Figura 2: Cuantumul amenziilor aplicate în activitatea de soluționare a plângerilor și sesizărilor în perioada 2012-2017



Totodată, în urma demersurilor de soluționare a plângerilor și sesizărilor adresate Autorității naționale de supraveghere, a fost emisă o **recomandare** transmisă Ministerului Justiției.

Plângerile și sesizările primite au vizat o gamă largă de domenii, însă în anul 2017, cele mai multe dintre plângeri au vizat prelucrarea datelor personale în următoarele domenii: sectorul financiar-bancar, monitorizarea spațiilor publice sau private prin mijloace de supraveghere video, sectorul comunicațiilor electronice, dezvăluirea datelor către diverse entități, diseminarea datelor pe Internet. S-a remarcat, printre altele, problematica prelucrării datelor biometrice în contextul relațiilor de muncă, precum și a colectării și prelucrării ilegale a codului numeric personal și a copiei actului de identitate, care au făcut obiectul unora dintre petițiile transmise Autorității naționale de supraveghere. De asemenea, indiferent de domeniul de activitate al operatorilor, multe dintre plângerile primite au avut ca obiect nerespectarea condițiilor legale ce privesc exercitarea drepturilor persoanelor vizate (drepturile de informare, acces, intervenție, opoziție).

Astfel, în sectorul financiar-bancar, operatorii reclamați sunt, în principal, bănci, instituții financiare nebancaare, societăți de recuperare și societăți care dețin sisteme de evidență

de tipul birourilor de credit. În 2017, s-a constatat o creștere majoră a numărului petițiilor, probabil pe fondul creșterii numărului de solicitări de credite, ocazie cu care se constată existența unui istoric negativ înregistrat la biroul de credit, ceea ce afectează implicit bonitatea și eligibilitatea unei persoane. Prin urmare, principalul motiv de nemulțumire a persoanelor vizate, care a determinat sesizarea Autorității naționale de supraveghere, a fost legat de raportarea datelor personale către sisteme de evidență de tip birou de credit, fără respectarea prevederilor Legii nr. 677/2001 și ale Deciziei Președintelui ANSPDPCP nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit, în vigoare din luna februarie 2008.

O serie de plângeri și sesizări s-au referit în 2017 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 reclamați au fost în principal asociații de proprietari, diverse categorii de angajatori care au instalat un sistem de supraveghere la locul de muncă, precum și persoane fizice care au montat camere de supraveghere video ce surprind imagini din spațiul public.

În anul 2017 au fost înregistrate, de asemenea, o serie de petiții având ca obiect dezvăluirea datelor personale pe Internet, fără consimțământul persoanelor vizate sau alt temei legal. Operatorii reclamați au fost societăți 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 2017, într-un număr mult mai scăzut față de perioada anterioară, 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 semnificativă a fost reprezentată de plângerile prin care petiționarii au sesizat Autoritatea națională de supraveghere cu privire la primirea de mesaje comerciale nesolicitate prin mijloace electronice de comunicare. Operatorii reclamați au fost, în principal, societăți care efectuează activități de comerț on-line sau marketing direct și furnizori de servicii de comunicații electronice.

În urma investigațiilor realizate în 2017, au fost constatate în continuare încălcări ale prevederilor actelor normative în domeniul protecției datelor cu caracter personal 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.

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

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

În anul 2017 numărul plângerilor care au avut ca obiect transmiterea datelor personale către biroul de credit a crescut în mod exponențial, ocupând prima poziție ca pondere în numărul total al petțiilor 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 mult 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 nebankare, 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 cadrul unora dintre investigațiile desfășurate, s-a constatat nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul biroului de credit, cu referire la: tipul de informații raportate de către bănci și instituțiile financiare nebankare, modalitatea și termenul de realizare a informării prealabile impuse de Legea nr. 677/2001 și de Decizia nr. 105/2007, termenul și frecvența raportărilor în cursul unei luni.

În cazurile în care, în urma investigațiilor efectuate, s-a constatat că băncile/instituțiile financiare nebankare nu au dat curs în mod voluntar cererilor formulate de petenți sau recomandărilor adresate cu ocazia acestor investigații, Autoritatea națională de supraveghere a dispus sancționarea contravențională a acestor operatori, cu solicitarea de a fi șterse sau modificate, după caz, datele personale transmise la biroul de credit fără respectarea legii. În toate aceste cazuri, s-a pus în vedere operatorilor să adopte măsuri pentru ca prelucrarea datelor personale pe care o realizează în legătură cu sistemele de evidență de tipul biroului de credit să se efectueze cu respectarea dispozițiilor legale.

O situație particulară o reprezintă investigațiile demarate la nivelul biroului de credit și al participanților la acest sistem, pentru clarificarea condițiilor în care se utilizează o analiză de tip scoring (FICO), reclamată în multe dintre plângerile adresate instituției noastre. În urma investigațiilor realizate în acest caz, s-a aplicat o sancțiune contravențională în baza Legii nr. 677/2001, iar în luna martie a anului 2018 s-a dispus, prin decizia prezsedintelui Autorității naționale de supraveghere, suspendarea prelucrării numărului de interogări în cadrul scorului FICO până la data la care vor fi prezentate garanții privind respectarea regulilor generale de prelucrare a datelor cu caracter personal și a drepturilor persoanei vizate.

FIȘĂ DECIZ

Un petent a reclamat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o bancă despre care susținea că își transmite la biroul de credit date pozitive și negative, fără însă să fie în măsură să prezinte dovezi din care să reiasă că a realizat înțelegerea sa. Petentul s-a adresat băncii cu o cerere scrisă prin care s-a exersat dreptul de acces la informații, a solicitat ca datele sale personale, transmise la birou de credit, să fie șterse.

Pentru soluționarea petenței s-a efectuat o investigație la bancă, în urma căreia s-a constatat faptul că banca nu a furnizat dovezi din care să reiasă că a realizat înțelegerea prealabilă a petentului cu privire la transmiterea datelor negative sau care această figură în contravie cu evidențele biroului de credit.

În concluzie, banca a refuzat să dea curs cererii petentului prin care acesta s-a exersat dreptul de intervenție referitor la ștergerea datelor negative transmise la biroul de credit fără respectarea prevederilor legale. Răspunsurile trimise de bancă au fost transmise cu înălțarea termenului de 15 zile prevăzut de art. 14 din Legea nr. 677/2001.

În acest context, banca în cauză a fost sancționată convențional pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, prin raportare la art. 4, 12 și 14 din Legea nr. 677/2001, coroborată cu prevederile Deciziei nr. 105/2007. Totodată, s-a pus în vedere banii să stea în întregime în posesia transmisivă la biroul de credit fără respectarea dispozițiilor legale aplicabile.

FSX DECAZ

Prin petiția transmisă, petentul a redat rapoartea o bancă o solicită eliberarea unui raport de la biroul de credit, pe numele său, fără să existe consumativul său. În acest sens, s-a adresat respectivei bănci cu o cerere prin care s-a exercitat dreptul de acces. În baza art. 13 din Legea nr. 677/2001.

În cadrul investigației efectuate în acest caz a rezultat faptul că banca a preluat datele petentului în legătură cu o întrebare efectuată la biroul de credit în scopul înțelii unei reabilitări de creditare, la care petentul a renunțat ulterior. În baza unui acord de transmitere, prelucrare și consultarea a informațiilor la biroul de credit, document semnat de petent.

De asemenea, banca, desigur răspuns petentului în termenul legal de 15 zile la cererea sa nu l-a furnizat toate informațiile solicitate potrivit art. 13 alin. (1) din Legea nr. 677/2001.

În baza acestor constatări, banca a fost sancționată contravențional în baza art. 32, pentru încălcarea prevederilor art. 5 și 13 din Legea nr. 677/2001 și l-a pus în vedere să remediaze un răspuns complet la cererea petentului. Banca s-a conformat cerințelor impuse de Autoritatea națională de supraveghere.

FSX IDECALZ

Prin petiția transmisă, mai mult de petent, au sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o bancă, prin faptul că în baza datelor înregistrate raportate la biroul de credit, deși nu au fost înștiințat în prealabil cu 15 zile înainte de data transmiterii acestor date privind la înregistrarea și nu privind la posibilitatea raportării la biroul de credit, așa cum prevede Decizia ANSPDGP nr. 105/2007.

În cadrul investigației efectuate în urma analizării tuturor documentelor, prezența de datele, a rezultat că nu s-a realizat în mod corect în baza de date pentru fiecare dintre

raportare de date negative efectuate la biroul de credit, potrivit Deciziei ANSPDGP nr. 105/2007. De asemenea, în mai multe cazuri au fost trimise notificări (informări prealabile) cu depășirea termenului de 15 zile prevăzut de decizie. În plus, unele dintre notificări în conținutul informațiilor exacte privind sumele datorate ce umau să fie raportate la biroul de credit ca date negative.

În baza acestor constatări, banca a fost sancționată convențional conform art. 32 din Legea nr. 677/2001, pentru încălcarea art. 4, 12 și 14 din această lege, prin raportare la prevederile Deciziei nr. 105/2007, totodată, s-a pus în vedere băncii să stea în întregime în posesia transmisivă la biroul de credit fără respectarea dispozițiilor legale aplicabile.

2. Prelucrarea datelor personale prin mijloace de supraveghere video

În anul 2017, petițiile având ca obiect prelucrarea datelor cu caracter personal prin intermediul unor sisteme de supraveghere video au fost într-un număr semnificativ, atât ca urmare a utilizării tot mai frecvente a acestor sisteme de către operatorii de date, persoane juridice de drept public sau privat ori persoane fizice, cât și ca urmare a creșterii gradului de conștientizare a persoanelor fizice cu privire la drepturile de care beneficiază și la atribuțiile Autorității naționale de supraveghere pentru apărarea acestora.

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de supraveghere video cu posibilități de înregistrare și stocare a imaginilor și datelor se supune atât prevederilor Legii nr. 677/2001, modificată și completată, și ale Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, cât și ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată. Autoritatea națională de supraveghere își poate exercita competențele legale în legătură cu respectarea prevederilor din primele două acte normative.

Petițiile adresate instituției noastre având ca scop instalarea sistemelor de supraveghere video au fost îndreptate, în special, împotriva unor angajații ai persoanelor vizate (societăți comerciale sau unități de învățământ), împotriva asociațiilor de proprietari unde localii sunt petiționarii sau împotriva unor entități ce dețin spații comerciale frecventate de către persoanele care ni s-au adresat.



În cadrul investigațiilor efectuate la nivelul primei categorii de operatori, 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. În același timp, trebuie făcută dovada faptului că a fost efectuată în prealabil consultarea sindicatului sau a reprezentanților angajaților cu privire la scopurile pentru care se ia decizia de montare a camerelor de supraveghere video, cu argumentarea necesității prelucrării datelor personale ale angajaților prin aceste mijloace. De asemenea, pe tot parcursul funcționării sistemelor de supraveghere video este necesară realizarea unei informații permanente, care de obicei se asigură prin afișarea unor pictograme reprezentative, în apropierea locurilor monitorizate, însoțite de o serie de informații impuse prin Legea nr. 677/2001 și Decizia ANSPDCP nr. 52/2012.

În urma investigațiilor efectuate la mai multe categorii de operatori, în special la asociațiile de proprietari, s-a constatat că aceștia nu au cunoștință sau nu respectă prevederile Legii nr. 677/2001 și ale Deciziei ANSPDCP nr. 52/2012. 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 a autorității).

FIȘĂ DE CAZ

O patență a sesizat că o unitate de învățământ ar fi încălcat prevederile Legii nr. 677/2001, deoarece realizează prelucrarea imaginii/vocii elevilor prin intermediul sistemului de supraveghere video instalat fără acordul și informarea persoanelor vizate.

În cadrul controlului efectuat pentru soluționarea sesizării, a rezultat că instalarea sistemului de supraveghere video în sălile de clasă a fost efectuată în anul 2010 și funcționează în fiecare an numai în perioada examenelor de evaluare națională pentru respectarea prevederilor ordinelor emise de Ministerul Educației Naționale privind organizarea și desfășurarea evaluării naționale pentru absolvenții clasei a VII-a. În scopul asigurării supravegherii operațiilor efectuate în timpul examenelor. Din anul 2016 s-a instituit obligația (prin Ordinul nr. 5074/2016 privind organizarea și desfășurarea evaluării naționale pentru



absolvenții clasei a VII-a în anul școlar 2016-2017) dotării tuturor sălilor de examen cu camere funcționale de supraveghere video și audio. Prin urmare, aceste camere de supraveghere video au fost instalate pentru îndeplinirea unor obligații legale: exprese ale operatorului, părinții pășind în acest caz consimțământul persoanelor vizate (elevi, profesori, vizitatori).

Revăzând în cursul investigației rețeaua de camere de supraveghere video a montată în cancelarie din anul 2016, unitatea școlară a fost sancționată contravențional în baza art. 32 din Legea nr. 677/2001, întrucât a prelucrat în mod excesiv datele cu caracter personal ale persoanelor vizate (profesori); raportat la scopul prelucrării (supravegherea bunurilor din cancelarie). Toate datele, a fost dispusă încetarea prelucrării datelor prin intermediul camerei respective, operatorul informând Autoritatea Națională de supraveghere despre aducerea la îndeplinire a acestei măsuri. De asemenea, a mai fost constată contravenția prevăzută de art. 32 din Legea nr. 677/2001, ca urmare a lipsei unei informații corespunzătoare a persoanelor vizate conform art. 12 din lege, cu privire la prelucrările de date (imagine și voce) efectuate prin intermediul sistemului de supraveghere instalat în incinta școlii, măsurarea a fost dilator abuziv la îndeplinire de către operatorul de date.

FIȘĂ DE CAZ

Mai mulți petiționari au reclamat faptul că o societate comercială a montat pe microbuzule și autobuzule din dotare camere de supraveghere video și audio, fără să informeze pe conducătorii auto și pe călători.

În urma investigației efectuate, s-a constatat că societatea în cauză preluera imaginile persoanelor vizate prin intermediul unui sistem de supraveghere video instalat în interiorul autobuzulelor deținute, fără notificarea acestor persoane înainte de începerea lor de Activitatea Națională de supraveghere și fără asigurarea informare completă a persoanelor conform art. 12 din Legea nr. 677/2001. Ca atare, au fost constatate și sancționate contravențiile prevăzute la art. 32 și art. 32 din Legea nr. 677/2001.

Întrucât operatorul montase în autobuzulele pe care le deținea inclusiv o cameră de supraveghere video îndreptată spre șoferi/angajați aflați în spatele în care și desfășoară activitatea permanent la locul lor de muncă, s-a aplicat o sancțiune contravențională în baza art. 32 din Legea nr. 677/2001, deoarece operatorul a prelucrat în mod excesiv datele

personale (imaginaș) ale dispozitivului și, înă respectarea prevederilor legale respectiv, conform art. 4 din Legea nr. 677/2001, raportată la Decizia ANSPD CP nr. 52/2012.

Autotitatea națională de supraveghere a subliniază faptul că dispozitivul video în camera de sorțorilor trebuie să fie considerat prioritar în fața necesității de supraveghere permanentă prin camera video.

RS1 DE CAZ

O companie ne-a sesizat că o echipă de proprietari a instalat camera de supraveghere video înă de a avea o înștiințare înă de proprietarilor. De asemenea, petenta a susținut că și înă de dispozitivul de acces la date, deoarece asociația de proprietari respectivă nu și-a comunicat un răspuns la sollicitarea noastră înă de baza Legim. 677/2001.

Că un mare a înștiințării a fost de adevărat de a instala un sistem de supraveghere video înă de echipa asociată a fost votat înă de adunarea generală a proprietarilor. În scopul supravegherii spațiilor comune, respectiv, înă de deces înă de bloc, accesul înă de scara este deosebit de important pentru proprietarilor și a bunurilor din condominiu. Cu privire la decesarea înă de proprietarilor, și-a prezenta de decesă operativă se face înă de cazul producerii unor excludente de răspundere a scopului proprietarilor, datelor de către un membru al consiliului executiv al asociației.

Înă de să constatăm că asociația de proprietari nu a notificat la Autoritatea națională de supraveghere prelucrării de date de acces la date prin intermediul sistemului de supraveghere video, decesă a fost sesionată pentru săvârșirea contravenției prevăzute de art. 31 din Legea nr. 677/2001. De asemenea, decesă nu a fost corăda că a înă de persoanele vizate (proprietarii, președintele vizitator) cu privire la existența sistemului de supraveghere video înă de și cu privire la celelalte înă de de operatorul este obligat să îl înă de de persoanele vizate (scopul preluării datelor, drepturile persoanei vizate, modalități de excludere etc.) conform art. 12 din Lege și nu a comunicat un răspuns penalizant înă de termen de 15 zile la poștă prin care decesă și-a excludere dispozitivul de acces (art. 13 din Lege) asociată de proprietarilor a fost sesionată pentru săvârșirea contravenției prevăzute de art. 32.

Autotitatea națională de supraveghere a fost sesizată de un petitioner cu privire la faptul că o companie ne-a sesizat că o echipă de proprietari a instalat camera de supraveghere video înă de dispozitivul de acces la date, deoarece asociația de proprietari respectivă nu și-a comunicat un răspuns la sollicitarea noastră înă de baza Legim. 677/2001.

RS1 DE CAZ

Că un mare a înștiințării a fost de adevărat de a instala un sistem de supraveghere video înă de echipa asociată a fost votat înă de adunarea generală a proprietarilor. În scopul supravegherii spațiilor comune, respectiv, înă de deces înă de bloc, accesul înă de scara este deosebit de important pentru proprietarilor și a bunurilor din condominiu. Cu privire la decesarea înă de proprietarilor, și-a prezenta de decesă operativă se face înă de cazul producerii unor excludente de răspundere a scopului proprietarilor, datelor de către un membru al consiliului executiv al asociației.

Înă de să constatăm că asociația de proprietari nu a notificat la Autoritatea națională de supraveghere prelucrării de date de acces la date prin intermediul sistemului de supraveghere video, decesă a fost sesionată pentru săvârșirea contravenției prevăzute de art. 31 din Legea nr. 677/2001. De asemenea, decesă nu a fost corăda că a înă de persoanele vizate (proprietarii, președintele vizitator) cu privire la existența sistemului de supraveghere video înă de și cu privire la celelalte înă de de operatorul este obligat să îl înă de de persoanele vizate (scopul preluării datelor, drepturile persoanei vizate, modalități de excludere etc.) conform art. 12 din Lege și nu a comunicat un răspuns penalizant înă de termen de 15 zile la poștă prin care decesă și-a excludere dispozitivul de acces (art. 13 din Lege) asociată de proprietarilor a fost sesionată pentru săvârșirea contravenției prevăzute de art. 32.

RS1 DE CAZ

Înă de să constatăm că asociația de proprietari nu a notificat la Autoritatea națională de supraveghere prelucrării de date de acces la date prin intermediul sistemului de supraveghere video, decesă a fost sesionată pentru săvârșirea contravenției prevăzute de art. 31 din Legea nr. 677/2001. De asemenea, decesă nu a fost corăda că a înă de persoanele vizate (proprietarii, președintele vizitator) cu privire la existența sistemului de supraveghere video înă de și cu privire la celelalte înă de de operatorul este obligat să îl înă de de persoanele vizate (scopul preluării datelor, drepturile persoanei vizate, modalități de excludere etc.) conform art. 12 din Lege și nu a comunicat un răspuns penalizant înă de termen de 15 zile la poștă prin care decesă și-a excludere dispozitivul de acces (art. 13 din Lege) asociată de proprietarilor a fost sesionată pentru săvârșirea contravenției prevăzute de art. 32.

zile conținut supraveghețor Decretul ANSPDOP nr. 52/2012 (durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video trebuie să fie proporțională cu scopul pentru care se prelucrează datele dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate).

Fără de aceste constatări, operatorii au fost sancționați pentru contravenția prevăzută la art. 32 din Legea nr. 677/2004, deoarece a păluciat în mod excesiv datele personale (imagini) ale persoanelor vizate prin intermediul acestor camere video, fără respectarea prevederilor legale conținute în Legea nr. 677/2004 raportat la Decretul ANSPDOP nr. 52/2012 pentru a fi respectată termenul de stocare limitat a imaginilor prevăzută în Decretul ANSPDOP nr. 52/2012.

3. Dezvăluirea datelor personale către diverse entități

În anul 2017, o pondere însemnată în numărul plângerilor și sesizărilor adresate Autorității naționale de supraveghere a fost reprezentată de petițiile prin care s-au semnalat situații diverse de încălcare a dispozițiilor legale privind condițiile în care date personale au fost dezvăluite publicului larg (prin publicarea pe Internet, de exemplu), către terțe persoane neautorizate sau către diverse entități de drept public și privat, fără să fi fost obținut în prealabil acordul persoanelor vizate, fără să existe un alt temel legal sau fără informarea acestora. În unele dintre aceste plângeri s-a reclamat publicarea fără consimțământul titularului a unor imagini (fotografii sau înregistrări video) pe rețelele de socializare, de către alți utilizatori persoane fizice ori crearea unor conturi false pe website-uri de dating prin folosirea unor date personale și fotografiilor însoțite de informații defăimătoare la adresa persoanelor vizate. În aceste ultime cazuri, instituția noastră a efectuat demersuri de investigare numai în măsura în care a fost posibilă identificarea deținătorilor respectivelor website-uri ca fiind operatori ce intră în sfera de competență teritorială a Autorității naționale de supraveghere.

Din investigațiile efectuate în anul 2017 s-a constatat faptul că, în anumite cazuri, dezvăluirea ilegală a datelor personale s-a produs ca urmare a neadoptării de către operatorii a măsurilor de securitate și confidențialitate necesare pentru a preveni accesul unor persoane neautorizate la date, datorate în special necunoașterii regulilor de protecție a datelor personale aplicabile în activitatea pe care o desfășoară.

FIȘĂ DE CAZ

Un patent a sesizat Autoritatea Națională de supraveghere cu privire la faptul că datele personale au fost dezvăluite către terți de fostul angajator.

În cadrul intervențiilor efectuate s-a constatat că datele personale ale titularului (date de identificare date de contractul individual de muncă și din fișa postului date privind starea de sănătate) au fost accesate și încheiate în cadrul unei proceduri disciplinare, au fost accesate prin intermediul sistemului electronic către toți angajații operatorului în vederea efectuării plății a salariului și pentru a fi realizată procedura de recrutare și sărbătorire în comună.

La finalizarea intervențiilor operatorului pentru viziua prevăzută de art. 32 din Legea nr. 677/2004 privind accesul către terți fără temel legal, datele cu caracter personal ale titularului au fost accesate în mod nelegal de art. 33 din Legea nr. 677/2004, întrucât operatorul nu a asigurat confidențialitatea datelor cu caracter personal ale titularului. Operatorul nu a asigurat confidențialitatea datelor cu caracter personal ale titularului în activitatea desfășurată de acesta și nu a luat măsurile tehnice și organizatorice necesare împotriva dezvăluirii datelor cu caracter personal ale acestuia.

FIȘĂ DE CAZ

Un operator a reclamat că asociația de proprietari din imobilul unde locuiește a prelucrat datele personale ale titularului în scopul de a realiza un raport privind activitatea adresă sa de către asociația de proprietari. Titularul a susținut că a fost în posesia datelor de proprietate în anul 2004 însă nu a primit niciun răspuns în termenul legal de 15 zile.

În urma investigației efectuate, s-a constatat că înscrisul menționat de titular a fost trimis la avizierul blocului și se referea la stadiul de avansare de recuperare debite pe care acesta îl avea în momentul de față de proprietar. În urma a unei încheieri de conciliere:

În ceea ce privește cererea titularului, adresați asociației de proprietari, operatorul a primit răspuns la cererea în ziua postată la titularului, fără a prezenta o dovadă în acest sens.

La finalizarea intervențiilor întreprinse operatorul a fost sancționat în baza art. 32 din Legea nr. 677/2004, întrucât a dezvăluit la avizierul blocului datele cu caracter personal, inclusiv numărul personal ale titularului, fără consimțământul acestuia sau alt temel legal și fără

și, în caz de ocazie înmărmurii acestuia. De asemenea, operatorul a fost sancționat întrucât nu a făcut dovada comunicării unui răspuns pozitiv, în ceea ce privește sa de excludere a dreptului de acces la prelucrarea datelor în 15 din Legea nr. 677/2001.

FIGURA 12

O plângere a rădănat faptul că datele sale au caracter personal ar fi fost dezvăluite ilegal de către o societate comercială (magazin de vânzare produselor).

Revenea la menționat și la o zi după procesul de divorț, fostul soț invocând calitatea de părinte și a solicitat de la operator o copie a unui bon de achiziție și a lui și a soției. Acesta a fost de acord să furnizeze în anul 2015, pretexând că îi este necesar în scopul trimiterii acestuia în o instituție de învățământ pentru realizarea unor activități.

În anul următor s-a realizat o copie după extrasul din sistem (factură) privind achiziția și a fost prezentat în anul 2015, în urma unei cereri scurte și a prezentați unor documente.

În urmărirea depusă la Autoritatea națională de supraveghere pentru prelucrarea de date biometrice în scop de furnizare de bunuri și servicii, operatorul a declarat că destinația și scopul activității este în vederea realizării activității operatorului, autoritatea judecătorească, poliția și autoritățile.

La finalizarea demersurilor întreprinse, operatorul a fost sancționat contravențional pentru epăa prelucrării de date 32 din Legea nr. 677/2001, întrucât a dezvăluit date cu caracter personal, în legătură cu conținutul documentelor de pe net.

4. Prelucrarea excesivă a datelor personale

Din practica de soluționare a plângerilor și sesizărilor adresate Autorității naționale de supraveghere în cursul anului 2017, 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 prelucreză 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 portării orelor de muncă, în situațiile incidente putând fi alese de către operator 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 (de exemplu, emiteria de facturi fiscale, returnarea unor produse comercializate), prin invocarea eronată a unor prevederi legale care ar impune această prelucrare. De asemenea, s-a constatat faptul că anumiți operatori de date personale colectează în mod excesiv și în lipsa unui temel legal expres copii ale actelor de identitate, în circumstanțe precum: plata unor facturi de utilități la ghișeele unor bănci, returnarea unor produse achiziționate de la diverși comercianți, permiterea accesului la anumite evenimente sociale.

În acest context, Autoritatea națională de supraveghere a urmărit respectarea art. 8 din Legea nr. 677/2001 și a Deciziei ANSPDCP nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.

a) Prelucrarea datelor biometrice

FIGURA 13

Au fost realizate activități de supraveghere a fost sesizată cu privire la faptul că o societate a realizat o activitate de supraveghere video în vederea și folosesc aparatul de implementare pentru monitorizarea activității.

În anul următor s-a realizat o copie după extrasul din sistem (factură) privind achiziția și a fost prezentat în anul 2015, în urma unei cereri scurte și a prezentați unor documente. În urmărirea depusă la Autoritatea națională de supraveghere pentru prelucrarea de date biometrice în scop de furnizare de bunuri și servicii, operatorul a declarat că destinația și scopul activității este în vederea realizării activității operatorului, autoritatea judecătorească, poliția și autoritățile.

În urma investigației operatorii a declarat că a dezafectat sistemul de prelucrare a datelor domeniilor de angajaților, a înscrisat prelucrarea acestor date și a procedat la ștergerea datelor domeniilor colectate.

b) Prelucrarea codului numeric personal și a copiei actului de identitate

FSX DE QIZ

Autoritatea națională de supraveghere a fost sesizată cu privire la colectarea codului numeric personal și al altor date societăți care comercializează produse vestimentare, în special în ceea ce privește șorții țării unui produs.

În urma a investigației efectuate, s-a constatat că societatea respectivă nu prelucraza în orice caz codul numeric personal de la persoanele fizice pentru înțirirea facturilor sau la furnizarea produselor însă în cazul prezentului, în mod egal, a colectat acestea date cu caracter special la schimbarea unui produs, CNP-ul fiind menționat atât pe factură, cât și pe dispoziția de plată, dar nefiind stocat în baza de date.

În urma investigației efectuate și prezentat codul numeric personal al persoanei vizate pentru înțirirea unui produs, fără reprezentarea prevederilor art. 8 din Legea nr. 677/2001, raportate la Decizia ANSPDCCP nr. 132/2011.

Societatea a implementat un manual de contabilitate la nivelul companiei, care a fost înlocuit cu sursele tuturor angajaților și care descrie procedura de natură de asamblare, efectuare și este inclusă în sensul completării documentelor legale doar cu datele prevăzute în procesul legislativ în vigoare.

FSX DE QIZ

Autoritatea națională de supraveghere a fost sesizată prin mai multe petiții cu privire la faptul că un organizator al unui eveniment internațional de muzică a solicitat CNP-ul și numărul de identitate în procedura de verificare (check-in) a bilețelor cumpărate online și a scanat acestea de rezervare a accesora la intrarea la festival.

În urma investigației efectuate în anul 2011 privind condițiile prelucrării codului numeric personal și al altor date societăți care comercializează produse vestimentare, în special în ceea ce privește șorții țării unui produs, CNP-ul fiind menționat atât pe factură, cât și pe dispoziția de plată, dar nefiind stocat în baza de date.

În urma investigației efectuate și prezentat codul numeric personal al persoanei vizate pentru înțirirea unui produs, fără reprezentarea prevederilor art. 8 din Legea nr. 677/2001, raportate la Decizia ANSPDCCP nr. 132/2011.

Societatea a implementat un manual de contabilitate la nivelul companiei, care a fost înlocuit cu sursele tuturor angajaților și care descrie procedura de natură de asamblare, efectuare și este inclusă în sensul completării documentelor legale doar cu datele prevăzute în procesul legislativ în vigoare.

Societatea a implementat un manual de contabilitate la nivelul companiei, care a fost înlocuit cu sursele tuturor angajaților și care descrie procedura de natură de asamblare, efectuare și este inclusă în sensul completării documentelor legale doar cu datele prevăzute în procesul legislativ în vigoare.

Societatea a implementat un manual de contabilitate la nivelul companiei, care a fost înlocuit cu sursele tuturor angajaților și care descrie procedura de natură de asamblare, efectuare și este inclusă în sensul completării documentelor legale doar cu datele prevăzute în procesul legislativ în vigoare.

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

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 intervenție asupra datelor (art. 14) și a dreptului de opoziție (art. 15), deși reprezintă o

obligație esențială a operatorilor de date, a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere și în anul 2017.

Astfel, ca urmare a investigațiilor efectuate, s-a constatat că operatorii nu cunosc obligațiile care le incumbă potrivit reglementărilor legale susmenționate ori le ignoră cu bună-știință; în alte cazuri, transmit persoanele vizate răspunsuri incomplete sau/și fără respectarea termenului de 15 zile prevăzut de lege. De asemenea, s-a mai constatat faptul că unii operatori nu au adoptat măsuri organizatorice interne care să se dovedească a fi eficiente pentru gestionarea cererilor adresate de persoanele vizate în baza drepturilor reglementate de Legea nr. 677/2001.

a) Nerespectarea dreptului de informare

CAZ DE CAZ

Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o societate de închiriere autoturisme (rent a car). Astfel, petentul reclamă că operatorul a furnizat date de geolocalizare cu privire la persoana sa, fără consimțământul său și fără o notificare prealabilă. În conformitate cu prevederile Legii nr. 677/2001,

operatorul este obligat să informeze persoana vizată înainte de a realiza activitatea de geolocalizare și să îi furnizeze datele de geolocalizare în baza legii nr. 677/2001.

Operatorul este obligat să informeze persoana vizată înainte de a realiza activitatea de geolocalizare și să îi furnizeze datele de geolocalizare în baza legii nr. 677/2001.

Din verificările efectuate, s-a constatat că încălcările, mai degrabă anexe la acestea și conținutul informațiilor complete privind înmănușarea persoanelor vizate, conform art. 12 din Legea nr. 677/2001. De asemenea, termenii și condițiile de utilizare disponibile pe site-ul societății nu făceau referință la prelucrarea datelor de localizare și nici la alte informații privind Legea nr. 677/2001.

Fără de a se constata, operatorul a fost sancționat.

pentru faptul prevăzut de art. 11 din Legea nr. 677/2001, întrucât nu a declarat în mod clar faptul de notificare la Autoritatea Națională de supraveghere preluarea datelor de geolocalizare.

Operatorul este obligat să informeze persoana vizată înainte de a realiza activitatea de geolocalizare și să îi furnizeze datele de geolocalizare în baza legii nr. 677/2001.

b) Nerespectarea dreptului de acces

CAZ DE CAZ

O petentă a sesizat faptul că două birouri ale unor executori judecătorești au prelucrat date personale cu încluzarea, printre altele, a art. 15 din Legea nr. 677/2001, întrucât au furnizat date de geolocalizare prin e-mail, cerere prin care își exercită dreptul de acces pe lângă

operatorii de date. În conformitate cu prevederile Legii nr. 677/2001, operatorii de date sunt obligați să informeze persoana vizată înainte de a realiza activitatea de geolocalizare și să îi furnizeze datele de geolocalizare în baza legii nr. 677/2001.

Din verificările efectuate, s-a constatat că încălcările, mai degrabă anexe la acestea și conținutul informațiilor complete privind înmănușarea persoanelor vizate, conform art. 12 din Legea nr. 677/2001. De asemenea, termenii și condițiile de utilizare disponibile pe site-ul societății nu făceau referință la prelucrarea datelor de localizare și nici la alte informații privind Legea nr. 677/2001.

Fără de a se constata, operatorul a fost sancționat.

FAȘA DE GLAZ

Un număr a rezizat o poștă încheiere a prevederilor Legii nr. 677/2001 și ale Legii nr. 116/2002 de către o societate de telecom. Petentul a susținut că operatorul în chestiune respectivă prezintă de art. 13-15 din Legea nr. 677/2001.

Petentul s-a adresat operatorului prin-o adresă prin care și exercita dreptul de acces la datele sale de telecom. solicitând informații referitoare la confirmarea faptului că datele sale sunt stocate în baza de date a operatorului respectiv în conformanță cu prevederile art. 13 din Legea nr. 677/2001 și ale Legii nr. 116/2002. Operatorul nu a răspuns la cererea respectivă în termenul stabilit în lege.

Societatea de telecom a transmis un răspuns petentului prin care înu a fost oferit niciun răspuns în privința operatorului de prelucrare a datelor efectuate de operator. Operatorul nu a încheiat în răspunsul către petent în mod clar dacă prelucrate sau nu datele personale referitoare la acesta, fiind astfel încheiate prevederile art. 13 din Legea nr. 677/2001.

Un număr învestiți în activitate, operatorul reclamant a fost sancționat pentru contravenția prevăzută de art. 32 din Legea nr. 677/2001, raportat la art. 13 din aceeași lege. Întrucât a încheiat dreptul de acces la date, prin faptul că nu a răspuns corect la solicitarea petentului de să în confirmat faptul că datele sale sunt sau nu prelucrate de societatea de telecom.

c) Nerespectarea dreptului de intervenție

FAȘA DE GLAZ

Autoritatea națională de supraveghere a fost sesizată în legătură cu o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către un minister.

Asfel petentul reclama faptul că a transmis o cerere către acest ministru înmănată în baza art. 14 din Legea nr. 677/2001, prin care a solicitat stingerea și/sau anonimizarea datelor personale prelucrate de datele sale personale afișate într-un sistem de evidență online considerată excesivă. Petentul a susținut că ministrul nu a răspuns solicitării sale.

Prin aceeași petiție înaintată Institutului Național de Protecție a Semnelor, faptului că, în sistemul de evidență online administrat de acest ministru sunt prelucrate date cu caracter personal date

Un număr a transmis o cerere către ministrul de telecom și cu privire la drepturile persoanelor vizate.

Prin cererea respectivă a fost sesizată de ministrul reclamant nu a răspuns corect cererii prin care acesta și-a exercitat dreptul de intervenție, în baza art. 14 din Legea nr. 677/2001.

Un număr a transmis o cerere către ministrul de telecom și cu privire la drepturile persoanelor vizate. Ministrul de telecom a răspuns cererii în baza art. 32 din Legea nr. 677/2001 și ale Legii nr. 116/2002.

d) Nerespectarea dreptului de opoziție

FAȘA DE GLAZ

Un număr multe petiții, un petent a sesizat Autoritatea națională de supraveghere cu privire la încălcarea dreptului la viața intimă, familială și privată cu privire la prelucrarea datelor personale de către o instituție financiară nebancară.

Un număr de petiții și solicitări de intervenție au fost încheiate în mod abuziv și în încălcarea dreptului la viața intimă, familială și privată. În acest caz intervenția cu privire la înregistrarea unor rezerve în cadrul contabilității. În acest caz petentul a sesizat de către o instituție financiară nebancară.

Un număr de petiții și solicitări de intervenție au fost încheiate în mod abuziv și în încălcarea dreptului la viața intimă, familială și privată. În acest caz intervenția cu privire la înregistrarea unor rezerve în cadrul contabilității. În acest caz petentul a sesizat de către o instituție financiară nebancară.

6. Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

În cursul anului 2017, Autoritatea națională de supraveghere a înregistrat în continuare un număr semnificativ de plângeri având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (SMS) sau prin poșta electronică. Majoritatea acestora au privit aspecte legate de protecția vieții private în sectorul comunicațiilor electronice prin primirea de mesaje comerciale nesolicitate prin poșta electronică, fără consimțământul expres și neechivoc al destinatarului în acest sens.

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

ANEXA DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o societate care l-a deranjat în numărul personal de telefon, un SMS care promova un magazin de distribuție telefonică mobilă și accesorii GSM, desi petentul si-a fi exprimat explicit opoziția față de astfel de servicii și de celelalte servicii de distribuție telefonică mobilă. După aceeași sesizare petentul a sesizat și faptul că s-a adresat societății, dar nuva primit năbuș răspuns.

În urma investigațiilor efectuate, s-a constatat faptul că operatorul colectă datele persoanelor care înregistrează în baza de date a societății din comenziile de prestări servicii de voce și date. În aceste condiții, clientii își pot exprima acordul sau opoziția față de prelucrarea datelor cu caracter personal de către operatorul de telefonie mobilă, printr-unul din opțiunile de servicii disponibile. Cu titlu excepțional, societatea prelucrază date ale persoanelor vizate în scopul activității de distribuție telefonică mobilă și în scopul comunicărilor comerciale.

Operatorul nu a stocat date cu caracter personal privindul pe petent, întrucât, în cazul achiziționării de cartele preplătite, societatea nu stochează informații privind identitatea

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o societate care l-a deranjat în numărul personal de telefon, un SMS care promova un magazin, desi nu a exprimat opoziția față de astfel de servicii și de celelalte servicii de distribuție telefonică mobilă. După aceeași sesizare petentul a sesizat și faptul că s-a adresat societății, dar nuva primit năbuș răspuns.

În urma investigațiilor efectuate, s-a constatat faptul că operatorul colectă datele persoanelor care înregistrează în baza de date a societății din comenziile de prestări servicii de voce și date. În aceste condiții, clientii își pot exprima acordul sau opoziția față de prelucrarea datelor cu caracter personal de către operatorul de telefonie mobilă, printr-unul din opțiunile de servicii disponibile. Cu titlu excepțional, societatea prelucrază date ale persoanelor vizate în scopul activității de distribuție telefonică mobilă și în scopul comunicărilor comerciale.

ANEXA DE CAZ

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o societate care l-a deranjat în numărul personal de telefon, un SMS care promova un magazin, desi nu a exprimat opoziția față de astfel de servicii și de celelalte servicii de distribuție telefonică mobilă. După aceeași sesizare petentul a sesizat și faptul că s-a adresat societății, dar nuva primit năbuș răspuns.

În urma investigațiilor efectuate, s-a constatat faptul că operatorul colectă datele persoanelor care înregistrează în baza de date a societății din comenziile de prestări servicii de voce și date. În aceste condiții, clientii își pot exprima acordul sau opoziția față de prelucrarea datelor cu caracter personal de către operatorul de telefonie mobilă, printr-unul din opțiunile de servicii disponibile. Cu titlu excepțional, societatea prelucrază date ale persoanelor vizate în scopul activității de distribuție telefonică mobilă și în scopul comunicărilor comerciale.

Operatorul nu a stocat date cu caracter personal privindul pe petent, întrucât, în cazul achiziționării de cartele preplătite, societatea nu stochează informații privind identitatea

Un petent a sesizat o posibilă încălcare a dispozițiilor Legii nr. 677/2001 de către o societate care l-a deranjat în numărul personal de telefon, un SMS care promova un magazin, desi nu a exprimat opoziția față de astfel de servicii și de celelalte servicii de distribuție telefonică mobilă. După aceeași sesizare petentul a sesizat și faptul că s-a adresat societății, dar nuva primit năbuș răspuns.

În urma investigațiilor efectuate, s-a constatat faptul că operatorul colectă datele persoanelor care înregistrează în baza de date a societății din comenziile de prestări servicii de voce și date. În aceste condiții, clientii își pot exprima acordul sau opoziția față de prelucrarea datelor cu caracter personal de către operatorul de telefonie mobilă, printr-unul din opțiunile de servicii disponibile. Cu titlu excepțional, societatea prelucrază date ale persoanelor vizate în scopul activității de distribuție telefonică mobilă și în scopul comunicărilor comerciale.

operatorilor fără consimțământul expres și prealabil al deținătorilor adreselor de poștă electronice.

REȘIDEECIZ

Autoritatea națională de supraveghere a fost sesizată de o persoană fizică în legătură cu faptul că a primit mai multe mesaje comerciale pe adresa sa personală de e-mail, de la o companie de e-mail care aparține unei societăți cu obiect de activitate realtă, marketing și servicii de servicii de servicii electronice, cu precizarea că nu și-a dat niciodată acordul pentru prelucrarea datelor pe care respectivul operator

reține și a destinat căi să-a adresat operatorului, prin intermediul poștei electronice, solicitându-l să înlătească datele cu caracter personal din baza de date a operatorului, dar nu a primit niciun răspuns.

Într-o a investigației efectuate, s-a constatat faptul că datele cu caracter personal ale operatorului, respectiv nume, prenume și adresă de e-mail, au intrat în baza de date a societății responsabile cu servicii de participare la un concurs de prestări servicii și birarea cărui sunt de acord cu termenii de înscriere în concurs și de primire de comunicații comerciale din partea societății.

La momentul controlului, operatorul nu a prezentat nicio dovadă a obținerii consimțământului expres prealabil al titularului pentru prelucrarea datelor sale cu caracter personal (nume, prenume, adresă de e-mail) de către societate, în scopul transmiterii de mesaje comerciale.

Cu toate acestea, s-a identificat faptul că numele și prenumele titularului precum și adresa de e-mail se află în baza de date a operatorului, la momentul controlului, având statusul de titular pentru transmiterea de mesaje comerciale. Dezvăluirea datelor titularului de la operatorul de mesaje comerciale s-a realizat cu umare a deciziei operatorului, și nu la solicitarea titularului.

Reprezentanții operatorului au declarat că singurul mesaj comercial transmis către adresa titularului a fost în cadrul unui concurs și că nu au fost găsiți în evidențele societății e-mail-uri transmise de titular prin care solicita ștergerea datelor sale din baza de date a operatorului.

Fără să fi fost sesizată operatorul a fost sancționat convențional în baza art. 15 raportat la art. 12 din Legea nr. 506/2004 și s-a solicitat să ștergă toate datele personale (numere de telefon), dar și adrese de e-mail, colectate și utilizate în a consumantului expres consimțământul și deținătorilor în scopul trimiterii de comunicații comerciale și să înceteze trimiterea de mesaje comerciale prin mijloace electronice fără consimțământul expres și prealabil al deținătorilor și să informeze de urgență operatorul.

7. Încălcarea regulilor de confidențialitate și securitate a prelucrării 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 prelucrării 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 2017, o parte din plângerile și sesizările ce au fost adresate Autorității naționale de supraveghere au avut ca obiect fie dezvăluirea datelor personale către terțe persoane, fie accesarea neautorizată a datelor personale (inclusiv de către angajații proprii), ca umare a faptului că operatorii în cauză (comercianții, autorități publice, furnizori de servicii de telefonie, clinici medicale etc.) nu au implementat proceduri interne eficiente, de ordin tehnic sau organizatoric, care să conducă la prevenirea unor astfel de probleme.

REȘIDEECIZ

Un titular a sesizat că angajați ai unui magazin de vânzare produse electrocasnice au accesat în mod neautorizat conținutul său de poștă electronică de pe telefonul cumpărat de la magazin și au transmis informații și nume ale altor titulari care au

accesat în mod neautorizat conținutul său de poștă electronică de pe telefonul cumpărat de la magazin și au transmis informații și nume ale altor titulari care au accesat în mod neautorizat conținutul său de poștă electronică de pe telefonul cumpărat de la magazin și au transmis informații și nume ale altor titulari care au

accesat în mod neautorizat conținutul său de poștă electronică de pe telefonul cumpărat de la magazin și au transmis informații și nume ale altor titulari care au accesat în mod neautorizat conținutul său de poștă electronică de pe telefonul cumpărat de la magazin și au transmis informații și nume ale altor titulari care au

de însoțire fără însă a se verifica în prealabil dacă telefonul a fost reabus la sechela din
Fără
În urma sesizării operatorului de către petent, ca e-mailul său a fost accesat de pe
telefonul reabus operatorului a încercat, fără rezultat, contactarea noului posesor al telefonului
ca să-l găsească posesorul telefonului să-l prezente în magazin și a reclamat că telefonul nu
a rămas în posesia sa. Operatorul a stornat factura, a reabus telefonul, l-a reabus și l-a
fără spre casă.

În cadrul investigației, s-a constatat că operatorul nu a văcut dovada că deține o poliție
de securitate în acest caz și că este produsul reabus și, eventual, revăcut, care pot conține
date cu caracter personal ale clientilor.

În urma verificării operatorului nu a luat măsură de verificare a telefonului reabus
de către în sensul de a fi reabus la sechela din răbită înainte de a fi vândut unei alte
persoane în acest caz și că este posibilă dezvăluirea reabusă a datelor cu caracter personal ale
clientilor.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a
sesionat operatorul pentru a prezenta datele nr. 677/2001, întrucât acesta
nu a luat măsură suficiente împotriva dezvăluirii sau accesului neautorizat în ceea ce privește
datele cu caracter personal ale petentului, stocate pe telefonul mobil reabus operatorului și
revăcut altui petent.

FISĂ DE CAZ

Autoritatea Națională de Supraveghere a fost sesizată de către un petent cu privire la
faptul că, în mod constant, pe adresa sa de e-mail, de la un operator care oferă
servicii medicale (dintre) a corespondență pentru o altă persoană, fiind dezvăluite, astfel,
datele cu caracter personal ale acestora. În urma bulime de analize medicale.

În cadrul raportului, operatorul a declarat că, din cauza faptului că adresele de poștă
electronică "gmail.com" nu au în considerare șanșele de punctuație (" ") în compunerea unei
adrese de e-mail, a fost posibilă transmiterea pe adresa de poștă electronică a petentului a
unor informații care erau destinate să fie transmise unui abonat al difuziei, cu o adresă de e-mail
reabusă.

În urma verificării operatorului nu a luat măsură de verificare a telefonului reabus
de către în sensul de a fi reabus la sechela din răbită înainte de a fi vândut unei alte
persoane în acest caz și că este posibilă dezvăluirea reabusă a datelor cu caracter personal ale
clientilor.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a
sesionat operatorul pentru să vădă datele nr. 677/2001, întrucât acesta
nu a luat măsură suficiente împotriva dezvăluirii datelor
cu caracter personal ale unei persoane vizate către un terț, deși a fost sesizată cu privire la acest aspect,
și în acest caz.

FISĂ DE CAZ

În urma verificării operatorului nu a luat măsură de verificare a telefonului reabus
de către în sensul de a fi reabus la sechela din răbită înainte de a fi vândut unei alte
persoane în acest caz și că este posibilă dezvăluirea reabusă a datelor cu caracter personal ale
clientilor.

În urma exercitării dreptului de acces la date, fără de înal multe instituții, petentului s-a
reabusă și datele sale cu caracter personal au fost furnizate de către autoritatea reabusă.
În urma verificării operatorului nu a luat măsură de verificare a telefonului reabus
de către în sensul de a fi reabus la sechela din răbită înainte de a fi vândut unei alte
persoane în acest caz și că este posibilă dezvăluirea reabusă a datelor cu caracter personal ale
clientilor.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a
sesionat operatorul pentru să vădă datele nr. 677/2001, întrucât acesta
nu a luat măsură suficiente împotriva dezvăluirii datelor
cu caracter personal ale unei persoane vizate către un terț, deși a fost sesizată cu privire la acest aspect,
și în acest caz.

Prin funcțiile prevăzute la art. 20 din această lege, în vederea operațiunii (autoritatea redată) nu s-a ipotezizat suficiența măsurii tehnice și organizatorice fiind astfel posibil accesul neautorizat la datele cu caracter personal ale persoanelor de către un angajat al serviciului local al operatorului, în agra îndeplinirii sarcinilor de serviciu.

CAPITOLUL AL V-LEA

ACTIVITĂȚI ÎN DOMENIUL RELAȚIILOR INTERNAȚIONALE

Activitatea în plan extern a Autorității naționale de supraveghere a fost marcată și în anul 2017 de participarea la o serie de grupuri de lucru, conferințe, seminarii și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului European, în domeniul protecției datelor cu caracter personal, precum și prin implicarea în activitatea desfășurată în cadrul acestora.

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 fi aplicabil pe întreg teritoriul Uniunii Europene începând cu data de 25 mai 2018. Astfel, Autoritatea națională de supraveghere, reprezentantă de membrii săi, a participat în 2017 la o serie de reuniuni și diverse grupuri de lucru la nivel european. Printre acestea se numără:

- Grupul de Lucru Articolul 29 (înființat în temeiul art. 29 din Directiva 95/46/CE) care reunește toate autoritățile europene, precum și Autoritatea Europeană pentru Protecția Datelor. Astfel, menționăm faptul că Autoritatea națională de supraveghere, prin membrii săi, a participat la următoarele subgrupuri de lucru: BTLE, Cooperare, eGovernare, Enforcement, Financial Matters, Future of Privacy, Key provisions, Tehnologie, Transferuri Internaționale,
- Comitetul Consultativ al Convenției 108 al Consiliului European (T-PD),
- Organismul comun de control în domeniul Europei și domeniul Varnai,
- Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II și Grupul de coordonare comună Eurodac,
- Grupul Internațional de Lucru pe Protecția Datelor în domeniul Telecomunicațiilor, dedicat protecției datelor cu caracter personal în sectorul comunicațiilor electronice,
- Grupul de Lucru pe protecția datelor în cadrul Convenției pentru stabilirea Centrului Sud-Est European de aplicare a legii.

Grupul de Lucru Articolul 29

În cursul anului 2017, Grupul de Lucru Articolul 29 și-a exprimat poziția față de probleme fundamentale precum reforma în domeniul vieții private și comunicațiilor electronice, prelucrarea datelor cu caracter personal la locul de muncă, prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative, prelucrarea datelor cu



caracter personal în cadrul activității polițienești și judiciare în materie penală și, totodată, a emis o serie de orientări cu privire la aplicarea Regulamentului General privind Protecția Datelor.

Astfel, menționăm următoarele documente ce au fost adoptate fie sub formă de avize, fie sub formă de ghiduri pentru interpretarea și aplicarea Regulamentului General privind Protecția Datelor:

> *avizul cu privire la propunerea de Regulament privind viața privată și comunicațiile electronice (2002/58/CE)* – documentul oferă o analiză a propunerii de Regulament ePrivacy. În acest context, menționăm faptul că Grupul de Lucru Articolul 29 apreciază în mod favorabil alegerea regulamentului ca instrument normativ și consideră că, astfel, se asigură uniformitatea normelor în întreaga UE și claritate atât pentru autoritățile de supraveghere, cât și pentru organizații. De asemenea, se asigură coerența cu Regulamentul general privind protecția datelor. În plus, la asigurarea coerenței contribuie și opțiunea de a desemna aceeași autoritate care răspunde de monitorizarea conformității cu RGPD pentru a răspunde și de asigurarea respectării normelor privind viața privată și comunicațiile electronice. Totodată, alegerea unui instrument juridic complementar prezintă un aspect pozitiv. Protecția comunicațiilor confidențiale și a echipamentelor terminale comportă caracteristici speciale care nu sunt abordate de RGPD. Prin urmare, sunt necesare dispoziții complementare cu privire la aceste tipuri de servicii, astfel încât să se asigure protecția corespunzătoare a dreptului fundamental la viață privată și confidențialitatea comunicațiilor, inclusiv confidențialitatea echipamentelor terminale. În această privință, Grupul de Lucru Articolul 29 sprijină abordarea principală adoptată în propunerea de Regulament, respectiv de extindere a interdicțiilor și de restrângere a excepțiilor, precum și aplicarea punctuală a conceptului de consimțământ. Cât privește consimțământul privind urmărirea („consent for tracking”), Grupul de Lucru Articolul 29 solicită interzicerea explicită a pereților de urmărire („tracking walls”), adică a opțiunilor de tipul „acceptare sau renunțare”, care îi obligă pe utilizatori să consimtă la urmărirea dacă doresc să aibă acces la serviciul respectiv. Grupul de Lucru Articolul 29 a identificat și alte motive de îngrijorare, referitoare, de exemplu, la domeniul de aplicare, la protecția echipamentelor terminale și la marketingul direct. Nu în ultimul rând, Grupul de Lucru Articolul 29 a identificat aspecte care necesită clarificări, pentru a proteja mai bine utilizatorii finali și pentru a asigura un nivel mai ridicat de securitate juridică pentru toate părțile interesate implicate;



> *avizul privind prelucrarea datelor la locul de muncă* – documentul completează Avizul Grupului de Lucru Articolul 29 nr. 8/2001 privind prelucrarea datelor personale în contextul angajării și Documentul de lucru din 2002 privind supravegherea comunicațiilor electronice la locul de muncă. Documentul realizează o nouă evaluare a echilibrului dintre interesul legitim al angajatorului și așteptările angajaților în ceea ce privește confidențialitatea datelor cu caracter personal/respectarea vieții private. Astfel, luând în considerare prevederile Directivei 95/46/CE privind protecția datelor, proiectul de opinie are în vedere obligațiile suplimentare impuse angajatorilor prin Regulamentul General privind Protecția Datelor. De asemenea, prin acest document, Grupul de Lucru Articolul 29 reiterează poziția și concluziile sale exprimate prin Opinia 8/2001 și Documentul de lucru din 2002. În acest context, se subliniază faptul că, atunci când se realizează o prelucrare a datelor cu caracter personal ale angajaților: (i) angajatorii trebuie să respecte întotdeauna principiile fundamentale de protecție a datelor cu caracter personal, indiferent de tehnologia utilizată; (ii) conținutul comunicațiilor electronice realizate în afara spațiului de afaceri beneficiază de aceeași protecție a drepturilor fundamentale ca și comunicațiile analogice; (iii) este foarte puțin probabil ca temeiul legal pentru prelucrarea datelor la locul de muncă să fie reprezentat de consimțământ, cu excepția cazului în care angajații pot refuza fără a exista consecințe negative; (iv) uneori se poate invoca executarea unui contract sau interesul legitim, cu condiția ca prelucrarea să fie strict necesară pentru îndeplinirea unui scop legitim și să respecte principiul proporționalității și cel al subsidiarității; (v) angajații ar trebui să primească informații eficiente cu privire la monitorizarea respectivă; (vi) orice transfer internațional de date ale angajaților ar trebui să aibă loc numai în situația în care se asigură un nivel de protecție adecvat;

> *avizul privind prelucrarea datelor cu caracter personal în contextul sistemelor de transport inteligente cooperative (STI)* – documentul elaborat la nivelul Grupului de Lucru Articolul 29 constă în furnizarea de informații generale privind prelucrarea datelor cu caracter personal în contextul STI cooperative și oferă îndrumări cu scopul de a îmbunătăți nivelul de protecție a datelor în cadrul acestor noi tipuri de aplicații. Astfel, Grupul de Lucru Articolul 29 consideră că următoarele aspecte ale protecției datelor cu caracter personal sunt deosebit de importante: Comisia ar trebui să pună în aplicare regulamente sectoriale pentru colectarea și prelucrarea de date în domeniul sistemelor de transport inteligente; Comisia ar trebui să stabilească o foale de parcurs pentru prelucrarea legală a datelor de localizare ale cetățenilor UE în contextul STI cooperative, obiectivul final fiind adoptarea unui instrument juridic la nivelul

UE [art. 6 (1) (c) din Regulamentul General privind Protecția Datelor]; adoptarea acestor instrumente juridice ar trebui să înceapă cu o evaluare a necesității și a proporționalității dispozitiilor lor; în plus, în cursul procesului legislativ, ar trebui să se efectueze o evaluare a impactului asupra protecției datelor [art. 35 (10) din Regulamentul General privind Protecția Datelor] pentru a se clarifica de la început riscurile și măsurile de remediere; celelalte temeiuri juridice avute în vedere în documentul grupului de lucru pentru STI cooperative (și anume, consimțământul, îndeplinirea unui interes legitim al contractantului) ar putea fi invocate numai în cazul în care pot fi soluționate aspectele critice identificate pentru fiecare dintre acestea în acest document; în oricare dintre temeiurile juridice selectate, setarea implicită a tuturor funcțiilor STI cooperative instalate trebuie să fie dezactivată; dispozitiile art. 25 din Regulamentul General privind Protecția Datelor (asigurarea protecției datelor începând cu momentul conceperii și în mod implicit) ar trebui să fie puse în aplicare, permițând utilizatorilor să selecteze opțiunile de urmărire (calendar, frecvență, locații) care corespund cel mai bine preferințelor proprii; securitatea ar trebui consolidată, pentru a limita riscul unei utilizări nelegitime a datelor din cadrul STI cooperative; ar trebui să fie introduse alte măsuri corective pentru protecția vieții private începând cu momentul conceperii; categoriile speciale de date și datele referitoare la condamnări penale și infracțiuni nu ar trebui să fie transmise; calitatea datelor ar trebui să fie evaluată cu atenție pentru a reduce orice risc; perioadele de păstrare a datelor prelucrate de către toate părțile implicate în platforma STI cooperative ar trebui să fie indicate în mod clar și ar trebui să fie interzisă crearea unei baze de date centralizate a mesajelor transmise de către oricare dintre actorii din cadrul STI cooperative;

> *avizul privind anumite aspecte importante ale Directivei (UE) 2016/680* – noua Directivă (UE) 2016/680 completează Regulamentul General privind Protecția Datelor. Directiva (UE) 2016/680, care trebuie transpusă în legislația națională până la data de 6 mai 2018, supraveghează prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, cercetării, detectării sau urmăririi penale a infracțiunilor sau executării de sancțiuni penale și asupra liberei circulații a acestor date. Pentru a sugera o înțelegere și o abordare coerentă și datorită diferențelor etape ale punerii în aplicare, Grupul de Lucru Articolul 29 a decis să se concentreze asupra unor aspecte-cheie pentru care sunt necesare orientări practice sau care se referă direct la activitatea autorităților de protecție a datelor sau atunci când procedura de punere în aplicare în unul sau mai multe state membre sugerează că transpunerea nu este în deplină conformitate cu principiile directivei. Având în vedere această

abordare, Grupul de Lucru Articolul 29 oferă în acest document orientări prin recomandări și observații cu privire la următoarele articole: art. 5 – termene de stocare și de revizuire, art. 10 – prelucrarea unor categorii speciale de date cu caracter personal, art. 11 – procesul decizional individual automatizat, inclusiv crearea de profiluri, art. 13-17 – drepturile persoanei vizate, art. 25 – înregistrarea (logs), art. 47 – competențele autorităților pentru protecția datelor;

> *ghidul privind dreptul la portabilitatea datelor* – Art. 20 din Regulamentul General privind Protecția Datelor introduce un drept nou, respectiv dreptul la portabilitatea datelor. Acest drept permite persoanelor vizate să primească datele cu caracter personal pe care le-au furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat, și să transmită datele respective altui operator, fără obstacole. Dreptul la portabilitatea datelor, care se aplică sub rezerva anumitor condiții, sprijină alegerea utilizatorului („user choice”), controlul utilizatorului („user control”) și responsabilizarea utilizatorului („user empowerment”). Noul drept la portabilitatea datelor are ca scop responsabilizarea persoanelor vizate în ceea ce privește propriile date cu caracter personal, întrucât facilitează capacitatea de a muta, copia sau transmite datele cu caracter personal de la un mediu IT la altul (fie la propriile sisteme, fie la sistemele unor părți terțe de încredere sau cele ale noulor operatori de date). Prin afirmarea drepturilor și controlul persoanelor vizate asupra datelor cu caracter personal care le privesc, portabilitatea datelor reprezintă, de asemenea, o oportunitate de a „re-echilibra” relația dintre persoanele vizate și operatorii de date. Cu toate că dreptul la portabilitatea datelor este un drept nou, alte tipuri de portabilitate deja există sau sunt discutate în alte domenii ale legislației (de exemplu în contextul rezilierii contractului, servicii de comunicații de roaming și accesul transfrontalier la servicii). Pot apărea unele sinergii și chiar beneficii pentru persoanele fizice între diferitele tipuri de portabilitate, în situația în care sunt prevăzute într-o abordare combinată, chiar dacă analogiile ar trebui să fie tratate cu precauție. Așadar, documentul oferă îndrumări operatorilor de date, astfel încât aceștia să-și actualizeze practicile, procesele și procedurile și clarifică înțelesul de portabilitate a datelor, pentru a permite persoanelor vizate să utilizeze acest drept în mod eficient;

> *ghidul privind responsabilitățile cu protecția datelor („DPO”)* – Regulamentul General privind Protecția Datelor ce urmează să devină aplicabil la data de 25 mai 2018 oferă un cadru legal modernizat pentru protecția datelor în Uniunea Europeană. Responsabilitățile cu protecția datelor (DPO) va reprezenta centrul acestui nou cadru juridic pentru multe organizații, facilitând respectarea prevederilor Regulamentului General privind Protecția Datelor. Potrivit



Regulamentului General privind Protecția Datelor, este obligatoriu ca anumiți operatori și persoane împuternicite de operatori să desemneze un DPO. Aceasta va fi situația pentru toate autoritățile și organismele publice (indiferent de tipul datelor prelucrate) și pentru celelalte organizații care – ca activitate principală – monitorizează în mod sistematic și pe scară largă persoanele fizice sau prelucrează categorii speciale de date cu caracter personal pe scară largă. Chiar și în situația în care Regulamentul General privind Protecția Datelor nu impune în mod expres numirea unui DPO, organizațiile pot găsi ca fiind utilă desemnarea unui DPO în mod voluntar. Grupul de Lucru Articolul 29 încurajează aceste eforturi voluntare. Conceptul de DPO nu este nou. Cu toate că Directiva 95/46/CE nu impune niciunei organizații să numească un DPO, această practică de numire a unui DPO s-a dezvoltat, de-a lungul anilor, în mai multe state membre. Anterior adoptării Regulamentului General privind Protecția Datelor, Grupul de Lucru Articolul 29 a susținut că DPO reprezintă un punct important al responsabilității și că numirea unui DPO poate facilita respectarea și, în plus, poate reprezenta un avantaj competitiv pentru companii. Pe lângă facilitarea respectării prin punerea în aplicare a instrumentelor de responsabilizare (precum facilitarea evaluărilor impactului asupra protecției datelor și efectuarea sau facilitarea auditurilor), DPO acționează ca intermediar între părțile interesate relevante (de exemplu autoritățile pentru protecția datelor, persoanele vizate și unitățile de afaceri din cadrul unei organizații). DPO nu este personal responsabil în caz de nerespectare a Regulamentului General privind Protecția Datelor. Regulamentul General privind Protecția Datelor stipulează că responsabil este operatorul sau persoana împuternicită de operator care trebuie să se asigure și să fie în măsură să demonstreze că prelucrarea este efectuată în conformitate cu dispozițiile sale (art. 24(1)). Respectarea normelor de protecție a datelor reprezintă responsabilitatea operatorului sau a persoanei împuternicite de operator. Operatorul sau persoana împuternicită de operator are de asemenea un rol crucial în a permite îndeplinirea eficientă a atribuțiilor DPO. Numirea unui DPO reprezintă un prim pas, dar trebuie să se asigure că DPO are autonomie și resurse suficiente pentru îndeplinirea sarcinilor într-un mod eficient. Regulamentul General privind Protecția Datelor recunoaște DPO ca un actor-cheie în noul sistem de guvernare al protecției datelor și stabilește condițiile pentru numirea sa, poziția și sarcinile sale. Obiectivul acestui ghid este de a clarifica prevederile relevante din Regulamentul General privind Protecția Datelor pentru a ajuta operatorii și persoanele împuternicite de operator în vederea respectării legii, dar și pentru a ajuta DPO în ceea ce privește rolul său. Ghidul oferă, de asemenea, recomandări de bune practici, bazându-se pe experiența acumulată în unele state membre UE;



> *ghidul privind stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator* – stabilirea unei autorități de supraveghere principale este importantă doar în cazul în care un operator sau o persoană împuternicită de operator efectuează prelucrări transfrontaliere de date cu caracter personal. Astfel, o „autoritate de supraveghere principală” este autoritatea care are responsabilitatea principală în activitatea de prelucrare transfrontalieră a datelor, de exemplu în cazul în care o persoană vizată depune o plângere referitoare la prelucrarea datelor sale personale. Autoritatea de supraveghere principală va coordona orice investigație, implicând alte autorități de supraveghere „vizate”. Stabilirea autorității de supraveghere principale depinde de identificarea locației „sedului principal” sau a „sedului unic” al operatorului, pe teritoriul UE. Considerentul 36 al Regulamentului General privind Protecția Datelor este util în clarificarea factorului principal care va fi utilizat pentru a stabili sediul principal al operatorului în cazul în care criteriul administrației centrale nu se aplică. Acest lucru implică identificarea locului în care se exercită efectiv și real activitățile de management, care stabilesc deciziile principale privind scopurile și mijloacele de prelucrare prin acorduri stabile. Esența autorității de supraveghere principale în Regulamentul General privind Protecția Datelor este că supravegherea prelucrării transfrontaliere ar trebui să fie în sarcina unei singure autorități de supraveghere pe teritoriul UE. În cazurile în care deciziile privind diferitele activități de prelucrare transfrontaliere sunt luate în cadrul administrației centrale pe teritoriul UE, va fi o singură autoritate de supraveghere principală pentru diversele activități de prelucrare a datelor efectuate de compania multinațională;

> *ghidul privind evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat” în sensul Regulamentului (UE) 2016/679* – art. 35 din Regulamentul General privind Protecția Datelor introduce conceptul de Evaluarea impactului asupra protecției datelor (DPIA), așa cum prevede și Directiva (UE) 2016/680. DPIA reprezintă o parte esențială a respectării Regulamentului General privind Protecția Datelor atunci când este planificată sau are loc o prelucrare a datelor cu risc ridicat. Aceasta înseamnă că operatorii de date ar trebui să utilizeze criteriile stabilite în acest document pentru a stabili dacă trebuie sau nu să realizeze o DPIA. Politica internă a operatorului de date ar putea extinde această listă în afara cerințelor legale ale Regulamentului General privind Protecția Datelor. Acest lucru ar trebui să ducă la o mai mare încredere a persoanelor vizate și a altor operatori de date. În cazul în care este planificată o prelucrare cu risc ridicat, operatorul de date trebuie: (i) să aleagă o metodologie DPIA care să îndeplinească

criteriile stabilite în ghid sau să specifice și să implementeze un proces sistematic de DPIA care să fie în conformitate cu criteriile prezentate în documentul adoptat de Grupul de Lucru Articolul 29, care este integrat în procesele existente de proiectare, dezvoltare, schimbare, risc și revizuire operațională, în conformitate cu procedurile interne, contextul și cultura, care implică părțile interesate și care definește în mod clar responsabilitățile acestora (operatorul, DPO, persoanele vizate sau reprezentanții acestora, întreprinderi, servicii tehnice, persoanele împuternicite de operatori, ofițerii de securitate a informațiilor etc.); (ii) să furnizeze raportul DPIA autorității de supraveghere competente atunci când este necesar să o facă; (iii) să consulte autoritatea de supraveghere atunci când nu a reușit să stabilească suficiente măsuri pentru atenuarea riscurilor ridicate; (iv) să revizuiască periodic DPIA și procesele pe care le evaluează, cel puțin atunci când există o schimbare a riscului reprezentat de prelucrarea operațiunii; (v) să documenteze deciziile luate.

La sfârșitul anului 2017, Grupul de Lucru Articolul 29 a adoptat următoarele ghiduri disponibile spre consultare publică și trimitere de propuneri:

➤ *ghidul privind notificarea încălcărilor de securitate în sensul Regulamentului (UE) 2016/679* – Regulamentul General privind Protecția Datelor introduce cerința privind notificarea autorității naționale pentru protecția datelor în legătură cu încălcarea securității datelor și, în anumite situații, comunicarea încălcării securității datelor către persoanele fizice ale căror date cu caracter personal au fost afectate de încălcare. Grupul de Lucru Articolul 29 consideră că noua cerință de notificare are numeroase beneficii. Atunci când notifică autoritatea de supraveghere, operatorii pot obține sfaturi dacă persoanele afectate trebuie să fie informate. Într-adevăr, autoritatea de supraveghere poate solicita operatorului să informeze acele persoane în legătură cu încălcarea securității datelor. Notificarea încălcării securității datelor trebuie privită ca un instrument de îmbunătățire a respectării legii în ceea ce privește protecția datelor cu caracter personal. Regulamentul General privind Protecția Datelor conține dispoziții cu privire la momentul în care o încălcare trebuie notificată și cui, precum și ce informații ar trebui furnizate ca parte a notificării. Informațiile solicitate pentru notificare pot fi furnizate în etape, dar, în orice caz, operatorii ar trebui să acționeze în timp util asupra oricărei încălcări. Trebuie subliniat faptul că neîndeplinirea acestei obligații poate însemna o eventuală sancțiune aplicabilă operatorului în temeiul art. 83 din Regulamentul General privind Protecția Datelor. Acest document explică cerințele obligatorii de notificare și de comunicare, precum și anumiți pași pe care operatorii și persoanele împuternicite de operator trebuie să îi parcurgă pentru a

îndeplini aceste noi obligații. Ghidul oferă, de asemenea, exemple de tipuri de încălcări și diferite scenarii privind cine ar trebui să fie notificat/informat;

➤ *ghidul privind procesul decizional individual automatizat, inclusiv crearea de profiluri în sensul Regulamentului (UE) 2016/679* – Regulamentul General privind Protecția Datelor se referă în mod special la crearea de profiluri și procesul decizional individual automatizat, inclusiv crearea de profiluri. Profilarea și luarea automată a deciziilor sunt utilizate într-un număr tot mai mare de sectoare atât private, cât și publice. Sistemul bancar și finanțele, asistența medicală, asigurări, marketing și publicitate sunt doar câteva exemple din domeniile în care se realizează o profilare mai regulată pentru a ajuta la luarea deciziilor. Cu toate acestea, crearea de profiluri și procesul decizional automatizat pot prezenta riscuri semnificative pentru drepturile și libertățile persoanelor fizice și, implicit, necesită garanții adecvate. Regulamentul General privind Protecția Datelor introduce noi dispoziții pentru a aborda riscurile care decurg din crearea de profiluri și procesul decizional automatizat, în special, dar fără a se limita la viața privată. Scopul acestor orientări este de a clarifica aceste dispoziții. Documentul publicat de Grupul de Lucru Articolul 29 abordează următoarele aspecte: definiția profilării și a procesului decizional automatizat; prevederile generale privind crearea de profiluri și procesul decizional automatizat; prevederile specifice privind deciziile bazate exclusiv pe prelucrarea automată, așa cum este menționat la art. 22 din Regulamentul General privind Protecția Datelor; minorii și crearea de profiluri; evaluarea impactului asupra protecției datelor și responsabilitii cu protecția datelor;

➤ *ghidul privind consimțământul în sensul Regulamentului (UE) 2016/679* – documentul oferă o analiză aprofundată a noțiunii de consimțământ din Regulamentul General privind Protecția Datelor. Conceptul de consimțământ, așa cum este menționat în Directiva 95/46/CE și Directiva ePrivacy, a evoluat. Regulamentul General privind Protecția Datelor oferă o clarificare suplimentară și o specificare a cerințelor pentru obținerea și demonstrarea consimțământului valabil. Ghidul se concentrează asupra acestor modificări și oferă orientări practice pentru a asigura conformitatea cu Regulamentul General privind Protecția Datelor, având la bază Avizul Grupului de Lucru Articolul 29 nr. 15/2011 privind consimțământul. Opiniile existente ale Grupului de Lucru Articolul 29 privind consimțământul rămân relevante, întrucât Regulamentul General privind Protecția Datelor menționează faptul că orientările și bunele practici generale ale Grupului de Lucru Articolul 29 existente și majoritatea elementelor-cheie ale consimțământului rămân aceleași. Așadar, prin acest document, Grupul de Lucru Articolul 29



extinde și completează opiniile anterioare pe teme specifice care includ trimiterea la consimțământul în temeiul Directivei 95/46/CE;

➤ *ghidul privind transparența în sensul Regulamentului (UE) 2016/679* – documentul oferă orientări practice și asistență interpretativă privind noua obligație de transparență în ceea ce privește prelucrarea datelor cu caracter personal în temeiul Regulamentului General privind Protecția Datelor. Transparența reprezintă o obligație generală în temeiul Regulamentului General privind Protecția Datelor care se aplică în trei domenii centrale: (1) furnizarea de informații persoanelor vizate legate de prelucrarea corectă; (2) modul în care operatorii de date comunică cu persoanele vizate în legătură cu drepturile lor în temeiul Regulamentului General privind Protecția Datelor; și (3) modul în care operatorii de date facilitează exercitarea de către persoanele vizate a drepturilor lor. În măsura în care respectarea transparenței este necesară în ceea ce privește prelucrarea datelor în conformitate cu Directiva (UE) 2016/680, aceste linii directoare se aplică, de asemenea, interpretării acestui principiu. Cerințele de transparență din Regulamentul General privind Protecția Datelor se aplică indiferent de temeiul juridic al prelucrării și pe întreaga durată a acesteia. Acest lucru este clar din art. 12 care prevede că transparența se aplică în următoarele etape ale ciclului de prelucrare a datelor: (i) înainte sau la începutul ciclului de prelucrare a datelor, în cazul în care datele cu caracter personal sunt colectate fie de la persoana vizată, fie obținute în alt mod; (ii) pe parcursul întregii perioade de prelucrare, în cazul în care comunică cu persoanele vizate în legătură cu drepturile lor; și (iii) în anumite etape, în timp ce prelucrarea este în desfășurare, de exemplu atunci când apar încălcări ale securității datelor sau în cazul unor modificări semnificative ale prelucrării.

Comitetul Consultativ al Convenției 108 al Consiliului European

În anul 2017, au fost continuate discuțiile în contextul modernizării Convenției pentru protejerea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (T-PD), cunoscută sub denumirea de Convenția 108. Totodată, în urma reuniunilor Comitetului Consultativ al Convenției 108 al Consiliului European, a fost publicat Ghidul privind protecția persoanelor în legătură cu prelucrarea datelor cu caracter personal în contextul Big Data. Big Data reprezintă o nouă paradigmă în ceea ce privește modul în care datele sunt colectate, combinate și analizate. Big Data, care beneficiază de interacțiunea cu alte medii tehnologice, precum Internetul Lucrurilor și cloud computing, poate reprezenta o sursă de inovație pentru societate.



În același timp, deoarece Big Data permite colectarea și analizarea unui volum mare de date pentru a identifica și prezice comportamentul grupurilor și comunităților, trebuie luată în considerare și dimensiunea colectivă a riscurilor asociate utilizării datelor. În acest context, Comitetul Consultativ al Convenției 108 a considerat ca fiind necesară elaborarea acestui ghid care oferă un cadru general în ceea ce privește implementarea de proceduri și măsuri adecvate pentru a asigura eficiența principiilor și dispozițiilor Convenției 108 în contextul Big Data. Acest document a fost elaborat luând în considerare principiile Convenției 108, ținând cont de procesul continuu de modernizare a acesteia, și se adresează în primul rând factorilor de decizie, operatorilor și persoanelor împuternicite de operator. Prin intermediul acestui ghid se recomandă operatorilor și persoanelor împuternicite de operator să implementeze măsuri pentru a preveni impactul negativ al utilizării Big Data asupra demnității umane, drepturilor omului și libertăților fundamentale, în special în ceea ce privește protecția datelor cu caracter personal.

De asemenea, Comitetul Consultativ al Convenției 108 a publicat proiectul de Ghid practic privind utilizarea datelor cu caracter personal în sectorul polițienesc. Documentul subliniază cele mai importante aspecte care pot apărea în utilizarea datelor cu caracter personal în sectorul polițienesc, dar și elementele cheie care trebuie luate în considerare în acest context. Acest ghid nu repetă prevederile Convenției 108 și nici pe cele ale Recomandării (87) 15, ci se axează pe îndrumări practice. Principiile explicate în acest document se aplică prelucrării datelor cu caracter personal în scopul prevenirii, cercetării și urmăririi penale a infracțiunilor, al executării pedepselor. Trebuie subliniat faptul că acest ghid intenționează să ofere orientări pentru situația practică cu care poliția se poate confrunta în cadrul operațiunilor sale zilnice și recunoaște faptul că pentru autoritățile de aplicare a legii colectarea și utilizarea legală a datelor cu caracter personal sunt esențiale în interesul securității naționale și al prevenirii infracționalității sau menținerii ordinii publice.

În ceea ce privește aderarea la Convenția 108, au fost primite solicitări de aderare din partea Republicii Argentina și a Statelor Unite Mexicane. Referitor la Republica Argentina, Comitetul Consultativ al Convenției 108 a considerat că legea națională referitoare la protecția datelor cu caracter personal respectă pe deplin prevederile Convenției 108. Prin urmare, pe baza analizei legislației aplicabile privind protecția datelor, Comitetul Consultativ al Convenției 108 a decis ca cererea Republicii Argentina de a fi invitată să adere la Convenția 108 să primească un răspuns favorabil. Astfel, Comitetul Consultativ al Convenției 108 recomandă, de

asemenea, ca Republica Argentina să fie invitată să adere la protocolul adițional. Față de solicitarea Statelor Unite Mexicane, Comitetul Consultativ al Convenției 108 consideră că dispozițiile legale naționale privind protecția datelor din Statele Unite Mexicane respectă, în general, principiile Convenției 108 și ale Protocolului său adițional. Comitetul Consultativ al Convenției 108 constată că sunt binevenite unele ajustări ale dispozițiilor legale. Pe baza analizei legislației aplicabile privind protecția datelor, Comitetul Consultativ al Convenției 108 a considerat că trebuie să se răspundă favorabil solicitării Statelor Unite Mexicane de a fi invitate să adere la Convenția 108 și la protocolul adițional.

Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II, Grupul de coordonare comună Eurodac și Consiliul de Cooperare Europol

Grupul de coordonare comună VIS a adoptat un chestionar privind implementarea art. 41 din Regulamentul VIS pentru a evalua punerea în aplicare a obligației autorităților de supraveghere de a efectua un audit independent cel puțin o dată la patru ani pentru a verifica legalitatea operațiunilor de prelucrare a datelor cu caracter personal înregistrate în sistemele VIS naționale. Una din constatările principale evidențiate în raportul redactat pe baza răspunsurilor primite este aceea că majoritatea statelor membre au efectuat deja auditul prevăzut la art. 41 sau acesta se află în curs de desfășurare. Metodologia cea mai frecvent utilizată de autoritățile pentru protecția datelor pentru realizarea auditului este aceea de investigație la fața locului. În plus, toate autoritățile de supraveghere au subliniat faptul că nu au primit nici resurse financiare, nici resurse umane suplimentare.

Referitor la activitatea în legătură cu Sistemul de Informații Schengen, în anul 2017, Grupul de coordonare comună SIS II a adoptat și a transmis către Președinția Parlamentului UE adresa ce exprimă poziția grupului față de pachetul legislativ cu privire la Sistemul de Informații Schengen. Astfel, prin acest document, Grupul de Coordonare Comună SIS II sprijină argumentele prezentate de Autoritatea Europeană privind Protecția Datelor prin Opinia sa nr. 7/2017 și subliniază aspectele care trebuie luate în considerare în cadrul viitoarelor tratative ce vor avea loc pe marginea pachetului legislativ SIS, respectiv:

- pregătirea unei analize prealabile cu privire la necesitatea introducerii noulor identificatori biometrici (imaginea facială, amprenta palmelor și profilele ADN),
- o mai bună definire a drepturilor și regulilor de access pentru Frontex,

➤ justificarea necesității extinderii perioadei de reținere a alertelor cu privire la persoane, de la 3 la 5 ani,

➤ introducerea posibilității pentru Biroul SIRENE de a șterge alertele cu privire la obiecte, după îndeplinirea scopului,

➤ desfășurarea de campanii de informare regulate în vederea creșterii conștientizării persoanelor vizate.

Drepturile persoanelor vizate reprezintă un element esențial pentru protecția datelor cu caracter personal, întrucât acestea permit un control al persoanelor fizice asupra prelucrării datelor lor cu caracter personal. În acest context, simplul fapt că se asigură persoanelor vizate accesul la datele personale proprii, într-un mod eficient, precum și corectarea sau ștergerea respectivelor informații personale poate constitui un sprijin pentru descoperirea prelucrărilor ilegale de date cu caracter personal și pentru creșterea calității datelor în ceea ce privește prelucrările legale efectuate de operatorul de date. Aceste considerații sunt cu atât mai relevante în privința cererilor de azil, având în vedere consecințele negative ale prelucrării ilegale sau eronate a datelor cu caracter personal asupra solicitanților de azil.

Grupul de Coordonare Comună Eurodac a investigat și în anii anteriori exercitarea drepturilor persoanelor vizate. În acest context, a adoptat un raport privind pregătirea națională pentru punerea în aplicare a reformei Eurodac, document ce a inclus mai multe întrebări referitoare la drepturile persoanelor vizate.

Având în vedere importanța problematicii drepturilor persoanelor vizate, Grupul de Coordonare Comună Eurodac a decis continuarea verificării modului în care drepturile persoanelor vizate sunt puse în aplicare, prin redactarea unui chestionar elaborat pe baza chestionarelor anterioare și a planului standard de inspecție în domeniul Eurodac.

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 (Regulamentul Eurocol) a fost adoptat în data de 11 mai 2016 și a devenit aplicabil începând cu data de 1 mai 2017. De la această dată, Autoritatea Europeană privind Protecția Datelor (AEPD) a înlocuit Organismul Comun de Supraveghere în calitate de autoritate competentă pentru monitorizarea legalității prelucrării datelor cu caracter personal efectuate de Eurocol, în timp ce competența autorităților naționale pentru protecția datelor a rămas neschimbată. Un aspect esențial al supravegherii legalității prelucrării datelor efectuate de Eurocol îl reprezintă cooperarea



autorităților naționale de supraveghere cu Autoritatea Europeană privind Protecția Datelor, în special în cadrul nou-înființatului Consiliu de Cooperare Europol, un forum cu funcții consultative pentru discutarea problemelor comune, care colaborează pentru a elabora, de exemplu, avize, ghiduri, recomandări și bune practici, pentru a analiza dificultățile de interpretare sau aplicare a Regulamentului Europol. Astfel, în anul 2017 a avut loc prima reuniune a Consiliului de Cooperare Europol, în cadrul căreia au fost adoptate Regulile de procedură prin care se stabilesc competențele acestui forum, atribuțiile președintelui Consiliului de Cooperare, metodele de lucru în cadrul forului.

Grupul Internațional de lucru pentru Protecția Datelor în domeniul Telecomunicațiilor

În cadrul reuniunilor Grupului Internațional de lucru pentru Protecția Datelor în domeniul Telecomunicațiilor, discuțiile s-au axat și în anul 2017 pe temele privind viața privată referitor la platformele de e-learning, aspecte privind viața privată cu privire la datele din registrul WHOIS, ICANN, inteligența artificială, viața privată și standardizarea internațională.

Discuțiile s-au concretizat prin adoptarea documentului de lucru privind viața privată pe platformele de tip e-learning, a documentului de lucru privind principiile sau instrumentele internaționale pentru colectarea informațiilor guvernamentale și a documentului de lucru referitor la aspecte privind viața privată în legătură cu datele din registrul WHOIS, ICANN.

Utilizarea platformelor de tip e-learning, care devine tot mai populară în numeroase state, conduce la creșterea numărului de date personale digitalizate generate de elevi și de comportamentul și performanța acestora. În plus, datele digitalizate detaliate despre elevi și studenți pot determina cererea de utilizare sporită a datelor în cadrul educației, inclusiv utilizarea așa-numitelor „analize de învățare”.

Această evoluție poate duce la o lipsă de transparență dacă părinții și studenții nu au acces la datele utilizate pentru a lua decizii și la procesul de luare a deciziilor. Mai mult decât atât, riscul ca societățile private care colectează date pe astfel de platforme să le folosească și dincolo de obiectivul academic este evident. În afară de scopurile evidente de marketing, astfel de date ar putea fi folosite chiar și pentru a lua decizii în lumea reală în legătură cu viitoarele oportunități ale studenților, inclusiv privind ocuparea forței de muncă, locuințele și creditele.

Documentul de lucru privind platformele de e-learning descrie și alte riscuri asociate acestor platforme în ceea ce privește confidențialitatea datelor. De asemenea, materialul oferă



recomandări instituțiilor de învățământ, furnizorilor de platforme de e-learning și autorităților pentru protecția datelor.

În ceea ce privește principiile sau instrumentele internaționale pentru guvernarea colectării inteligente, în ultimii ani a existat o creștere a gradului de conștientizare publică, precum și discuții în legătură cu interesul statelor cu privire la securitatea națională și drepturile persoanelor la viața privată.

Documentul de lucru intitulat „Către principii internaționale sau instrumente pentru colectarea informațiilor guvernamentale” subliniază recentele solicitări de consens privind standardele internaționale în acest domeniu și oferă recomandări autorităților pentru protecția datelor care contribuie la elaborarea unor noi principii.

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

În anul 2017, discuțiile din cadrul Grupului de Lucru PCC SEE s-au axat pe proiectul de Acord de implementare privind protecția datelor referitor la Convenția de Cooperare Polițienească în Europa de Sud-Est (PCC SEE). În acest context, au fost formulate o serie de observații și recomandări menite să aducă mai multă claritate documentului. Având în vedere contribuția importantă a reprezentantului Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal la elaborarea proiectului de Acord de implementare, Secretariatul PCC SEE a propus ca partea română să își asume rolul de raportor al unui subgrup, format din experți ai Grupului de Lucru PCC SEE privind protecția datelor – reprezentanți ai autorităților naționale pentru protecția datelor și ai poliției, precum și experți în elaborarea acordurilor internaționale, care va defini Acordul de implementare privind protecția datelor referitor la Convenția de Cooperare Polițienească în Europa de Sud-Est.

A 38^a Conferință Internațională a Comisarilor din domeniul Protecției Datelor și a Vieții Private

În anul 2017, cea de-a 39^a Conferință Internațională a Comisarilor din domeniul Protecției Datelor și a Vieții Private a fost organizată de Autoritatea pentru protecția datelor din Hong Kong. În cadrul conferinței au fost adoptate 3 rezoluții:

- rezoluția privind protecția datelor în legătură cu vehiculele automatizate și conectate
- prin care se face apel la toate părțile relevante implicate să respecte pe deplin drepturile

utilizatorilor cu privire la protecția datelor cu caracter personal și a vieții private și să abțin vederea aceste drepturi în cadrul fiecărei etape de creare și/sau dezvoltare de noi dispozitive sau servicii;

- rezoluția privind cooperarea dintre autoritățile pentru protecția datelor și autoritățile pentru protecția consumatorilor pentru o mai bună protecție a cetățenilor și consumatorilor într-o economie digitală – document prin care se subliniază necesitatea identificării unor modalități de îmbunătățire a colaborării la nivel internațional între autoritățile pentru protecția datelor și autoritățile pentru protecția consumatorilor în scopul asigurării unei mai bune protecții cetățenilor și consumatorilor într-o economie digitală;
- rezoluția privind explorarea viitoarelor opțiuni de cooperare internațională pentru o aplicare consolidată a prevederilor legale în domeniul protecției datelor cu caracter personal.

Conferința de primăvară a autorităților europene pentru protecția datelor

În anul 2017, Conferința de primăvară a autorităților europene pentru protecția datelor cu caracter personal a fost organizată de autoritatea pentru protecția datelor din Cipru. Subiectele dezbătute au vizat aspecte precum:

- noul regim juridic în domeniul protecției datelor cu caracter personal,
- activitatea de conștientizare/informare – apropierea dintre autoritățile pentru protecția datelor, companii și publicul larg,
- asigurarea transparenței și respectarea principiului responsabilității în mediile de stocare virtuale,
- accesul autorităților de aplicare a legii la datele cu caracter personal – sisteme la scară largă, interoperabilitate și fluxuri transfrontaliere de date cu caracter personal,
- bazele de date ADN – provocări pentru viața privată.

În cadrul conferinței au fost adoptate 2 rezoluții: rezoluția privind modernizarea Convenției pentru protecția persoanelor fizice cu privire la prelucrarea automată a datelor cu caracter personal și rezoluția privind regulile și procedurile aferente Conferinței Autorității Europene pentru Protecția Datelor.

Misiuni de evaluare Schengen

O parte însemnată a activității Autorității naționale de supraveghere în plan extern, în cursul anului 2017, a constituit participarea instituției noastre la misiunile de evaluare Schengen în domeniul protecției datelor din Islanda și Portugalia.

Misiunile Schengen se referă la evaluarea și monitorizarea aplicării *acquis-ului* Schengen, respectiv analiza modulului 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 fiecărei misiuni de evaluare se întocmește un raport pe baza răspunsurilor transmise de statul evaluat la chestionarul standard¹ și a informațiilor furnizate de autoritățile statului respectiv pe durata vizitei de evaluare. Acest document conține, printre altele, constatări și evaluări privind legislația, autoritatea pentru protecția datelor, drepturile persoanelor vizate, cooperarea internațională.

Sistemul de Informații Schengen de a doua generație (SIS II)

În decembrie 2016, Comisia Europeană a lansat un pachet legislativ de revizuire a cadrului legal în domeniul Sistemului de Informații Schengen de a doua generație (SIS II), compus din 3 propuneri de regulament care modifică baza legală la nivel european în ceea ce privește funcționarea SIS II, respectiv:

- propunerea de regulament privind returnarea resortisanților țărilor terțe aflați în situație de sedere ilegală,
- propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul controalelor la frontieră, modificarea Regulamentului (UE) 515/2014 și abrogarea Regulamentului (CE) 1987/2006,
- propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și judiciare în materie penală, modificarea Regulamentului (UE) 515/2014 și abrogarea Regulamentului (CE) 1986/2006, a Deciziei Consiliului 533/2007, a Deciziei Comisiei 261/2010.

¹ 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



Propunerea de regulament privind returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală dezvoltă și îmbunătățește sistemul existent. Aceasta extinde domeniul de aplicare al actualului SIS prin introducerea unei noi categorii de alertă pentru deciziile de returnare. Impactul său asupra drepturilor fundamentale este, prin urmare, limitat, deoarece funcționarea solidă a sistemului a fost deja dovedită și au fost deja puse în aplicare garanții importante și eficiente. Cu toate acestea, deoarece propunerea implică prelucrarea datelor cu caracter personal, există un posibil impact asupra drepturilor fundamentale ale unei persoane fizice. Acest lucru a fost luat în considerare și au fost instituite garanții pentru a se respecta principiile enunțate în Carta drepturilor fundamentale a Uniunii Europene.

Față de propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul controalelor la frontieră, cadrul juridic actual al SIS II referitor la utilizarea acestuia în scopul controalelor la frontiere ale resortisanților țărilor terțe se bazează pe un instrument al fostului pilon 1, și anume Regulamentul (CE) nr. 1987/2006. Această propunere înlocuiește cadrul legal existent pentru:

- a obliga statele membre să introducă o alertă în SIS în toate cazurile în care a fost emisă o interdicție de intrare unui resortisant al unei țări terțe aflat în situație de ședere ilegală, în conformitate cu dispozițiile care respectă Directiva 2008/115/CE;
- a armoniza procedurile naționale de utilizare a SIS în legătură cu procedura de consultare pentru a evita ca un resortisant al unei țări terțe care face obiectul unei interdicții de intrare să dețină un permis de ședere valabil emis de un stat membru;
- a introduce modificări tehnice în vederea îmbunătățirii securității și pentru a contribui la reducerea sarcinilor administrative;

- a aborda utilizarea completă a SIS, acoperind nu numai sistemele centrale și naționale, ci și necesitățile utilizatorului final prin asigurarea faptului că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile și a respecta toate cerințele de securitate atunci când prelucrează datele SIS.

Această propunere dezvoltă și îmbunătățește un sistem existent, în loc să stabilească unul nou și, prin urmare, se bazează pe garanții importante și eficiente care au fost deja puse în aplicare. Cu toate acestea, întrucât sistemul continuă să prelucreze date cu caracter personal și va prelucra alte categorii de date biometrice sensibile, există un posibil impact asupra drepturilor fundamentale ale unei persoane fizice. Aceste aspecte au fost luate în considerare



cu atenție și au fost instituite măsuri de protecție suplimentare pentru a se limita colectarea și prelucrarea ulterioară a datelor la ceea ce este strict necesar din punct de vedere operațional.

În ceea ce privește propunerea de regulament pentru înființarea, funcționarea și utilizarea SIS în domeniul cooperării polițienești și judiciare în materie penală, cadrul juridic actual al SIS II referitor la utilizarea sa în scopul cooperării polițienești și judiciare în materie penală se bazează pe un instrument al fostului pilon 3, și anume Decizia 2007/533/JAI a Consiliului și pe fostul pilon 1, respectiv Regulamentul (CE) 1986/2006.

Această propunere consolidează conținutul instrumentelor existente adăugând în același timp noi dispoziții pentru a:

- armoniza mai bine procedurile naționale de utilizare a SIS, în special în ceea ce privește infracțiunile legate de terorism, precum și copiii expuși riscului de răpire de către părinți;

- extinde domeniul de aplicare al SIS prin introducerea de noi elemente de identificare biometrică în alertele existente;

- introduce modificări tehnice în vederea îmbunătățirii securității și pentru a contribui la reducerea sarcinii administrative prin furnizarea copiilor naționale obligatorii și a standardelor tehnice comune de punere în aplicare;

- aborda utilizarea completă a SIS, acoperind sistemele centrale și naționale, cu asigurarea că utilizatorii finali primesc toate datele necesare pentru a-și îndeplini sarcinile și a respecta toate normele de securitate atunci când prelucrează datele SIS.

Deoarece SIS II va continua să prelucreze date cu caracter personal, precum și alte categorii de date cu caracter special, respectiv date biometrice, ar putea exista un impact asupra drepturilor fundamentale ale persoanelor fizice ale căror date sunt prelucrate. În acest sens, au fost implementate măsuri suplimentare de protecție pentru a se limita colectarea și prelucrarea ulterioară a datelor cu caracter personal. În plus, propunerea consolidează măsurile de protecție a drepturilor fundamentale, deoarece stabilește în legislație cerințele pentru care trebuie ștearsă o alertă și introduce o evaluare a proporționalității în cazul în care se prelungeste perioada de valabilitate a unei alerte.

Față de cele 3 propuneri de regulament ce fac parte din pachetul legislativ de revizuire a cadrului legal în domeniul Sistemului de Informații Schengen de a doua generație (SIS II), Autoritatea națională de supraveghere a formulat o serie de observații și propuneri, în special cu referire la drepturile persoanelor vizate ale căror date cu caracter personal sunt prelucrate.

Revizuirea Regulamentului (CE) 45/2001

Dreptul la protecția datelor cu caracter personal se aplică și prelucrării datelor cu caracter personal efectuate de instituțiile, organismele, officele și agențiile UE. În 2001 a fost adoptat Regulamentul (CE) nr. 45/2001, principala parte a legislației UE privind protecția datelor cu caracter personal în cadrul instituțiilor Uniunii Europene, având în vedere două obiective: protejerea dreptului fundamental la protecția datelor și garantarea liberei circulații a datelor cu caracter personal în întreaga Uniune Europeană.

În aprilie 2016, Parlamentul European și Consiliul au adoptat Regulamentul General privind Protecția Datelor, care va deveni aplicabil începând cu data de 25 mai 2018. Regulamentul General privind Protecția Datelor cere ca Regulamentul (CE) 45/2001 să fie adaptat la principiile și normele stabilite în Regulamentul General privind Protecția Datelor, pentru a asigura un cadru solid și coerent de protecție a datelor în Uniune și pentru a permite ca ambele instrumente să fie aplicabile în același timp.

Propunerea de regulament este în concordanță cu abordarea coerentă a protecției datelor cu caracter personal în întreaga Uniune pentru a alinia, în măsura posibilităților, normele de protecție a datelor pentru instituțiile, organismele, officele și agențiile Uniunii Europene la normele de protecție a datelor adoptate pentru statele membre.

Sistemul european de informații și de autorizare privind călătoriile (European

Travel Information and Authorisation System – ETIAS)

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, care 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 exonerate 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.

Propunerea de regulamentul are un impact asupra drepturilor fundamentale, în special asupra dreptului la demnitate, la libertate și securitate, la respectarea vieții private și familiale,

la protecția datelor cu caracter personal, la azil și la protecția în caz de îndepărtare, expulzare sau extrădare, la nediscriminare, asupra drepturilor copilului, precum și asupra dreptului la o cale de atac eficientă.

Interesul public legitim legat de asigurarea unui nivel ridicat de securitate este afectat în mod pozitiv de punerea în aplicare a unui sistem de tip ETIAS. O mai bună și mai precisă identificare a riscului de securitate în cazul resortisanților țărilor terțe aflați în afara regimului de vize, care traversează frontiera externă a spațiului Schengen, sprijină detectarea traficului de ființe umane (în special în cazul minorilor) și a criminalității transfrontaliere și, în general, facilitează identificarea persoanelor a căror prezență în spațiul Schengen ar reprezenta o amenințare la adresa securității. Prin urmare, ETIAS contribuie la îmbunătățirea securității cetățenilor prezenți în spațiul Schengen și la consolidarea securității interne în UE.

Față de propunerea de regulament ce va institui sistemul ETIAS, Autoritatea națională de supraveghere a formulat o serie de observații și propuneri, în special cu referire la drepturile persoanelor vizate ale căror date cu caracter personal sunt prelucrate.

Conferințe, seminarii și alte reuniuni privind aplicarea Regulamentului

General privind Protecția Datelor

Pe parcursul anului 2017, reprezentanții Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal au participat la o serie de evenimente dedicate cadrului legal în domeniul protecției datelor și noutăților aduse de Regulamentul General privind Protecția Datelor.

În cadrul evenimentelor privind aplicarea Regulamentului General privind Protecția Datelor, participanții au fost informați în legătură cu impactul noii reglementări la nivel european, precum și cu obligațiile ce le revin potrivit Regulamentului General privind Protecția Datelor, cum ar fi desemnarea unui responsabil cu protecția datelor, notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal, efectuarea evaluării impactului asupra protecției datelor în situația în care prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, păstrarea evidenței activității de prelucrare desfășurate și, nu în ultimul rând, asigurarea securității datelor cu caracter personal.



CAPITOLUL VI

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRIILOR DE DATE CU CARACTER PERSONAL

În anul 2017, Autoritatea națională de supraveghere a soluționat **6.437** solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări și cereri prin care se solicita punctul de vedere sau clarificarea unor aspecte privind prelucrările de date cu caracter personal efectuate.

Au fost soluționate **6.115** notificări privind prelucrări de date cu caracter personal, dintre care **4795** efectuate pe teritoriul României și **1320** transferuri de date către state din Uniunea Europeană, Zona Economică Europeană și state terțe.

Din cele **1320** notificări cu transferuri de date către entități din străinătate, în **1030** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terțe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entități care au aderat la principiile Privacy Shield).

Totodată, au fost notificate **290** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, în baza contractelor cu clauze standard și a regulilor corporatiste obligatorii (Binding Corporate Rules).

În urma analizării transferurilor de date în străinătate către state terțe, a fost emis un număr de **74** autorizații de transfer.

În același timp, au fost analizate **322** solicitări ale operatorilor privind aspecte referitoare la dispozițiile Legii nr. 677/2001, modificată și completată.

Secțiunea 1- Activitatea de înregistrare a prelucrărilor de date

Potrivit prevederilor Deciziei nr. 200/2015, emisă în temeiul art. 22 alin. (9) din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, modificată și completată, notificarea Autorității naționale de supraveghere nu mai este necesară, cu excepția cazurilor enumerate la art. 1 alin. (1) din Decizia nr. 200/2015.



La elaborarea acestui act normativ s-au luat în considerare prevederile 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 referitoare la eliminarea obligației operatorilor de a notifica autoritățile naționale de supraveghere pentru prelucrările de date efectuate.

Deși, prin Decizia președintelui Autorității naționale de supraveghere au fost reglementate expres cazurile pentru care este necesară notificarea autorității, reprezentanții unor autorități și instituții publice au emis, contrar prevederilor deciziei susmenționate, acte normative prin care au stabilit obligația pentru operatorii din diferite domenii de activitate de a notifica Autoritatea națională de supraveghere pentru prelucrările de date care nu intrau sub incidența dispozițiilor Deciziei nr. 200/2015.

Dintre acestea, precizăm:

- Ordinul nr. 4/2017 emis de președintele Autorității Naționale pentru Protecția Consumatorului privind documentația și informațiile necesare înregistrării, precum și modalitatea și termenele de raportare pentru dezvoltorii imobiliari, care a stabilit obligația acestora de a face dovada că sunt operatorii de date cu caracter personal;
- Ordinul nr. 1/2017 emis de președintele Autorității Naționale pentru Protecția Consumatorului privind documentația și informațiile necesare înregistrării, precum și modalitatea și termenele de raportare pentru entitățile de recuperare creanțe, care a stabilit obligația acestora de a face dovada că sunt operatorii de date cu caracter personal;
- Ordinul nr. 2632/2016 pentru dezvoltarea serviciilor Ministerului Finanțelor Publice puse la dispoziția autorităților și instituțiilor publice prin sistemul informatic propriu, emis de Ministrul Finanțelor Publice, prin care s-a stabilit obligația autorităților/instituțiilor publice de a se înregistra ca operatorii de date cu caracter personal;
- Ordonanța de urgență a Guvernului nr. 52/2016 privind contractele de credit oferite consumatorilor pentru bunuri imobile, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 50/2010 privind contractele de credit pentru consumatori, prin care s-a stabilit obligația intermediarilor de credite de a se înregistra ca operatorii de date cu caracter personal.

Având în vedere prevederile actelor normative menționate mai sus cu referire la obligația entităților din diferite sectoare de activitate de a se înregistra ca operatori de date cu caracter personal, Autoritatea națională de supraveghere a întreprins o serie de demersuri în vederea modificării acestor dispoziții legale, în sensul eliminării acestei obligații.

Totodată, furnizorii de asistență medicală, respectiv cabinetele medicale ambulatorii ale medicilor de familie și de alte specialități, centrele de diagnostic și tratament, centrele medicale, centrele de sănătate, laboratoarele, precum și alte unități sanitare publice și private, care își desfășoară activitatea curentă în baza Legii nr. 95/2006 privind reforma în domeniul sănătății, republicată, au notificat Autoritatea națională de supraveghere cu privire la prelucrările de date efectuate în scopul furnizării serviciilor de sănătate.

În aceste cazuri, Autoritatea națională de supraveghere a supus atenției Ministerului Sănătății propunerea de a se dispune luarea măsurilor necesare în vederea asigurării informării furnizorilor de asistență medicală cu privire la scutirea de la obligația de notificare, conform prevederilor Deciziei nr. 200/2015, coroborate cu cele ale Legii nr. 95/2006 privind reforma în domeniul sănătății, republicată.

În plus, operatorii de date care își desfășoară activitatea în domeniul turismului, imobiliilor, hotelier, precum și entități care desfășoară o activitate independentă (bucouri notariale, birouri de executori judecătorești, societăți de avocatură, cabinete medicale individuale) au notificat Autorității naționale de supraveghere prelucrările pe care le efectuează în scopul îndeplinirii atribuțiilor lor legale.

Autoritatea națională de supraveghere a informat aceste entități că au calitatea de operator și, implicit, obligația de a respecta legislația din domeniul protecției datelor, în special cu privire la dispozițiile art. 12, 19 și 20 din Legea nr. 677/2001, modificată și completată, însă sunt scutite de obligația de a notifica.

Scutirea de obligația de a notifica Autoritatea națională de supraveghere nu exonerează, însă, operatorii de îndeplinirea celorlalte obligații care le revin potrivit dispozițiilor legale aplicabile în domeniul protecției datelor cu caracter personal (ex.: informarea persoanelor vizate în condițiile reglementate de art. 12 din Legea nr. 677/2001 și adoptarea unor măsuri adecvate pentru asigurarea securității prelucrării datelor conform prevederilor art. 20 alin. 1 din același act normativ și cerințelor minime aprobate prin Ordinul nr. 52/2002).

Sub incidența prevederilor Deciziei nr. 200/2015, Autoritatea națională de supraveghere a înregistrat în registrul de evidență 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 și/sau bunurilor publice/private prin utilizarea GPS-ului);
- prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea și/sau evaluarea unor aspecte de personalitate, precum competența profesională, credibilitatea, comportamentul sau alte asemenea (crearea și utilizarea de profileuri ale persoanelor vizate în vederea transmiterii unor newsletteruri, semnalaarea 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 școlare și extrășcolare, postarea unor imagini din tabere școlare);
- prelucrarea datelor efectuată prin mijloace de supraveghere video în scopul monitorizării/securității persoanelor, spațiilor și/sau bunurilor publice/private.

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

- verificarea condițiilor de prelucrare a datelor biometrice și genetice ale angajaților unei societăți în scopul monitorizării accesului în incinta acestei entități;
- verificarea condițiilor în care se efectuează prelucrarea datelor cu caracter personal în scopul "ținerii evidenței orelor de muncă prestate de fiecare angajat (realizarea pontajelor), prin utilizarea unui sistem de control acces cu recunoaștere facială;
- controlul legitimității prelucrării datelor biometrice în scopul „resurselor umane”, respectiv „realizarea unui pontaj biometric”;
- verificarea condițiilor de funcționare a unei aplicații mobile de geolocalizare și închiriere biciclete, a necesității folosirii datelor referitoare la contul de Facebook și a celor privind locul de muncă, precum și a necesității păstrării datelor de geolocalizare după închiderea aplicației;

- verificarea condițiilor de prelucrare a datelor biometrice în scopul „îmbunătățirii și evaluării performanțelor algoritmilor biometrici”;
- verificarea condițiilor în care se efectuează monitorizarea video a angajaților în spațiile în care își desfășoară activitatea;
- verificarea legitimității prelucrării datelor de către o asociație de proprietari în vederea supravegherii video, în special în lifturi;
- controlul legitimității prelucrării datelor clienților, consumatorilor și debitorilor, în scopul efectuării unor rapoarte de credit, prin intermediul unui registru al facturilor neincasate;
- verificarea modalității de prelucrare a datelor cu caracter personal efectuate în scopul „implementării unui sistem de autentificare pentru autorizarea plăților bazat pe recunoașterea amprentelor digitale prin intermediul cititorului biometric”;
- controlul respectării dreptului de acces al persoanelor vizate de către o instituție publică.

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

Din cele **1320** notificări cu transferuri de date către entități din străinătate, în **1030** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terțe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entități care au aderat la principiile Privacy Shield), precum și transferuri către state terțe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată și completată.

Totodată, au fost notificate **290** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată și completată, în baza contractelor cu clauze standard și a regulilor corporatiste obligatorii (Binding Corporate Rules).

Numar notificari transfer date în
străinatate

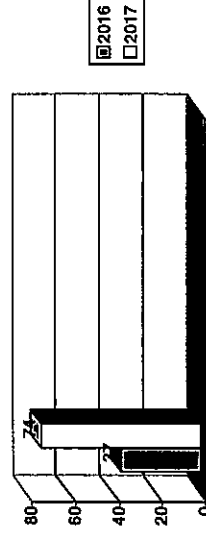


În anul 2017, dintre domeniile care au vizat transferurile de date către state terțe, efectuate în baza prevederilor art. 29 alin. 4 din Legea nr. 677/2001, modificată și completată, respectiv efectuate în baza clauzelor contractuale standard și a regulilor corporatiste obligatorii, menționăm următoarele:

- gestiune economico-financiară și administrativă, respectiv calculul rentabilității clientului, facturarea, condițiile de plată, gestionarea și raportarea de management, inclusiv raportarea și punerea în aplicare a programelor corporative, raportare financiară;
- suport cu privire la tehnologia informației și securitatea informației;
- gestionare date în domeniul farmacovigilenței;
- asigurarea conformității respectării normelor, aplicarea uniformă a regulamentelor, soluționarea sesizărilor de tip compliance formulate de orice persoană interesată cu privire la fapte de încălcare a legii, săvârșirea infracțiunilor de corupție, infracțiunilor de serviciu, abateri disciplinare, contravenții;
- resurse umane, recrutarea, evaluarea și promovarea personalului, dezvoltarea personală a angajaților, gestionarea trainingului și a formării profesionale a angajaților, a potențialilor angajați și a colaboratorilor;
- activități comerciale, realizarea de proiecte și comenzi de la clienți, achiziționarea de bunuri și servicii de la furnizori, comunicare internă, cooperare la scară globală.

În urma analizării transferurilor de date în străinătate către state terțe, a fost emis un număr de 74 de autorizații de transfer.

Numar autorizatii



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

În cursul anului 2017, au fost analizate **322** solicitări ale operatorilor privind aspecte referitoare la dispozițiile Legii nr. 677/2001, modificată și completată, precum și la prevederile Deciziei nr. 200/2015.

În același timp, au fost înregistrate numeroase solicitări referitoare la necesitatea desemnării unui responsabil cu protecția datelor, precum și la sarcinile pe care acesta trebuie să le îndeplinească potrivit prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulația a acestor date și de abrogare a Directivei 95/46/CE.

Prezentăm mai jos o serie de spețe semnificative supuse spre analiză Autorității naționale de supraveghere:

1) Președintele unei asociații de proprietari a solicitat punctul de vedere cu privire la necesitatea obținerii consimțământului tuturor proprietarilor dintr-un condominiu pentru supravegherea video a exteriorului clădirilor, curții interioare, spațiilor de parcare și aleii de acces.

S-a apreciat că se poate recurge la o monitorizare prin videosupraveghere numai dacă această măsură este proporțională cu riscurile cu care se confruntă asociația de proprietari și determină luarea unei asemenea măsuri. În același timp, s-a precizat faptul că trebuie să se țină cont și de interesele, drepturile și libertățile persoanelor vizate.

Astfel, anterior implementării unui astfel de sistem de supraveghere prin camere video se impune o justificare temeinică a luării acestei măsuri (inclusiv sub aspectul numărului de camere și al poziționării acestora), pentru motivarea interesului legitim al asociației față de drepturile și libertățile fundamentale sau interesele proprietarilor. Această analiză și argumentare trebuie să se regăsească în conținutul actelor asociației emise în urma adunării generale a proprietarilor, realizată în condițiile Legii nr. 230/2007 privind înființarea, organizarea și funcționarea asociațiilor de proprietari, în special cele privind atribuțiile Adunării generale a proprietarilor și ale Comitetului Executiv (art. 27-30).

Regulile stabilite prin Normele metodologice de aplicare a Legii nr. 230/2007, referitoare la convocarea adunării generale, informarea prealabilă a proprietarilor, condițiile de organizare

a adunării generale și de cvorum/majoritate pentru adoptarea hotărârilor trebuie respectate de asociația de proprietari pentru ca hotărârea instalării sistemului de supraveghere video să fie adoptată legal (constitute dovezi ale convocării și reconvoacării afșur de la avizier și tabelul nominal convocator cu semnătură). Hotărârile adunării generale a asociației de proprietari trebuie aduse la cunoștința proprietarilor, conform Legii nr. 230/2007. Persoanele care nu sunt de acord cu hotărârea adoptată, o pot contesta în termenele și condițiile legale.

2) O societate comercială a solicitat opinia Autorității naționale de supraveghere în ceea ce privește *implementarea unui sistem de acces în sediu al angajaților pe bază de amprentă digitală*.

În acest sens, s-a precizat că amprentele digitale sunt o categorie de date cu caracter special, întrucât ele privesc caracteristicile fizice/fiziologice ale persoanelor și pot conduce la identificarea acestora.

Totodată, s-a menționat că potrivit dispozițiilor art. 4 alin. (1) din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credință și în conformitate cu dispozițiile legale în vigoare, colectate în scopuri determinate, explicite și legitime, cu respectarea dispozițiilor în vigoare. De asemenea, datele colectate trebuie să fie strict cele necesare îndeplinirii scopului, aspect ce solicită o analiză prealabilă a necesității imperioase a colectării amprentelor digitale, pentru evitarea unor ingerințe în viața privată a unei persoane, și găsirea unor soluții mai puțin intruzive.

În același timp, autoritatea a subliniat faptul 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.

Astfel, Autoritatea națională de supraveghere a recomandat folosirea unei soluții alternative la *sistemul de acces pe bază de amprentă digitală*.

Autoritatea națională de supraveghere a subliniat faptul că această abordare referitoare la prelucrarea datelor biometrice a fost confirmată și de instanțele de judecată.

3) Mai multe persoane juridice au solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la necesitatea declarării prin intermediul formularului de notificare a



transferului datelor cu caracter personal în Statele Unite ale Americii, ținând cont de prevederile Deciziei nr. 200/2015, precum și de Acordul UE-SUA Privacy Shield.

În contextul solicitărilor formulate, s-a menționat că în situația în care importatorul a aderat la principiile Privacy Shield nu este necesară notificarea autorității, întrucât sunt incidente dispozițiile art. 2 alin. (1) din Decizia nr. 200/2015, conform căreia vor face obiectul notificării Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal doar transferurile datelor cu caracter personal către statele situate în afara Uniunii Europene, a Zonei Economice Europene, precum și către statele cărora Comisia Europeană nu le-a recunoscut, prin Decizie, un nivel de protecție adecvat. În caz contrar, se impune identificarea altor garanții care să permită transferul datelor către entități din aceste state, în conformitate cu prevederile art. 29 sau 30 din Legea nr. 677/2001, modificată și completată.

4) O societate care prelucrează date cu caracter personal prin intermediul unor dispozitive mobile de geolocalizare a unor persoane fizice (pacienți cu Alzheimer sau alte forme de deficiență mintală, bătrâni singuri) pe baza unei aplicații mobile a solicitat informații cu privire la obligațiile ce-i revin în ceea ce privește prelucrarea datelor cu caracter personal. În plus, societatea menționată mai sus a precizat că datele referitoare la monitorizarea geolocației persoanelor vizate vor fi stocate pe servere în China.

În contextul celor prezentate, s-a apreciat că prelucrarea se circumscripte prevederilor art. 1 alin. (1) lit. c) din Decizia nr. 200/2015, iar notificarea Autorității naționale de supraveghere se impune dacă, prin intermediul aplicației, se realizează, direct sau indirect, localizarea geografică a persoanelor fizice care o utilizează.

Cât privește faptul că datele conținute în conturile private ale clienților contractanți vor fi stocate în China, s-a apreciat că se impune declararea prelucrării efectuate prin completarea formularului de notificare (inclusiv transferul datelor în China).

5) O societate civilă de avocatură a solicitat informații referitoare la condițiile în care pot fi prelucrate datele participanților la campanii publicitare cu acordarea de premii după încheierea acestora, în activități de marketing direct.

În acest context, s-a menționat că prelucrarea datelor personale în cadrul campaniilor publicitare se poate realiza cu consimțământul expres și neechivoc al persoanei vizate și cu informarea completă a acesteia, potrivit art. 12 din Legea nr. 677/2001. Informarea se poate



realiza atât prin intermediul regulamentului fiecărei campanii publicitare, cât și prin intermediul documentului de colectare a datelor personale.

În același timp, persoana vizată trebuie informată că, potrivit art. 15 alin. 2 din Legea nr. 677/2001, se poate opune oricând prelucrării datelor sale în activități de marketing direct, fără nici o justificare.

În consecință, prelucrarea datelor cu caracter personal ale participanților la o campanie publicitară, precum și prelucrarea ulterioară a acestor date în activități de marketing direct, se realizează doar cu respectarea prevederilor menționate mai sus.

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, în anul 2017, Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal i s-au alocat fonduri prin Legea bugetului de stat nr. 339/2017 și prin Ordonanțele Guvernului nr. 14 și nr. 86/2017 privind rectificarea bugetului de stat pe anul 2017, rezultând un buget final în sumă de 4.287.000 lei, cu următoarea structură:

- mii lei -

Denumire indicator	Cod	Buget inițial 2017	Buget actualizat la 31.12.2017	Sume cheltuite până la 31.12.2017	Execuție (%)
Total cheltuieli	51.01	4.585	4.287	4.280	99,84
Cheltuieli de personal	10	3.878	3.588	3.587	99,97
Bunuri și servicii	20	672	664	659	99,22
Alte cheltuieli	59	10	10	10	100
Cheltuieli de capital	71	25	25	24	97,31

Pentru că, pe parcursul exercițiului 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 privește modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorității Naționale de Supraveghere a constituit un procent de 84% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat

efectiv credite în valoare de 3.586.994 lei (prin ocuparea unor posturi temporar, prin delăsare), înregistrându-se în continuare un deficit major de personal (11 posturi neocupate, 5 posturi ocupate temporar prin delăsare, reprezentând 32% din numărul total de 50 de posturi – exclusiv demnitarii – prevăzute de Legea nr. 102/2005). Majoritatea cheltuielilor de personal au fost aferente plăgilor efectuate pentru achitarea drepturilor salariale ale angajaților din compartimentele de specialitate.

Cheltuielile aferente titlului Bunuri și servicii în anul 2017 au avut o pondere de 15,5% în bugetul instituției, iar din acestea, cheltuielile cu pondere mai importantă au fost:

- 33% costuri de închiriere și cheltuieli cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI
- 37% bunuri și servicii pentru întreținere și funcționare (curățenie, abonament program legislativ, servicii de actualizare informatică etc.)

Trebuie menționat faptul că Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal își realizează obiectul principal de activitate prin investigații și controale efectuate la operatorii situați pe teritoriul României, precum și la consulatele României.

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

În anul 2017, cheltuielile cu bunuri și servicii au scăzut cu 5% față de anul 2016, fapt cu un impact deosebit asupra activității instituției și cheltuielilor bugetare, fiind efectuate mai puțin de jumătate din cheltuielile privind deplasările externe estimate.

De asemenea, trebuie precizat și faptul că s-au avut permanent în vedere mai mulți factori – oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice, alăturat unor cerințe tehnice atent stabilite – ceea ce a condus la utilizarea eficientă a fondurilor bugetare alocate acestui titlu de cheltuieli.

În ceea ce privește cheltuielile de capital, în anul 2017, Autoritatea Națională de Supraveghere a continuat – în măsura posibilităților oferite de alocările bugetare – proiectul de reînnoire a infrastructurii IT, în acest scop fiind utilizate fondurile prevăzute în bugetul final al titlului Cheltuieli de capital.

Politicile contabile utilizate la înlocuirea situațiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare.



AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL



Situațiile financiare anuale oferă o imagine fidelă a realității poziției financiare a Autorității naționale de supraveghere, încadrarea în creditele bugetare alocate pe grupe, titluri, articole și alineate de cheltuieli, așa cum sunt prevăzute acestea în bugetul autorității.

Cheltuielile bugetare s-au efectuat cu respectarea principiilor privind legalitatea, oportunitatea, continuitatea și eficiența.

Toate documentele care intră sub incidența controlului financiar preventiv propriu sunt verificate și vizate.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, subliniem că acestea au fost utilizate cu maximă eficiență și printr-o atență administrare de către instituția noastră.

