AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

R A P O R T A N U A L

2018

Raportul de activitate este transmis Senatului României, Camerei Deputaţilor, Guvernului României, Comisiei Europene şi Comitetului European pentru Protecţia Datelor, în temeiul art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

Bucureşti

CUVÂNT ÎNAINTE

Stimate Domnule Preşedinte al Senatului,

Stimaţi Senatori,

Anul 2018 a reprezentat un moment de reformă în domeniul protecției datelor cu caracter personal, prin începerea aplicării efective, din data de 25 mai 2018, a Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor), adoptat pe data de 27 aprilie 2016, de către Parlamentul European și Consiliul.

Efectul adoptării acestei reglementări europene a constat în uniformizarea principiilor și regulilor de prelucrare a datelor personale în toate statele membre ale Uniunii Europene, în consolidarea adusă drepturilor persoanelor fizice și în creșterea responsabilității operatorilor în legătură cu prelucrările efectuate.

Un aspect de noutate, pe care doresc să-l supun atenţiei dumneavoastră, constă în instituirea obligației instituţiilor publice şi, în anumite situații, a entităţilor private, de a-şi desemna o persoană responsabilă cu protecţia datelor, în funcţie de anumite criterii stabilite expres prin dispozițiile art. 37 din Regulament. Apreciem că aceasta a avut un impact pozitiv în activitatea operatorilor din România și, implicit, efecte benefice în privința respectării drepturilor persoanelor fizice.

Pentru asigurarea concordanței competențelor și sarcinilor de monitorizare și control ale instituției noastre cu prevederile art. 55-59 din Regulamentul General privind Protecția Datelor, instituția noastră a pregătit proiectul de lege de modificare și completare a Legii nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Acest proiect a fost adoptat de Parlament și a devenit Legea nr. 129/2018.

De asemenea, Autoritatea Națională de supraveghere a fost implicată și în faza de susținere legislativă în fața Parlamentului a Legii nr. 190/2018 privind unele măsuri

de aplicare a Regulamentului General privind protecția datelor, intrată în vigoare pe 31 iulie 2018.

Pentru a veni în sprijinul operatorilor și a asigura aplicarea efectivă a noilor reglementări europene și naționale, Autoritatea națională de Supraveghere a adoptat și publicat în Monitorul Oficial, în cursul anului 2018, cinci decizii cu caracter normativ, care s-au dovedi deja instrumente utile în activitatea tuturor operatorilor de conformare cu exigențele acestei Regulamentului european.

Totodată, în anul 2018, 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, evidențiem că, în anul 2018, acţiunile Autorităţii au urmărit în mod special:

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

În final, permiteți-mi să vă mulțumesc pentru sprijinul 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.

Ancuţa Gianina OPRE,

Preşedinte

CUPRINS

CAPITOLUL IV
ACTIVITATEA DE CONTROL

CAPITOLUL V

CAPITOLUL VI

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

CAPITOLUL VII

CAPITOLUL I
PREZENTARE GENERALĂ

Raportul de activitate pe anul 2018 al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe şapte capitole, după cum urmează:

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

În cuprinsul **Capitolului al II-lea** sunt prezentate principalele aspecte reglementate prin acte normative adoptate la nivel european, în special cu privire la Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, aplicabil în toate statele membre începând cu data de 25 mai 2018.

Capitolul al III-lea cuprinde informații relevante referitoare la activitatea de avizare a proiectelor de acte normative şi la aceea de consultare referitoare la aplicarea regulilor de protecţie a datelor personale, inclusiv de clarificare a unor chestiuni semnalate de diverşi operatori. Aceasta s-a concretizat în emiterea avizelor asupra unui număr însemnat de proiecte de acte normative şi 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 şi operatorii de date și-au exprimat interesul pentru noile reglementări aduse în materia protecției datelor de acest act normativ și au solicitat, în special, informaţii cu privire la aplicabilitatea Regulamentului.

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

Secţiunea privind informarea publică expune principalele modalităţi de popularizare a Regulamentului General privind Protecția Datelor, utilizate în cursul anului 2018, în limitele resurselor bugetare alocate.

Capitolul al IV-lea constă într-o prezentare a principalelor aspecte din activitatea de control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite.

Investigaţiile efectuate din oficiu au vizat verificarea modului de respectare a prevederilor legale aplicabile, 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 semnificative a numărului acestora, în anul 2018 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 investigaţiilor efectuate în anul 2018, au fost aplicate sancţiuni contravenţionale constând în avertismente şi amenzi în cuantum total de 631.500 lei.

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

Capitolul al VI-lea privind activitatea de supraveghere a prelucrărilor de date cu caracter personal cuprinde principalele concluziile rezultate din analizarea formularelor transmise de operatorii de date, persoane fizice şi juridice, care au avut obligaţia depunerii acestora. Au fost înregistrate un număr total de 5066 notificări privind prelucrări de date realizate atât pe teritoriul României, cât şi în statele membre, ori transferuri în state terţe.

Capitolul al VII-lea referitor la resursele materiale şi financiare conţine informaţii privind creditele bugetare puse la dispoziţia Autorităţii naţionale de supraveghere şi cheltuielile aferente.

CAPITOLUL II

NOI ACTE LEGISLATIVE LA NIVELUL UNIUNII EUROPENE

Secţiunea 1 - Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor)

Pachetul legislativ adoptat la nivelul Uniunii Europene pe data de 27 aprilie 2016 cuprinde două acte normative de impact:

- Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
- Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi 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 Regulamentul General privind Protecția Datelor constă în obligativitatea instituţiilor publice şi entităţilor private de a-şi desemna un responsabil cu protecţia datelor la nivel intern, în funcţie 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 obligaţiilor operatorilor, un accent deosebit fiind pus pe creşterea gradului de responsabilizare a acestora. Consacrarea expresă a principiilor de prelucrare privacy by design și privacy by default reprezintă un alt element de noutate al acestei reglementări, implicând asigurarea protecției datelor din momentul inițial al stabilirii mijloacelor de prelucrare.

Subliniem că Regulamentul General privind Protecția Datelor a stabilit și un mecanism nou de cooperare între autoritățile naționale de supraveghere care implică 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 instituţională şi administrativă a Autorităţii naționale de supraveghere, inclusiv prin alocarea și asigurarea unor resurse umane, materiale și financiare corespunzătoare.

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

Prevederile Regulamentului General privind Protecția Datelor au devenit aplicabile, începând cu data de 25 mai 2018, în toate statele membre ale Uniunii Europene.

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

Această reglementare europeană distinctă a fost 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 urmăririi penale a infracţiunilor sau al executării pedepselor.

Astfel, a fost adoptată Legea nr. 363 din 28 decembrie 2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date, publicată în Monitorul Oficial nr. 13 din 7 ianuarie 2019.

Prin această reglementare s-a avut în vedere, în principal, următoarele:

- definirea termenilor utilizați în lege;
- obligația păstrării evidenței operațiunilor de prelucrare;
- evaluarea impactului asupra protecției datelor;
- asigurarea respectării drepturilor persoanelor vizate;
- desemnarea responsabilului cu protecția datelor;
- asigurarea protecției datelor începând cu momentul conceperii
- condițiile de transfer al datelor cu caracter personal;

În același timp, prin Legea nr. 363/2018 a fost abrogată Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice.

CAPITOLUL III

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

Secțiunea 1 - Crearea cadrului legal național privind punerea în aplicare a Regulamentului General privind Protecția Datelor

Extinderea competențelor și sarcinilor autorităților naționale de supraveghere prin prisma Regulamentului (UE) 2016/679 a determinat luarea unor măsuri legale naționale de consolidare a capacității instituţionale şi administrative a Autorității Naționale de Supraveghere.

În prima jumătate a anului 2018, în continuarea activității dedicate adoptării măsurilor legale naționale de punere în aplicare a Regulamentului (UE) 2016/679, Autoritatea Națională de Supraveghere a participat, în mod susținut, la discuțiile din comisiile de specialitate de la nivelul Parlamentului României, purtate cu ocazia dezbaterilor următoarelor proiecte de acte normative:

- Proiectul de Lege pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date; și
- Propunerea legislativă privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

La finalul procesului legislativ, Parlamentul României a adoptat Legea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia

persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, publicată în Monitorul Oficial nr. 503 din 19 iunie 2018. Urmare a intervențiilor legislative, Legea nr. 102/2005 a fost republicată în Monitorul Oficial nr. 947 din 9 noiembrie 2018.

De asemenea, a fost adoptată Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), publicată în Monitorul Oficial nr. 651 din 26 iulie 2018.

➢ ***Legea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date***

Măsurile legale adoptate prin Legea nr. 129/2018 s-au bazat, în principal, pe art. 52 alin. (4) din Regulamentul general privind protecția datelor care prevede că ”Fiecare stat membru se asigură că fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce, al cooperării și al participării în cadrul comitetului.”

În acest context, prin Legea nr. 129/2018 s-a urmărit, în principal, asigurarea competențelor și sarcinilor de monitorizare și control ale Autorității Naționale de Supraveghere în acord cu prevederile art. 55-59 din Regulamentul (UE) 2016/679, asigurând în acest mod un cadru legal adecvat pentru respectarea drepturilor specifice ale persoanelor fizice în domeniul prelucrării datelor cu caracter personal (dreptul de informare, dreptul de acces, dreptul la rectificare, dreptul la restricționarea prelucrării, dreptul la ștergerea datelor – dreptul ”de a fi uitat”, dreptul la opoziție, dreptul la

portabilitatea datelor), precum și o interacțiune eficientă în relația administrație-cetățeni.

Astfel, s-au stabilit principalele atribuţii ale Autorităţii Naţionale de Supraveghere și ale președintelui acesteia, în acord cu elementele de noutate aduse de cele două acte normative ale Uniunii Europene, Regulamentul (UE) 2016/679 şi Directiva (UE) 2016/680.

În acest sens, s-au consolidat independența și autonomia Autorităţii Naţionale de Supraveghere în concordanță cu dispozițiile art. 52 din Regulamentul (UE) 2016/679.

Totodată, au fost enumerate entitățile care intră sub incidența legislației referitoare la protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal, care au calitatea de operatori de date, pentru a se evita apariția, în practică, a unor situații de interpretare și aplicare neunitară a definiției operatorului din Regulamentul (UE) 2016/679.

În acest context, Legea nr. 129/2018 a întărit obligația acestor entități de a acorda Autorității Naționale de Supraveghere, în exercitarea atribuțiilor sale legale, sprijinul solicitat, de a-i comunica sau, după caz, de a-i pune la dispoziţie informaţiile, documentele sau actele pe care le deţin, în condițiile legii, în acord cu atribuțiile de investigare conferite prin art. 58 din Regulamentul (UE) 2016/679.

Actul normativ sus-menționat a stabilit, în concordanță cu art. 59 din Regulamentul (UE) 2016/679, faptul că raportul anual se transmite Senatului României, Guvernului României, Comisiei Europene şi Comitetului european pentru protecţia datelor.

Totodată, prin această lege s-au modificat condițiile de încetare înainte de termen a mandatului preşedintelui, respectiv al vicepreşedintelui Autorităţii Naţionale de Supraveghere, precum și de revocare din funcție a acestora, în concordanță cu art. 53 din Regulamentul (UE) 2016/679.

În îndeplinirea sarcinilor stabilite de art. 57 și 58 din Regulamentul (UE) 2016/679, a fost necesară inserarea în actul normativ, a unui nou capitol, intitulat „Exercitarea atribuțiilor de control și de soluționare a plângerilor”, care stabilește reguli generale de efectuare a investigațiilor și soluționare a plângerilor.

Totodată, în considerarea elementelor de noutate referitoare la măsurile corective pe care Autoritatea Națională de Supraveghere le poate aplica, potrivit art. 58 alin. (2) din Regulamentul (UE) 2016/679, a fost necesară consacrarea la nivel național, prin prezenta lege, a sancțiunilor contravenționale principale, respectiv avertismentul și amenda, precum și a măsurii corective de tipul avertizării.

În același timp, prin acest act normativ s-a stabilit și modalitatea de contestare a măsurilor dispuse de Autoritatea Națională de Supraveghere, atât de către operatori, cât și de către persoanele vizate, în conformitate cu sarcinile trasate statului membru prin art. 58 alin. (4) și (5) din Regulamentul (UE) 2016/679.

De asemenea, s-a avut în vedere suplimentarea numărului de posturi/angajați, pentru a se asigura posibilitatea îndeplinirii noilor competenţe și sarcini ale Autorităţii Naţionale de Supraveghere stabilite prin Regulamentul (UE) 2016/679, dar și a celor prevăzute de Directiva (UE) 2016/680 și Directiva (UE) 2016/681.

Totodată, este de subliniat faptul că Legea nr. 129/2018 este în concordanță și cu jurisprudența relevantă a Curții de Justiție a Uniunii Europene în ceea ce privește interpretarea cerinței de independență a autorităților naționale de supraveghere, în sensul că aceasta a fost instituită pentru a consolida protecția persoanelor și a organismelor care sunt avute în vedere prin deciziile acestora și pentru a crea în toate statele membre un nivel ridicat de protecție a persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal (Cauza C-518/07 și C-614/10).

De asemenea, prin acest act normativ s-au stabilit dispoziții tranzitorii în contextul abrogării Legii nr. 677/2001, astfel:

- Regulamentul (UE) 2016/679 se aplică plângerilor şi sesizărilor depuse şi înregistrate la Autoritatea Națională de Supraveghere începând cu data aplicării acestuia, precum şi celor depuse înainte de 25 mai 2018 şi aflate în curs de soluţionare;

- investigaţiile începute anterior datei de 25 mai 2018 şi nefinalizate la această dată sunt supuse dispoziţiilor Regulamentului, iar constatarea faptelor şi aplicarea măsurilor corective, inclusiv a sancţiunilor contravenţionale, după data de 25 mai 2018, se realizează în conformitate cu prevederile Regulamentului și ale dispoziţiilor legale de punere în aplicare a acestuia.

➢ ***Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)***

Inițiată ca propunere legislativă, această reglementare era necesară având în vedere prevederile Regulamentului (UE) 2016/679, care reglementează obligativitatea statelor membre sau dau posibilitatea acestora de a adopta anumite reglementări naționale destinate aplicării acestei reglementări europene în concordanță cu specificul regimului juridic național.

Astfel, la adoptarea Legii nr. 190/2018 au fost avute în vedere următoarele prevederi din actul normativ european:

- prevederile art. 9 alin. (4) din Regulamentul (UE) 2016/679, potrivit cărora statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea;

- prevederile art. 43 din Regulamentul (UE) 2016/679, care menționează obligația statelor membre de a se asigura că aceste organisme de certificare sunt acreditate de către una sau amândouă dintre următoarele entități: (a) autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56; (b) organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului, în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de autoritatea de supraveghere care este competentă în temeiul articolului 55 sau 56;

- prevederile art. 83 alin. (4) - (6) din Regulamentul (UE) 2016/679, referitoare la regimul sancționator aplicabil în sectorul privat;

- prevederile art. 83 alin. (7) din Regulamentul (UE) 2016/679, care dispun că, fără a aduce atingere competențelor corective ale autorităților de supraveghere menționate la articolul 58 alineatul (2), fiecare stat membru poate prevedea norme

prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi administrative autorităților publice și organismelor publice stabilite în statul membru respectiv;

- prevederile art. 83 alin. (7) din Regulamentul (UE) 2016/679, care dispun că exercitarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil;

- prevederile Capitolului IX din Regulamentul (UE) 2016/679, care permit introducerea de dispoziții naționale referitoare la situații specifice de prelucrare, cum ar fi aceea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, prelucrarea unui număr de identificare național sau prelucrarea în contextul ocupării unui loc de muncă;

- aspectele reținute de Curtea Europeană a Drepturilor Omului (Marea Cameră) în Cauza Bărbulescu împotriva României (5.09.2017), referitoare la protecția vieții private a angajatului în comunicațiile electronice, în contextul relațiilor de muncă;

Față de prevederile de mai sus, Legea nr. 190/2018 aduce elemente de noutate în peisajul juridic al protecției datelor personale, prin următoarele aspecte:

- menționează expres autorităţile şi organismele publice cărora le sunt aplicabile dispozițiile Regulamentului General privind Protecția Datelor - *Camera Deputaţilor şi Senatul, Administraţia Prezidenţială, Guvernul, ministerele, celelalte organe de specialitate ale administraţiei publice centrale, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice locale şi de la nivel judeţean, alte autorităţi publice, precum şi instituţiile din subordinea/coordonarea acestora; sunt asimilate autorităţilor/organismelor publice şi unităţile de cult şi asociaţiile şi fundaţiile de utilitate publică;*

- definește o serie de termeni cum ar fi: *număr de identificare naţional, plan de remediere, măsură de remediere, termen de remediere;*

- stabilește reguli speciale privind prelucrarea unor categorii de date cu caracter personal, precum *date genetice, date biometrice sau date privind sănătatea;*

- stabilește condițiile de prelucrare a unui număr de identificare naţional (de exemplu, codul numeric personal) atunci când prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță;

- instituie prevederi specifice privind prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă;
- prevede derogări pentru prelucrările efectuate în scopuri jurnalistice, în scopul exprimării academice, artistice sau literare ori în scopuri de cercetare ştiinţifică, istorică, statistică, de arhivare în interes public;
- menționează condițiile desemnării şi sarcinile responsabilului cu protecţia datelor, în special în cazul autorităților/instituțiilor publice și al organismelor publice;
- desemnează Asociația de Acreditare din România – RENAR ca organism național de acreditare a organismelor de certificare prevăzute la art. 43 din Regulament;
- stabilește regimul sancționator derogatoriu, inclusiv sub aspectul sancțiunilor pecuniare, aplicabil autorităților și organismelor publice, acordându-se prioritate mecanismului de prevenire, anterior aplicării amenzilor contravenționale.

Secțiunea a 2-a Activitatea de reglementare a ANSPDCP

În temeiul atribuțiilor de reglementare conferite de Legea nr. 102/2005, Autoritatea Națională de Supraveghere a emis, pe parcursul anului 2018, următoarele decizii administrative cu caracter normativ, necesare desfășurării în special a activității de soluționare a plângerilor și de efectuare a investigațiilor, precum și pentru abrogarea unor acte administrative emise sub imperiul Legii nr. 677/2001:

- **Decizia nr. 99/2018 privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date**, publicată în Monitorul Oficial nr. 432 din 22 mai 2018

Având în vedere necesitatea existenței unui cadru juridic predictibil și clar, în concordanță cu normele de tehnică legislativă, a fost publicată Decizia nr. 99/2018. Aceasta a fost emisă și având în vedere Comunicarea Comisiei Europene către Parlamentul European și Consiliu din 24 ianuarie 2018, intitulată *„Protecție sporită, noi*

oportunități – Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecția datelor de la 25 mai 2018", în care se preciza că „În momentul adaptării legislației lor naționale, statele membre trebuie să ia în considerare faptul că orice măsuri naționale care ar avea ca rezultat crearea unui obstacol în calea aplicării directe a regulamentului și punerea în pericol a aplicării simultane și uniforme a acestuia în întreaga UE sunt contrare tratatelor."

La data intrării în vigoare a acestui act normativ și-au încetat aplicabilitatea deciziile emise de Autoritatea Naţională de Supraveghere, în aplicarea Legii nr. 677/2001, cu modificările şi completările ulterioare, precum şi ordinele emise de Avocatul Poporului, în calitate de autoritate de supraveghere în domeniul protecţiei datelor, în perioada 2002-2005, în aplicarea Legii nr. 677/2001, cu modificările şi completările ulterioare.

➢ **Decizia nr. 128/2018 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)**, publicată în Monitorul Oficial nr. 557 din 3 iulie 2018

Prin această decizie s-a stabilit formularul tipizat de notificare a încălcării securității datelor cu caracter personal, în aplicarea art. 33 alin. (1) din Regulamentul General privind Protecția Datelor care obligă operatorii să anunțe încălcarea Autorității Naționale de Supraveghere, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta. Formularul-tip este disponibil pe pagina web a instituției www.dataprotection.ro și se poate transmite pe cale electronică.

➢ **Decizia nr. 133/2018 privind aprobarea Procedurii de primire și soluționare a plângerilor**, publicată în Monitorul Oficial nr. 600 din 13 iulie 2018

Modificările semnificative intervenite în legătură cu condițiile de admisibilitate și de soluționare a plângerilor de către Autoritatea Națională de Supraveghere, inclusiv în contextul prelucrărilor transfrontaliere, stabilite de Regulamentul General privind Protecția Datelor și Legea nr. 102/2005, au condus la emiterea Deciziei nr. 133/2018.

Astfel, în temeiul dispoziţiilor art. 3 alin. (5) şi (6), ale art. 10 alin. (1) lit. a)-d) şi f), ale art. 12 şi 14^7 -14^8 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, a fost emis actul normativ sus-menționat care vizează, în principal, faptul că:

- plângerile pot fi adresate de orice persoană vizată, în special în cazul în care reşedinţa sa obişnuită, locul său de muncă sau presupusa încălcare se află sau, după caz, are loc pe teritoriul României;
- plângerile pot fi depuse la sediul Autorității Naționale de Supraveghere sau transmise prin poştă, inclusiv cea electronică, ori prin utilizarea formularului electronic de plângere, disponibil pe pagina web a instituției www.dataprotection.ro;
- plângerile pot fi depuse personal sau prin mandatar, inclusiv prin intermediul unei organizaţii fără scop patrimonial, activă în domeniul protecţiei datelor cu caracter personal;
- petiţionarii sunt informaţi în scris cu privire la admiterea plângerii, inclusiv cu privire la efectuarea unei investigaţii mai amănunţite sau coordonarea cu alte autorităţi de supraveghere, precum și în legătură cu evoluţia sau cu rezultatul investigaţiei întreprinse;
- persoana vizată nemulțumită de modalitatea de soluționare a plângerii sale se poate adresa secţiei de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare.

➢ **Decizia nr. 161/2018 privind aprobarea Procedurii de efectuare a investigațiilor**, publicată în Monitorul Oficial nr. 892 din 23 octombrie 2018

În temeiul dispoziţiilor art. 3 alin. (5) şi (6), ale art. 10 alin. (1) lit. a)-d), ale art. 12 şi art. 14^1-14^6 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi

funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, a fost emisă Decizia nr. 161/2018, care stabilește condițiile de desfășurare a investigațiilor.

Potrivit prevederilor deciziei menționate mai sus, investigația se poate finaliza cu întocmirea unui proces-verbal de constatare/sancționare sau a unei decizii a Președintelui Autorității Naționale de Supraveghere, prin care se pot dispune măsuri corective și/sau sancțiuni contravenționale (avertisment, amendă). În cazul autorităților/organismelor publice, anterior acordării unei sancțiuni pecuniare se aplică avertisment și se întocmește un plan de remediere potrivit modelului prevăzut de Legea nr. 190/2018 și care trebuie îndeplinit în termenul acordat de Autoritatea Națională de Supraveghere.

Măsurile dispuse pot fi contestate în termen de 15 zile la secția de contencios administrativ a tribunalului competent, potrivit legii.

➢ **Decizia nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal**, publicată în Monitorul Oficial nr. 919 din 31 octombrie 2018

Această decizie a fost emisă în scopul asigurării unei protecţii eficiente a drepturilor persoanelor ale căror date cu caracter personal sunt supuse prelucrării, în special în cazul anumitor operaţiuni de prelucrare a datelor cu caracter personal care prezintă riscuri pentru drepturile şi libertăţile persoanelor, datorită naturii datelor prelucrate (de exemplu: date sensibile precum cele genetice, biometrice, privind sănătatea), domeniului de aplicare, a contextului şi scopurilor prelucrării, caracterului specific al categoriilor de persoane vizate (de exemplu: persoane vulnerabile – angajați, minori) și numărului acestora sau mecanismelor utilizate pentru prelucrarea datelor, în special cele bazate pe utilizarea noilor tehnologii.

Prelucrarea datelor în situațiile vizate de această decizie obligă operatorii la efectuarea unei evaluări a impactului asupra protecției datelor, potrivit art. 35 din Regulamentul General privind Protecția Datelor.

În acest context, potrivit prezentei decizii, evaluarea impactului asupra protecţiei datelor cu caracter personal de către operatori este obligatorie, în special, în următoarele cazuri:

- prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
- prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;
- prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, pieţe, parcuri sau alte asemenea spaţii;
- prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;
- prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;
- prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);
- prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor

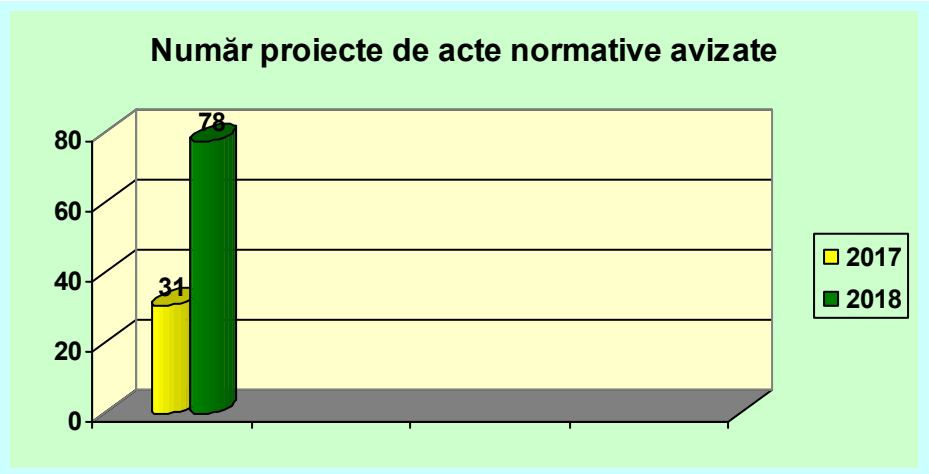
de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

Anterior emiterii acestei decizii, a fost consultat Comitetul European privind Protecția Datelor, în concordanță cu dispozițiile Regulamentului General privind Protecția Datelor.

Secțiunea a 3-a Avizarea actelor normative

Autoritatea Naţională de Supraveghere a emis, în temeiul art. 57 alin. (1) lit. c) din Regulamentul General privind Protecția Datelor, avize asupra unui număr de **78 de proiecte de acte normative** elaborate de instituţii şi autorităţi publice, care implicau aspecte complexe privind prelucrarea datelor cu caracter personal.

Comparativ cu anul anterior, constatăm că numărul de proiecte de acte normative avizate în anul 2018 de Autoritatea Naţională de Supraveghere a depășit dublul numărului actelor normative avizate în anul 2017.



În cele mai multe cazuri, Autoritatea Naţională de Supraveghere 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, s-au efectuat recomandări pentru reanalizarea acestora și armonizarea lor cu dispozițiile legale privind protecția datelor.

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

❖ **Ministerul Dezvoltării Regionale și Administrației Publice a transmis spre avizare proiectul *Ordonanței de urgență a Guvernului privind modificarea și completarea Legii cadastrului și a publicității imobiliare nr. 7/1996*.**

Faţă de textul proiectului sus-menționat, Autoritatea Națională de Supraveghere a formulat observații și propuneri având în vedere necesitatea respectării principiului responsabilității operatorului de date cu caracter personal, ținând cont de calitatea de operatori atât a Agenției Naționale de Cadastru și Publicitate Imobiliară, cât și a oficiilor județene, în contextul prelucrării datelor personale.

Referitor la mențiunile privind încheierea unui protocol între autorități publice, Autoritatea Națională de Supraveghere a atras atenția asupra necesității respectării exigențelor Curții de Justiție a Uniunii Europene din Cauza Smaranda Bara și alții (C-201/14), în care Curtea a statuat faptul că articolele 10, 11 și 13 din Directiva 95/46/CE trebuie interpretate în sensul că se opun unor măsuri naționale, care permit unei autorități a administrației publice a unui stat membru să transmită date personale unei alte autorități a administrației publice în vederea prelucrării ulterioare, fără ca persoanele vizate să fi fost informate despre această transmitere sau despre această prelucrare.

De asemenea, instanța europeană a constatat faptul 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 acest sens, Autoritatea Națională de Supraveghere a considerat ca fiind necesară stabilirea condițiilor de acces la Registrul Național de Evidență a Persoanelor printr-un act care să facă obiectul unei publicări oficiale, potrivit celor statuate de CJUE.

În același timp, s-a atras atenția cu privire la necesitatea respectării principiilor prevăzute de art. 5 din Regulamentul General privind Protecția Datelor, în special cel al reducerii la minimum a datelor, al responsabilității, stabilit de art. 24, precum și a principiului transparenței statuat de art. 12, 13 și 14 din același regulament.

Față de cele de mai sus, Autoritatea Națională de Supraveghere a apreciat ca fiind necesară completarea textelor supuse analizei, corespunzător observațiilor și propunerilor prezentate în punctul său de vedere.

❖ **Ministerul Afacerilor Interne a transmis spre avizare proiectul de *Lege pentru modificarea şi completarea Ordonanţei Guvernului nr. 83/2001 privind înfiinţarea, organizarea şi funcţionarea serviciilor publice comunitare pentru eliberarea şi evidenţa paşapoartelor simple şi serviciilor publice comunitare regim permise de conducere şi înmatriculare a vehiculelor.***

Faţă de textul proiectului sus-menționat, Autoritatea Națională de Supraveghere a formulat unele observații și propuneri, având în vedere atât necesitatea asigurării clarității unor articole, precum și respectarea principiului reducerii la minimum a datelor în ceea ce privește colectarea acestora în Registrul Național de Evidență a Pașapoartelor Simple.

Astfel, referitor la dispozițiile privind conținutul Sistemului național informatic de evidență a pașapoartelor simple, s-a apreciat că sintagma ”precum și a altor persoane care au avut legătură cu activitatea desfășurată la nivelul Direcției generale de pașapoarte sau al serviciilor publice comunitare pentru eliberarea și evidența pașapoartelor simple” are o formulare generală, fiind lipsită de claritate, motiv pentru care s-a recomandat precizarea concretă a acestor categorii de persoane. Aceleași aspecte au fost remarcate și în ceea ce privește sintagma ”foștilor cetățeni români care au avut legătură cu activitatea desfășurată la nivelul Direcției generale de pașapoarte sau al serviciilor publice comunitare pentru eliberarea și evidența pașapoartelor simple”. În acest sens, s-a solicitat și argumentarea necesității evidenței unor astfel de categorii de persoane.

În ceea ce privește categoriile de date cu caracter personal enumerate de proiectul de act normativ, raportat la scopurile precizate de acesta și mențiunile cu privire la punerea în acord a OG nr. 83/2001 cu Legea nr. 141/2010, precum și necesitatea reglementării la nivel de lege a categoriilor de date ce pot fi prelucrate, Autoritatea Națională de Supraveghere a apreciat că datele și categoriile de date sunt excesive iar unele au o formulare generică, fiind lipsite de claritate.

În acest context, s-a solicitat precizarea concretă a datelor vizate, precum și necesitatea colectării unora dintre acestea (eventual necesitatea menținerii lor), astfel: datele din actele de stare civilă: datele din permisul de conducere și certificatul de înmatriculare; profesia și locul de muncă; formare profesională, diplome, studii; situația familială; date privind bunurile deținute.

Prin urmare, față de textul proiectului supus analizei, s-a apreciat că se impune reanalizarea textelor în discuție și modificarea/completarea acestora în concordanță cu observațiile și propunerile efectuate de Autoritatea Națională de Supraveghere.

❖ **Ministerul pentru Relaţia cu Parlamentul a solicitat exprimarea unui punct de vedere cu privire la proiectul de *Lege pentru modificarea și completarea unor acte normative în materie electorală (L. 302/2018).***

Urmare a solicitării adresate, au fost efectuate următoarele precizări:

a) Față de modificările și completările propuse la Legea nr. 370/2004 pentru alegerea Președintelui României, s-a subliniat necesitatea respectării principiului minimizării datelor, prevăzut de art. 5 din Regulamentul general privind protecția datelor, recomandându-se analizarea necesității colectării anumitor date și categorii de date.

În același timp, s-a mai precizat necesitatea respectării principiului responsabilității operatorului, prin reformularea unor articole astfel încât să reiasă cu claritate responsabilitatea fiecărei entități potrivit atribuțiilor legale, în contextul prelucrării datelor personale, precum și faptul că se impune clarificarea calității acestora inclusiv raportat la obligativitatea luării de măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel corespunzător de securitate și confidențialitate a datelor, în acord cu prevederile art. 32 din Regulamentul (UE) 2016/679.

S-a recomandat, de asemenea, luarea în considerare a definițiilor date operatorului, împuternicitului și operatorilor asociați, potrivit art. 4 pct. 7 și 8 și art. 26 din Regulament, în cadrul prelucrărilor de date efectuate, fiecare dintre entitățile implicate având obligații potrivit rolului îndeplinit în cadrul prelucrărilor de date în scop electoral și în cadrul Sistemului informatic de monitorizare a prezenței la vot, gestionat de Autoritatea Electorală Permanentă, precum și necesitatea respectării principiului limitării legate de stocare statuat de art. 5 din Regulament, prin limitarea perioadei de

stocare a datelor cu caracter personal strict pe perioada necesară îndeplinirii scopului prelucrării.

b) Față de modificările și completările propuse la Legea nr. 33/2007 privind organizarea şi desfăşurarea alegerilor pentru Parlamentul European, Autoritatea Națională de Supraveghere a recomandat reanalizarea necesității colectării, în anumite situații, a unor date precum copia actului de identitate prin raportare la art. 5 din Regulamentul (UE) 2016/679, potrivit căruia datele cu caracter personal trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

De asemenea, s-a accentuat necesitatea luării în considerare a principiilor de protecţie a datelor, în special prin stabilirea clară a calității de operator/operatori, precum și a celei de destinatari ai datelor cu caracter personal, respectiv a garanţiilor adecvate pentru respectarea drepturilor persoanelor vizate şi stabilirea persoanelor autorizate care vor avea acces la date, în scopuri legitime.

❖ **Ministerul Muncii şi Justiţiei Sociale a transmis spre avizare *proiectul de Lege privind sistemul public de pensii.***

Având în vedere textul proiectului, Autoritatea Națională de Supraveghere a formulat următoarele observații:

Faţă de prevederile referitoare la schimbul de date cu alte instituţii publice şi autorităţi „pe bază de protocoale”, s-a atras atenția cu privire la cele statuate de Curtea de Justiție a Uniunii Europene în Cauza C-201/14 - Smaranda Bara împotriva României.

Totodată, având în vedere faptul că operatorii au obligaţia implementării de măsuri tehnice şi organizatorice adecvate pentru a asigura un nivel de securitate corespunzător acestui risc, potrivit dispoziţiilor art. 32 din Regulamentul General privind Protecţia Datelor, Autoritatea Națională de Supraveghere a propus inserarea unor prevederi în acest sens în proiectul de lege.

Ulterior, după însuşirea de către Ministerul Muncii şi Justiţiei Sociale a observaţiilor şi propunerilor formulate de Autoritatea Națională de Supraveghere, proiectul de lege a fost avizat favorabil.

❖ **Ministerul Justiției a transmis spre avizare *proiectul de Lege pentru modificarea și completarea Legii nr. 211/2004 privind unele măsuri pentru asigurarea protecției victimelor infracțiunilor.***

Față de proiectul transmis, Autoritatea Națională de Supraveghere a formulat observații și propuneri:

Referitor la prelucrarea datelor cu caracter special ale persoanelor fizice „rasă, origine etnică sau socială, religie sau credință, opiniile politice sau de oricare altă natură, dizabilitatea, orientarea sexuală", s-a recomandat analizarea acestora prin raportare la dispozițiile art. 9 alin. (2) din Regulamentul General privind Protecția Datelor.

În ceea ce privește „consemnarea" datelor, precum și "crearea unui Registru special privind victimele infracțiunilor", Autoritatea Națională de Supraveghere a subliniat necesitatea luării în considerare a dispozițiilor art. 5 coroborate cu art. 24 și art. 25 din Regulament, astfel încât sistemul de evidență, care va asigura colectarea, înregistrarea și stocarea datelor personale ale victimelor infracțiunilor, să fie constituit în concordanță cu principiile stabilite de Regulamentul General privind Protecția Datelor.

S-a atras atenția asupra necesității stabilirii unui termen de stocare a datelor în conformitate cu prevederile art. 5 lit. e) din Regulament.

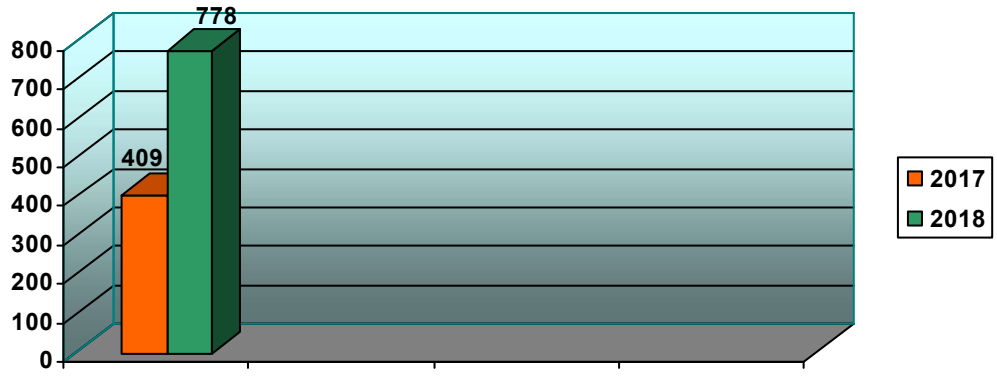
Sub aspectul respectării drepturilor persoanelor vizate, s-a subliniat faptul că art. 12 din Regulament prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil.

În acest context, Autoritatea Națională de Supraveghere a propus includerea unor prevederi referitoare la respectarea regulilor de prelucrare a datelor personale, inclusiv a drepturilor persoanelor fizice vizate, de către entitățile menționate în prezentul proiect de lege.

După însuşirea de către Ministerul Justiției a observaţiilor şi propunerilor formulate de Autoritatea Națională de Supraveghere, proiectul de lege a fost avizat favorabil.

Secțiunea a 4-a Puncte de vedere privind diverse chestiuni de protecţia datelor

În anul 2018, au fost emise **778 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, ceea ce reprezintă aproape o dublare a numărului acestora față de anul 2017 și reflectă interesul manifestat în asigurarea respectării noilor reguli europene de prelucrare a datelor personale.



Prezentăm mai jos o serie de spețe semnificative supuse spre analiză Autorităţii Naționale de Supraveghere:

a) Prelucrarea datelor privind starea de sănătate

O serie de persoane fizice, dar și autorități sau instituții publice, precum și entități din domeniul privat au solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la prelucrarea datelor cu caracter special, îndeosebi cele privind starea de sănătate.

În acest context, s-au precizat următoarele:

Art. 4 din Regulamentul General privind Protecția Datelor stabilește o serie de definiții, printre care și cea a datelor cu caracter personal. De asemenea, datele privind sănătatea sunt definite de aceleași dispoziții legale sus-menționate, ca fiind ”date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv

prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia" (art. 4 pct. 15).

Prin urmare, în accepțiunea definițiilor sus-citate, Autoritatea Națională de Supraveghere a precizat că informațiile precum codurile diagnosticelor ce aparțin unor persoane fizice (angajații) reprezintă date cu caracter personal ce vizează starea de sănătate.

În ceea ce privește legitimitatea prelucrării (inclusiv a dezvăluirii) acestor categorii de date speciale, art. 9 din Regulamentul General privind Protecția Datelor precizează condițiile în care se pot prelucra. Astfel, regula instituită de aceste dispoziții legale este aceea de interzicere a prelucrării de date privind starea de sănătate, cu unele excepții de strictă interpretare și aplicare, reglementate de art. 9 alin. (2) din Regulament.

În ceea ce privește prelucrarea bazată pe consimțământul persoanei vizate, Autoritatea Națională de Supraveghere a subliniat faptul că este necesară respectarea dispozițiilor art. 4 pct. 11 și art. 7 din Regulamentul General privind Protecția Datelor.

În același timp, alin. (4) al art. 9 din Regulamentul General privind Protecția Datelor prevede că: „Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea de date genetice, date biometrice sau date privind sănătatea."

În acest context, prin art. 3 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 au fost stabilite aceste condiții de prelucrare, astfel:

„(1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

(2) Prelucrarea datelor privind sănătatea realizată în scopul asigurării sănătăţii publice, astfel cum este definită în Regulamentul (CE) nr. 1338/2008 al Parlamentului European şi al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum şi la sănătatea şi siguranţa la locul de muncă,

publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 354/70 din 31 decembrie 2008, nu se poate efectua ulterior, în alte scopuri, de către terţe entităţi."

S-a subliniat, totodată, necesitatea respectării principiilor privind prelucrarea, statuate de art. 5 din Regulamentul General privind Protecția Datelor, a asigurării transparenței prelucrării datelor potrivit art. 12, 13 și 14 din Regulament, prin furnizarea în mod adecvat și complet a informațiilor stabilite de aceste dispoziții, precum și a respectării art. 24 din actul normativ european menționat mai sus.

În ceea ce privește prelucrarea datelor privind starea de sănătate de către angajații din cadrul compartimentelor de resurse umane, precizăm faptul că art. 29 din Regulamentul General privind Protecția Datelor prevede că orice persoană care acţionează sub autoritatea operatorului (angajații) care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

Prin urmare, Autoritatea Națională de Supraveghere a apreciat că datele privind starea de sănătate pot fi prelucrate (dezvăluite) fie cu consimțământul persoanei vizate, fie în celelalte condiții de excepție, de strictă interpretare și aplicare prevăzute de Regulamentul General privind Protecția Datelor, iar în îndeplinirea anumitor scopuri, datele se prelucrează de către un profesionist supus obligaţiei de păstrare a secretului profesional sau de către o altă persoană supusă unei obligaţii de confidenţialitate.

b) Monitorizarea angajaților la locul de muncă

În mai multe situații, s-a solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la monitorizarea angajaților la locul de muncă, în special prin intermediul mijloacelor de supraveghere video.

În acest context, s-a precizat faptul că dispozițiile art. 5 din Legea nr. 190/2018 stabilesc următoarele:

„În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

- angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

- angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

- alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi

- durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate."

Prin urmare, supravegherea video a angajaților la locul de muncă se poate institui în condițiile art. 6 din Regulamnetul General privind Protecția Datelor, coroborate, după caz cu prevederile art. 5 din Legea nr. 190/2019. În cazul invocării interesului legitim al operatorului, s-a precizat că justificarea trebuie să se regăsească la angajator într-o documentație argumentată temeinic, din care să rezulte prevalența interesului legitim asupra intereselor sau drepturilor şi libertăţilor angajaților.

Referitor la interesul legitim, s-a subliniat faptul că se impune ca acesta să fie temeinic justificat de către operator, având în vedere că prelucrarea are loc fără consimțământul persoanelor vizate. În acest sens, se poate recurge la o monitorizare prin videosupraveghere, în temeiul dispoziţiilor legale de mai sus, dar numai dacă această măsură este proporţională cu riscurile cu care se confruntă operatorul şi determină luarea unei asemenea măsuri intruzive în viaţa privată a persoanelor vizate.

În toate situațiile, în cazul în care se apelează la o altă entitate care gestionează sistemul de supraveghere video (prelucrează datele) pe seama operatorului (angajatorul), în calitate de împuternicit, se impune respectarea dispozițiilor art. 28 din Regulamentul General privind Protecția Datelor.

Totodată, devin aplicabile celelalte dispoziții ale Regulamentului General privind Protecția Datelor, cum ar fi principiile de prelucrare statuate de art. 5, drepturile persoanelor vizate, inclusiv sub aspectul transparenței și al informării, garantate de art. 12-22, responsabilitatea operatorului stabilită de art. 24, obligația operatorului de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit, prevăzută de art. 25, obligația de implementare a măsurilor tehnice și organizatorice

adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, prevăzută de art. 32 etc.

De asemenea, Autoritatea Națională de Supraveghere a subliniat că instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video urmează să respecte și Legea nr. 333/2003 şi normele metodologice de aplicare a acesteia.

c) Calitatea de operator, împuternicit sau operatori asociați

Solicitări numeroase au venit din partea diverselor entități din mediul privat, în special, beneficiari sau prestatori de diverse servicii, cu privire la stabilirea concretă, de către Autoritatea Națională de Supraveghere, a calității de operator, împuternicit sau operatori asociați.

S-a precizat faptul că, în contextul prelucrării datelor personale de către diverse entități în vederea realizării scopurilor propuse, acestea pot avea, după caz, calitatea de operatori, împuterniciți sau operatori asociați, așa cum sunt aceștia definiți de Regulamentul general privind protecția datelor.

Raportat la prevederile legale incidente, o anumită entitate și partenerii săi contractuali ar putea avea calitatea de operatori asociați, în măsura în care aceștia stabilesc în comun scopurile și mijloacele de prelucrare, au încheiat un acord prin care se stabilesc responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul Regulamentului și, indiferent de clauzele acordului, persoana vizată își poate exercita drepturile în temeiul Regulamentului cu privire la și în raport cu fiecare dintre operatori.

De asemenea, o societate și partenerii săi pot avea fiecare calitatea de operator pentru prelucrările de date pe care le realizează în mod individual, potrivit scopurilor și mijloacelor stabilite de operator sau de un act normativ și pentru care poartă întreaga răspundere.

În ceea ce privește calitatea de împuternicit, art. 4 pct. 8 din Regulamentul General privind Protecția Datelor definește „persoana împuternicită de operator” ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului. De asemenea, art. 28 alin. (3) lit. a) și alin. (10) din același Regulament stabilește o serie de obligații în sarcina operatorului și a împuternicitului.

În consecință, raportat la activitatea concretă ce urmează a fi realizată și în contextul căreia se prelucrează date personale, față de prevederile legale aplicabile, s-a apreciat că operatorii și împuterniciții sunt în măsură să își stabilească calitatea, având în vedere cunoașterea activității de prelucrare a datelor în anumite scopuri și folosind anumite mijloace, precum și a drepturilor și obligațiilor fiecărei părți, raportat la fiecare situație specifică.

d) Transferul datelor cu caracter personal într-un stat terț

Mai multe entități din domeniul privat au solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la condițiile în care se poate realiza transferul datelor cu caracter personal către un stat terț care nu oferă un nivel adecvat de protecție.

Cu privire la acest aspect, art. 46 alin. (1) din Regulamentul General privind Protecția Datelor prevede că în absenţa unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru persoanele vizate.

Garanţiile adecvate menţionate mai sus pot fi furnizate fără să fie nevoie de vreo autorizaţie specifică din partea unei autorităţi de supraveghere, prin:

a) existența unui instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;

b) reguli corporatiste obligatorii;

c) clauze standard de protecţie a datelor adoptate de Comisie;

d) clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisie;

e) un cod de conduită, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) existența unui mecanism de certificare, aprobat în conformitate cu articolul 42, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a

persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

Totodată, art. 46 alin. (3) din Regulament stabilește că pot fi furnizate, de asemenea, garanţii adecvate prin clauze contractuale încheiate între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională sub rezerva autorizării din partea autorităţii de supraveghere competente.

În acest context, considerentul (109) din Regulament subliniază că „Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecţie a datelor, adoptate de Comisie sau de o autoritate de supraveghere, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceştia să includă clauzele standard în materie de protecţie a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator şi o altă persoană împuternicită de operator, şi nici să adauge alte clauze sau garanţii suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard adoptate de Comisie sau de o autoritate de supraveghere sau nu prejudiciază drepturile sau libertăţile fundamentale ale persoanelor vizate.”

Raportat la prevederile legale sus-menționate, transferul datelor cu caracter personal către state terțe care nu oferă un nivel adecvat de protecție se poate realiza în temeiul art. 46 din Regulament, cu respectarea principiilor de prelucrare a datelor cu caracter personal.

e) Prelucrarea datelor cu caracter personal de către asociațiile de proprietari în scopul supravegherii video

Numeroase asociații de proprietari au solicitat Autorității Naționale de Supraveghere exprimarea unui punct de vedere cu privire la condițiile de prelucrare a datelor cu caracter personal ale proprietarilor/locatarilor unui imobil prin mijloace de supraveghere video.

Față de aceste solicitări, Autoritatea Națională de Supraveghere a menționat că prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune prevederilor Regulamentului General privind Protecția Datelor

Instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video se realizează și în conformitate cu Legea nr. 333/2003 şi normele metodologice de aplicare a acesteia.

În acest context, operatorii au fost informați cu privire la condițiile de legalitate care trebuie îndeplinite potrivit art. 6 din Regulamentul General privind Protecția Datelor.

Totodată, s-a subliniat că prelucrările de date efectuate vor fi precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din Regulament, care obligă operatorul să furnizeze persoanei vizate o serie de informații.

În ceea ce privește informarea persoanelor vizate, Autoritatea Națională de Supraveghere a precizat faptul că în spaţiile monitorizate trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană. În plus, s-a recomandat ca perioada de stocare a datelor cu caracter personal (imaginea) prelucrate de asociaţie ca urmare a instalării sistemului de supraveghere video să nu depăşească 30 zile.

În acelaşi timp, s-a precizat că, potrivit art. 48 alin. (1) din Legea nr. 196/2018 privind înfiinţarea, organizarea şi funcţionarea asociaţiilor de proprietari, adunarea generală poate adopta hotărâri, dacă majoritatea proprietarilor membri ai asociației de proprietari sunt prezenți personal sau prin reprezentanți care au o împuternicire scrisă și semnată de către proprietarii în numele cărora votează.

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

În anul 2018, 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:

- Cauzele conexate C-262-263-273/17 Solvay Chimica Italia e.a. și alții (instanță de trimitere – Tribunale Amministrativo Regionale per la Lombardia - Italia);

- Cauza C-193/18 – Google LLC (instanţă de trimitere din Germania - Oberverwaltungsgericht für das Land Nordrhein-Westfalen) privind interpretarea articolului 2 litera (c) din Directiva-cadru 2002/21/CE privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice;

- Cauza C-673/17 (instanţă de trimitere din Germania) referitoare la interpretarea art. 5 alin. (3) și art. 2 lit. (f) din Directiva 2002/58/CE, coroborat cu art. 2 lit. h) din Directiva 95/46/CE;

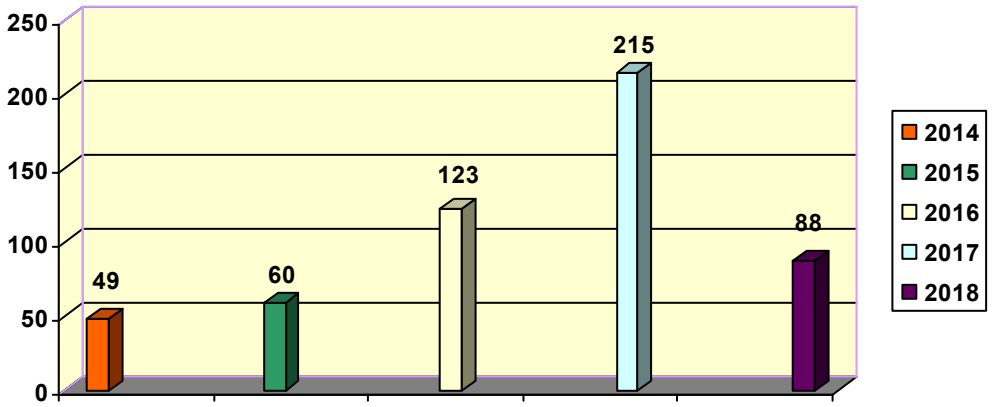
- **Cauza C-70/18** (instanță de trimitere_din Țările de Jos) referitoare la interpretarea art. 2 lit a) și b), 5, 6, 7, 8, 12, 13 din Directiva 95/46/CE, precum și a art. 29 alin. (5) din Regulamentul (UE) nr. 603/2013 din 26 iunie 2013 privind instituirea sistemului „Eurodac" pentru compararea amprentelor digitale în scopul aplicării eficiente a Regulamentului (UE) nr. 604/2013 de stabilire a criteriilor şi mecanismelor de determinare a statului membru responsabil de examinarea unei cereri de protecţie internaţională prezentate într-unul dintre statele membre de către un resortisant al unei ţări terţe sau de către un apatrid şi privind cererile autorităţilor de aplicare a legii din statele membre şi a Europol de comparare a datelor Eurodac în scopul asigurării respectării aplicării legii şi de modificare a Regulamentului (UE) nr. 1077/2011 de instituire a Agenţiei europene pentru gestionarea operaţională a sistemelor informatice la scară largă, în spaţiul de libertate, securitate şi justiţie;

- **Cauza C-520/18** (instanță de trimitere din Belgia) referitoare la interpretarea art. 15 alin. (1) din Directiva 2002/58/CE.

Secțiunea a 5-a Activitatea de reprezentare în faţa instanţelor de judecată

În anul 2018, un număr total de **88 de noi acțiuni de chemare în judecată** au fost înregistrate în cadrul Autorității Naționale de Supraveghere.

Spre deosebire de anul 2017 când s-au primit 215 cereri de chemare în judecată, în anul 2018 a avut loc o diminuare a acestora în contextul efectelor modificării cadrului normativ.



Având în vedere finalizarea în mod favorabil pentru instituția noastră a multor acțiuni aflate pe rolul instanțelor de judecată, pe parcursul anului 2018, prezentăm mai jos câteva cazuri relevante:

- ***Hotărâri pronunțate în litigii privind modalitatea de prelucrare a datelor cu caracter personal în sistemul Biroului de Credit***

Sub aspectul respectării drepturilor persoanelor vizate în contextul raportării datelor în sistemul Biroului de Credit, în anul 2018 au fost confirmate, prin hotărâri judecătorești definitive, atât sancțiunile dispuse de Autoritatea Națională de Supraveghere, cât și modalitatea de interpretare și aplicare a Legii nr. 677/2001 și Deciziei nr. 105/2007.

Astfel, unele dintre cele mai importante aspecte reținute de instanțele de judecată s-au referit la modalitatea de respectare a dreptului la informare al persoanei

vizate în activitatea instituțiilor financiare de raportare a datelor la Biroul de Credit și a dreptului de intervenție, respectiv de ștergere, asupra datelor.

Spre exemplu, într-o speță, Curtea de Apel București a statuat următoarele: „Cu privire la prima faptă constând în lipsa transmiterii informațiilor prevăzute de art. 12 alin. (1) lit. d) din Legea nr. 677/2001 raportat la art. 8 alin. (2) și art. 9 alin. (1) din Decizia ANSPDCP nr. 105/2007, Curtea reține că susținerile operatorului sunt neîntemeiate și vor fi respinse, având în vedere că ”legiuitorul prevede în mod expres obligația de comunicare prealabilă a informațiilor, ori de câte ori are loc o prelucrare a datelor cu caracter personal. Prin urmare, faptul că notificările priveau clienți care înregistrau, în mod succesiv, restanțe la creditele aflate în derulare nu conduce la concluzia că banca ar fi fost exonerată de obligația de comunicare în mod complet a informațiilor prevăzute de art. 12 alin. (1) lit. d) din Legea nr. 677/2001 raportat la art. 8 alin. (2) și art. 9 alin. (1) din Decizia ANSPDCP nr. 105/2007”.

Totodată, Curtea a reținut faptul că ”Conduita ulterioară a clientului, constând în achitarea sau neachitarea restanțelor nu prezintă relevanță în ceea ce privește existența faptei contravenționale, în sensul că fapta există, dacă transmiterea a avut loc (...), chiar dacă clientul nu a achitat restanțele (...)”.

În altă cauză similară, Curtea de Apel București a confirmat, prin hotărâre definitivă, cele statuate de instanța de fond, care a reținut faptul că, ”fiind vorba de o sumă restantă, aceasta este o «dată negativă», potrivit art. 3 alin. 2 lit. b) din Decizia nr. 105/2007, astfel că nu se poate reține că societatea petentă nu mai avea obligativitatea în raport de dispozițiile art. 12 alin. (1) din Legea nr. 677/2001 să repete notificările la fiecare transmitere ulterioară a datelor negative despre debitoare”.

De asemenea, instanța a reținut că „Contrar susținerilor din plângerea contravențională, debitoarea (persoana vizată) nu poseda deja informațiile respective și nici nu avea de unde să le cunoască, atâta timp cât acestea se schimbă de la o perioadă la alta de raportare”, precum și faptul că, „concluzia evidentă este aceea că în cauză se impunea informarea persoanei vizate înainte de fiecare raportare cu date negative la Biroul de Credit, fie că acestea erau acumulate din aceeași restanță, sau din una nouă”.

Totodată, în altă speță soluționată definitiv, Curtea de Apel Bucureşti a stabilit că „Dispoziţiile legale prevăd o singură excepţie, şi anume situaţia în care persoana posedă informaţiile respective, astfel că nu pot fi adăugate la lege, pe cale de interpretare sau aplicare, alte excepţii. Situaţia din speţă nu intră sub incidenţa excepţiei prevăzute de art. 12 alin. 1 din Legea nr. 677/2001, întrucât debitorul nu cunoaşte toate informaţiile prevăzute (...) în mod special cele de la lit. d), astfel cum au fost detaliate prin Decizia nr. 105/2007, astfel că o notificare generală (...) nu respectă exigenţele legale".

În altă speță, în care de asemenea instanța s-a pronunțat în mod definitiv, Curtea a statuat faptul că "modalitatea de săvârșire a faptelor (...) presupune o acțiune continuă, iar nu una instantanee, pentru că «faptul de a nu șterge datele negative» în urma unor cereri repetate, precum și «faptul de a nu comunica informațiile», presupune o acțiune care persistă în timp și care se epuizează abia în momentul în care datele au fost șterse și informațiile comunicate", aspecte neprobate de bancă.

De asemenea, în aceeași speță, Curtea a reținut faptul că "Împrejurarea – că respectivii clienți ar fi cunoscut faptul că înregistrează rate restante, că au fost somați în nenumărate rânduri pentru a plăti ori în sensul că au cunoștință de posibilitatea comunicării respectivelor informații negative către Biroul de Credit încă de la momentul semnării contractului de credit – constituie o apărare ce nu poate fi primită deoarece obligațiile legale ale băncii sunt neechivoce, nesusceptibile de vreo interpretare, statuând în mod clar obligația de comunicare a datelor numai după înștiințarea realizată cu cel puțin 15 zile calendaristice înainte de data transmiterii, obligații neîndeplinite, astfel cum corect s-a reținut prin procesul-verbal de contravenție, fapt nedovedit de documentația ce a stat la baza emiterii, depusă la dosarul de fond".

Într-o altă speță, Curtea de Apel a statuat faptul că nu a intervenit prescripția răspunderii contravenționale în ceea ce privește dreptul la informare, întrucât răspunderea contravențională nu a fost angajată pentru neîndeplinirea obligației de informare a clienților, ci această împrejurare a fost reținută ca element circumstanțial în conținutul constitutiv al unei contravenții diferite, constând în refuzul de respectare a dreptului de intervenție (ștergere) asupra datelor.

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

Instanțele de judecată au confirmat măsurile dispuse de Autoritatea Națională de Supraveghere în cazul transmiterii de mesaje comerciale nesolicitate.

Autoritatea Națională de Supraveghere a efectuat o investigaţie 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, reclamându-se totodată lipsa unui răspuns al operatorului la cererea de ștergere.

Analizând probatoriul administrat în cauză, instanţa de fond a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea Națională de Supraveghere este legal întocmit, înlocuind însă măsura amenzii, dispusă prin procesul-verbal, cu măsura avertismentului, pe motiv că operatorul ar fi eliminat ulterior investigației datele personale ale petentului din baza proprie de date, ținând cont, totodată, de lipsa unor antecedente ale operatorului în domeniul protecției datelor cu caracter personal.

Instanța de apel însă, prin hotărârea pronunțată, a admis apelul declarat de Autoritatea Națională de Supraveghere și a schimbat în tot sentința instanței de fond, respingând plângerea operatorului sancționat de Autoritate. Pentru a dispune astfel, în considerentele deciziei pronunțate a arătat că „”Astfel, după cum reiese din textele mai sus citate, o reindividualizare a sancțiunii amenzii în sensul aplicării sancțiunii avertismentului nu se poate realiza decât în ipoteza în care fapta este de o gravitate redusă (…) Curtea apreciază că faptele din sfera protecției datelor cu caracter personal reglementate de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date și Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice nu pot fi apreciate ca fiind fapte de o gravitate redusă decât cu caracter de excepție, având în vedere scopul urmărit de legiuitor, respectiv garantarea și protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal. În acest sens, curtea reține că domeniului

vieții private, respectiv al protecției datelor cu caracter personal i s-a acordat o atenție deosebită la nivel de reglementare internațională."

Alegerea petentei de a nu respecta dispozițiile legale privitoare la transmiterea unui răspuns solicitantului, chiar dacă aceasta este dublată de eliminarea din baza de date, constituie la rândul său contravenție, astfel că nu se poate reține că împrejurările în care a fost săvârșită fapta, modul și mijloacele justifică reindividualizarea sancțiunii aplicate".

Hotărârea instanței favorabilă Autorității Naționale de Supraveghere a rămas definitivă.

- ***Hotărâre pronunțată într-un litigiu privind prelucrarea datelor prin mijloace de localizare geografică precum și prin mijloace de supraveghere video***

Autoritatea Națională de Supraveghere a efectuat o investigație la un operator, ca urmare a unei plângeri având ca obiect prelucrarea datelor cu caracter personal prin intermediul mijloacelor de localizare geografică, precum și prin intermediul mijloacelor de supraveghere video.

În acest sens, Autoritatea Națională de Supraveghere a solicitat operatorului informaţii privind prelucrarea datelor personale prin intermediul mijloacelor menționate mai sus, precum şi documente în susţinerea celor declarate.

Operatorul a răspuns solicitării Autorităţii Naționale de Supraveghere transmiţând documentele pe care le deţinea raportat la această solicitare.

Din documentele puse la dispoziţie de operator a rezultat că acesta nu a notificat prelucrarea datelor privind localizarea geografică și nici a celor privind supravegherea video.

S-a mai constatat că operatorul a instalat în autovehiculele deținute camere de supraveghere video orientate spre șoferi/angajați, încălcând astfel prevederile art. 8 din Decizia Autorității Naționale de Supraveghere nr. 52/2012, cât și prevederile art. 4 alin. (1) lit. a) și c) din Legea nr. 677/2001. De asemenea, operatorul nu a prezentat dovezi din care să rezulte existența unei dispoziții legale sau a avizului autorității

pentru supravegherea video a angajaților societății și nici nu a justificat faptul că interesul operatorului prevalează asupra dreptului la viață privată al șoferilor.

De asemenea, s-a constatat că nu se realiza informarea persoanelor vizate, raportat la prelucrarea datelor de trafic şi de localizare. În ceea ce priveşte sistemul de supraveghere video, s-a constatat că informarea persoanelor vizate nu era în conformitate cu cerinţele art. 12 din Legea nr. 677/2001.

Pentru faptele sus menționate operatorul a fost sancţionat contravenţional, procesul-verbal de constatare/sancţionare contravenţională fiind contestat în instanţă.

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

Hotărârea instanței, favorabilă Autorității Naționale de Supraveghere, a rămas definitivă.

- ***Hotărâre pronunțată într-un litigiu privind prelucrarea datelor biometrice***

Autoritatea Naţională de Supraveghere a efectuat o investigație din oficiu la un operator din mediul privat, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, sub aspectul prelucrărilor de date biometrice, respectiv imaginea facială a propriilor angajați.

În urma investigaţiei efectuate, Autoritatea Națională de Supraveghere a constatat săvârşirea faptei contravenţionale, constând în prelucrarea nelegală a datelor cu caracter personal cu încălcarea prevederilor art. 4 alin. (1) lit. c) din Legea nr. 677/2001, întrucât operatorul a colectat, stocat și prelucrat date biometrice (imaginea facială), prelucrare excesivă față de scopul prelucrării, respectiv pontarea timpului de lucru al angajaților, contravenție prevăzută de art. 32 din Legea nr. 677/2001.

Totodată, în urma investigaţiei, Autoritatea Națională de Supraveghere a constatat săvârşirea faptei contravenţionale constând în neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate cu încălcarea prevederilor art. 20 alin. (5) din Legea nr. 677/2001, întrucât operatorul nu a putut pune la dispoziția echipei de control instrucțiunile în baza cărora persoana împuternicită trebuia

să asigure un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate, contravenție prevăzută de art. 33 din Legea nr. 677/2001.

Prin același proces-verbal de constatare/sancţionare, Autoritatea Națională de Supraveghere a recomandat operatorului de date să adopte, printre altele, și următoarele măsuri:

- ștergerea datelor cu caracter personal (date biometrice – imaginea facială) stocate în aparatul biometric constând în expresia feței angajaților;

- modificarea modului de efectuare a pontajului utilizând alte mijloace pentru atingerea acestui scop, mai puțin intruzive, astfel încât datele biometrice (imaginea facială) să nu mai fie stocate și prelucrate de acest sistem informațional.

Datele biometrice obţinute din structura imaginii faciale constituie date cu caracter personal, întrucât se circumscriu definiţiei date acestora de Legea nr. 677/2001 ca fiind „orice informaţie" referitoare la o persoană fizică, au legătură cu persoane identificabile (în speță, angajații operatorului), astfel că prelucrarea intră sub incidenţa dispoziţiilor Legii nr. 677/2001.

În Avizul nr. 4 privind conceptul de date personale, emis de Grupul de Lucru Art. 29 se precizează următoarele: „Având în vedere formatul sau suportul pe care sunt stocate informaţiile, conceptul de date cu caracter personal cuprinde informaţiile disponibile în orice formă, indiferent că aceasta este, de exemplu, alfabetică, numerică, grafică, fotografică sau acustică. Acesta cuprinde informaţiile scrise pe hârtie, precum şi informaţiile stocate în memoria unui calculator cu ajutorul unui cod binar sau stocate, de exemplu, pe o casetă video. Acest lucru reprezintă o consecinţă logică a faptului că prelucrarea automată a datelor cu caracter personal intră în domeniul de aplicare al acestui concept."

Cât privește mijloacele de identificare, considerentul (26) din Directivă acordă o atenţie specială termenului „identificabil" arătând că „(...) pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată."

Astfel, dacă scopul prelucrării presupune identificarea persoanelor fizice, în speţă angajații operatorului, în scopul permiterii accesului acestora în locațiile sale,

precum și pontarea angajaților ca urmare a identificării acestora la intrarea în locațiile deținute, se poate presupune că operatorul dispune de mijloace „care pot fi utilizate în mod rezonabil" pentru a identifica persoana vizată.

Instanța de fond a respins acțiunea operatorului și a menținut procesul-verbal de constatare/sancționare încheiat de Autoritatea Națională de Supraveghere ca temeinic și legal.

Prin hotărârea sa, instanța de fond a reținut că:

„În privința primei fapte, se constată că, potrivit art. 4 alin. 1 lit. c din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie: (...) c) adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate. Sub acest aspect reclamanta nu a invederat, motivat și nici dovedit în niciun fel prin plângerea sa caracterul neexcesiv al prelucrării datelor prin raportare la scopul de colectare și prelucrare. Aspectele privind existența consimțământului angajaților sau notificarea autorității sunt nerelevante în acest context întrucât pentru înlăturarea răspunderii trebuia arătat și dovedit de ce un altfel de sistem, mai puțin invaziv nu ar fi fost suficient și eficient pentru atingerea scopului declarat. Un asemenea raționament nu a fost prezentat de către reclamantă.

Hotărârea instanței, favorabilă Autorității Naționale de Supraveghere, a rămas definitivă.

- ***Hotărâre pronunțată într-un litigiu privind nerespectarea dreptului de acces la date***

Instanțele de judecată au confirmat măsurile dispuse de Autoritatea Națională de Supraveghere, în cazul nerespectării dreptului de acces.

Astfel, Autoritatea Națională de Supraveghere a efectuat o investigaţie la un operator, ca urmare a unei plângeri prin care o persoană vizată și-a exprimat nemulțumirea față de răspunsul comunicat de către operator, la cererea sa, prin care și-a exercitat dreptul de acces la date, prevăzut de art. 13 din Legea nr. 677/2001, și prin care solicita informatii cu privire la: scopul prelucrării datelor sale cu caracter personal, destinatarii/categoriile de destinatari ai datelor, datele care fac obiectul prelucrării, orice informații disponibile cu privire la originea datelor, activitatea desfășurată, durata activității, veniturile realizate, salariul brut, încadrarea în grupe de

muncă, vechime în muncă și în specialitate conform contractului individual de muncă pe perioada în care acesta a avut calitatea de angajat al operatorului.

Analizând probatoriul administrat în cauză, instanţa de fond a constatat că „prin răspunsul adresat solicitantului (...) operatorul a menționat că pune la dispoziție solicitantului, prin poștă, copia integrală a dosarului personal pe suport de hârtie.

Punerea la dispozitia solicitantului, prin poștă, a copiei dosarului personal pe suport de hârtie, nu echivalează cu comunicarea informațiilor solicitate prin cererea formulată de petent în temeiul art. 13 din Legea nr. 677/2001.

Prin urmare, operatorul nu a comunicat solicitantului toate informațiile solicitate de acesta prin cererea adresată acestuia și prevăzute de art. 3 din Legea nr. 677/2001, respectiv: veniturile totale realizate, salariul brut, vechime în muncă și în specialitate, încadrarea în grupe de muncă, conform contractului individual de muncă pe perioada (...).

Faptul că operatorul a comunicat persoanei vizate (...) răspuns cu referire la prelucrarea datelor sale nu constituie o îndeplinire a obligației prevăzută de dispozițiile art. 13, acesta fiind comunicat ca urmare a recomandării de către Autoritatea Națională de Supraveghere, prin procesul-verbal de constatare/sancționare a contravenției.

Cum, în speță, cu probele administrate s-a facut dovada săvârșirii contravenției de către reclamantă, tribunalul a constatat că procesul-verbal de constatare/sancționare este ”legal și temeinic întocmit.”

În ceea ce privește individualizarea sancțiunii, în concret, ”Tribunalul apreciază că fapta comisă de reclamantă prezintă un grad de pericol social care justifică aplicarea amenzii, în cuantumul stabilit de instituția pârâtă, dat fiind pericolul social al faptei săvârșite, aplicarea sancțiunii contravenționale fiind în concordanță cu dispozițiile art. 21 alin. 3 din OG nr. 2/2001, în limitele prevăzute de Legea nr. 677/2001.”

Hotarârea instanței, favorabilă Autorității Naționale de Supraveghere, a rămas definitivă.

- ***Hotărâre pronunțată într-un litigiu privind prelucrarea datelor prin mijloace de localizare geografică precum și prin mijloace de supraveghere video***

Autoritatea Națională de Supraveghere a efectuat o investigație din oficiu, la un operator, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, precum și respectarea dispozițiilor Legii nr. 506/2004.

Ca urmare a investigaţiei efectuate, Autoritatea Națională de Supraveghere a constatat că operatorul investigat a săvârşit mai multe contravenţii.Astfel, s-a constatat că operatorul, care prelucra date personale în mai multe scopuri, nu notificase prelucrarea datelor personale în scop de localizare geografică a persoanei fizice, deşi instalase pe autovehicule acest sistem încă din anul 2017. Operatorul investigat avea montat un tahometru analog pentru un autovehicul pe care îl utiliza pe diagramă, unde erau notate manual numele și prenumele şoferului (angajat), locul de plecare, data începerii timpului de lucru, data terminării timpului de lucru, timpul de odihnă, nr. de înmatriculare al autovehiculului şi nr. de km parcurşi. Aceste diagrame erau păstrate timp de 30 de zile, iar ulterior erau distruse.

De asemenea, s-a constatat că operatorul nu realiza informarea persoanelor vizate sub forma statuată de Legea nr. 677/2001, nu avea întocmită şi implementată o politică de securitate şi de păstrare a confidenţialităţii datelor prelucrate, care să cuprindă cerinţele minime de securitate a prelucrării datelor cu caracter personal. De asemenea, s-a constatat că, la nivelul site-ului operatorului verificat, nu exista o politică de confidenţialitate şi o politică de cookies, dar nici modalitatea de exprimare a acordului utilizatorului de plasare şi accesare a informaţiilor stocate. Astfel, operatorul prin faptele săvârşite nu respecta dispoziţiile Legii nr. 677/2001 şi ale Legii nr. 506/2004.

Pentru contravenţiile constatate, operatorul a fost sancţionat contravențional, procesul-verbal de constatare/sancţionare fiind contestat în instanţă.

Instanţa, analizând probatoriul administrat în cauză, a constatat că procesul-verbal de constatare/sancţionare emis de Autoritatea Națională de Supraveghere este legal întocmit, fiind menţinute sancţiunile contravenţionale aplicate.

Hotărârea instanței, favorabilă Autorității Naționale de Supraveghere, a rămas definitivă.

Secțiunea a 6-a Informare publică

În cursul anului 2018, Autoritatea Naţională de Supraveghere a continuat activităţile de comunicare destinate informării publicului larg, cu privire la regulile specifice de prelucrare a datelor cu caracter personal, în contextul Regulamentului (UE) 2016/679.

Astfel, a fost organizată Ziua Europeană a Protecţiei Datelor, eveniment de prestigiu ce a fost onorat, ca în fiecare an, 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, precum și în mijloacele de transport în comun ale Regiei Autonome de Transport Bucureşti.

De asemenea, au fost acordate interviuri în cadrul emisiunilor difuzate la posturi naționale de radio, pentru a aduce în atenția publicului larg drepturile de care beneficiază persoanele vizate, potrivit Regulamentului General privind Protecția Datelor.

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

În acest context, subliniem că s-a acordat consultanță mai multor operatori din domeniul public și privat, cu privire la modalitatea de punere în practică a prevederilor Regulamentului General privind Protecția Datelor, fiind explicitate și clarificate o serie de măsuri pe care operatorii sunt obligați să le implementeze în vederea respectării dispozițiilor Regulamentului. Astfel, au fost efectuate întâlniri cu autorități și instituții publice, precum: Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală, Autoritatea Electorală Permanentă, Consiliul Concurenței, Agenția

Națională de Cadastru și Publicitate Imobiliară, ANCOM, ICI, Ministerul Justiției, reprezentanții unor culte din România, Camera Deputaților, Institutul Național de Cercetare-Dezvoltare Medico-Militară „Cantacuzino”, Consiliul Național pentru Studierea Arhivelor Securității (C.N.S.A.S.), Ministerul Educației Naționale, Curtea de Conturi, Avocatul Poporului, Ministerul Afacerilor Europene, Autoritatea de Supraveghere Financiară, Ministerul Afacerilor Interne, Registrul Auto Român, Compania Națională „Poșta Română” SA, Administrația Națională a Penitenciarelor.

În același timp, în contextul continuării acțiunilor de conștientizare a prevederilor Regulamentului, în cursul anului 2018, Autoritatea Națională de Supraveghere a transmis tuturor ministerelor de resort și instituțiilor publice centrale adrese de informare privind aplicarea în plan național, începând cu data de 25 mai 2018, a Regulamentului general privind protecția datelor, principalele obligații generale și specifice, ce le revin în calitate de operator de date, inclusiv sub aspectul obligativității numirii unui responsabil cu protecția datelor în sectorul public.

În ceea ce privește operatorii din sectorul privat, au fost purtate discuții pe aspecte privind condițiile legale de prelucrare a datelor în cadrul întâlnirilor efectuate cu Asociația Română a Băncilor, SC Biroul de Credit SA, Biroul Român de Audit Transmedia, Intesa Sanpaolo Bank, Orange România SA, Asociația pentru Bune Practici GDPR, Asociația Română de Marketing Direct, Biroul Român de Audit Transmedia, Provident Financial România IFN SA.

O informare promptă şi eficientă a persoanelor fizice, dar și a operatorilor, s-a realizat prin site-ul Autorității, la secțiunea specială privind Regulementul General privind Protecția Datelor, dar și în cadrul celor 682 de audienţe acordate la sediul Autorităţii Naţionale de Supraveghere.

S-a remarcat în acest an o creștere semnificativă a audiențelor (638), precum și a solicitărilor de consultare telefonică, în cadrul programului zilnic de relații cu publicul, ceea ce reflectă creșterea nivelului de conștientizare a publicului larg cu privire la regulile de folosire a datelor personale și preocuparea evidentă a operatorilor de respectare a acestor noi reguli.

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

❖ **Ziua Europeană a Protecției Datelor**

Pe data de 28 ianuarie 2018, s-a aniversat Ziua Europeană a Protecţiei Datelor, care a marcat împlinirea a 37 de ani de la semnarea la Strasbourg, în anul 1981, a Convenţiei 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal - primul instrument legal adoptat în domeniul protecţiei datelor.

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

În cinstea Zilei Europene a Protecţiei Datelor, Autoritatea Națională de Supraveghere a organizat, pe data de 26 ianuarie 2018, la Palatul Parlamentului, Conferința cu tema „Aplicarea noului Regulament european privind protecția datelor”, la care au participat conducători ai principalelor autorităţi şi instituţii publice centrale naţionale, ai forului executiv şi ai celui legislativ, reprezentanţi ai mediilor academice, ai organizaţiilor nonguvernamentale, ai principalelor uniuni/asociaţii profesionale din sectorul public şi privat, precum şi ai mass-media.

Cu acest prilej, Autoritatea Națională de Supraveghere a promovat un clip informativ referitor la principalele noutăți stabilite prin Regulamentul General privind Protecția Datelor. Acest clip a fost difuzat, ca mesaj de interes public, la Televiziunea Română și în mijloacele de transport în comun ale Regiei Autonome de Transport Bucureşti, cu impact asupra publicului larg, constituind un mijloc semnificativ de popularizare a noilor reglementări europene.

De asemenea, au fost postate pe website-ul Autorităţii comunicate de presă în legătură cu semnificaţia acestei Zile, precum și broșuri și pliante dedicate acestui eveniment. În același timp, comunicatele de presă au fost transmise și către principalele agenţii de presă româneşti.

Totodată, cu ocazia acestui eveniment, în perioada 8-30 ianuarie 2018, a fost afișat, la sediul Autorităţii, banner-ul cu inscripţionarea „28 ianuarie – Ziua Europeană a Protecţiei Datelor”.

În aceeași zi aniversară, Autoritatea Națională de Supraveghere a organizat evenimentul *„Ziua porților deschise”* , prilej cu care persoanele interesate de domeniul protecţiei datelor au fost invitate la sediul instituţiei noastre și au avut posibilitatea de a vizita zonele deschise publicului şi de a primi informaţii generale privind activitatea specifică a Autorităţii Naţionale de Supraveghere.

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

Autoritatea Națională de Supraveghere a participat la conferința „Data Protection – Soluții și responsabilități” organizată pe data de 23 februarie 2018, în cadrul căreia reprezentantul Autorității a prezentat tema „Consolidarea drepturilor persoanelor vizate din perspectiva RGPD”. În cadrul evenimentului, la care au participat în jur de o sută de reprezentanți ai operatorilor din domeniul public și privat, au avut loc discuții interactive care au pus în lumină multiple chestiuni privind modalitatea de respectare a regulilor de protecție a datelor personale în diferite sectoare de activitate.

În 2 martie 2018, Camera Notarilor Publici București a organizat simpozionul profesional în cadrul căruia reprezentanții Autorității Naționale de Supraveghere au susținut temele „Noutățile aduse de Regulamentul general privind protecția datelor” și „Temeiurile Juridice și Consolidarea Drepturilor Persoanelor Vizate din perspectiva Regulamentului General privind Protecţia Datelor (RGPD)”. În cadrul simpozionului au avut loc dezbateri asupra diverselor probleme puse în discuție de notari, referitoare la aspecte specifice privind protecția datelor personale în cadrul activității notariale.

Pe data de 6 martie 2018, reprezentanții Autorității Naționale de Supraveghere au participat la evenimentul „*Securitate și standardizare în sănătate. Cât de pregătiți suntem pentru implementarea GDPR în mai 2018?*” organizat de New Strategy Center, eveniment adresat operatorilor din domeniul sănătății, atât din sfera publică, cât și privată. În cadrul acestuia, Autoritatea Națională de Supraveghere a prezentat tema „Prelucrarea datelor în domeniul medical din perspectiva Regulamentului general privind protecția datelor (RGPD)”.

Pe data de 15 martie 2018, reprezentanții Autorității Naționale de Supraveghere au participat la un eveniment dedicat informării asupra legislației actuale în domeniul prelucrării datelor cu caracter personal, organizat de Camera de Comerț, Industrie și

Agricultură Galați.

Au fost puse în discuție elementele de noutate aduse de Regulamentul (UE) 2016/679, precum și impactul noii reglementări europene asupra respectării drepturilor persoanelor vizate.

Totodată 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 fost puse în discuție situații distincte ridicate de operatorii participanți, cu referire 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 interesul sectorului privat pentru aplicarea regulilor de prelucrare stabilite de Regulament.

În data de 30 martie 2018, Legal Magazine, cu sprijinul Universității Transilvania Brașov, a organizat o Conferință dedicată noilor reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor.

Participanții la eveniment au pus în discuție situații practice ridicate de operatorii din sistemul public, cu precădere din sistemul de învățământ, cu privire la condițiile de legitimitate ale prelucrărilor efectuate, obligația anumitor categorii de operatori de a păstra o evidență a activităților de prelucrare, notificarea încălcărilor de securitate în condițiile art. 33 din Regulament și evaluarea de impact în conformitate cu art. 35 din același act normativ.

Pe data de 17 aprilie 2018, reprezentanții Autorității Naționale de Supraveghere au participat la un eveniment dedicat noilor reguli de protecție a datelor aduse de Regulamentul General privind Protecția Datelor, în organizarea Universității Titu Maiorescu.

Invitaților prezenți, printre care studenți, dar și reprezentanți ai societăților de avocatură și ai operatorilor din mediul privat, li s-au prezentat principalele schimbări aduse de Regulamentul (UE) 2016/679, aplicabil de la data de 25 mai 2018.

Manifestarea interactivă a participanților în cadrul evenimentului a reliefat interesul deosebit privind conformarea cu noile reguli de prelucrare a datelor personale. Acest eveniment, derulat cu participarea Autorității Naționale de Supraveghere, a fost reflectat în mass-media.

Reprezentanții Autorității Naționale de Supraveghere au participat, în data de 4 mai 2018, la conferința organizată în contextul pregătirii profesionale a avocaților, organizată de Baroul București, în cadrul căruia a fost prezentată tema „Drepturile Persoanelor Vizate din perspectiva Regulamentului General privind Protecţia Datelor (RGPD)". Cu această ocazie, au fost puse în discuție diverse probleme pe care le întâmpină avocații în practică, în ceea ce privește respectarea normelor de protecție a datelor personale.

În data de 15 noiembrie 2018, reprezentanții Autorității Naționale de Supraveghere au participat la Conferința anuală organizată de o societatea de avocatură, intitulată „GDPR – Greu De pus în PRactică?". La acest eveniment, reprezentanții Autorității au adus în atenția participanților principalele „Măsuri legale naționale pentru punerea în aplicare a RGPD" adoptate în anul 2018, atât în ceea ce privește legislația primară, cât și cea secundară. Conferința s-a adresat operatorilor din domeniul privat și public, reunind peste 100 de participanți.

Ziarul Financiar a organizat în anul 2018 mai multe evenimente în cadrul cărora s-au discutat aspecte referitoare la Regulamentul (UE) 2016/679 sau care au avut secțiuni dedicate discuțiilor privind aplicarea acestui nou act normativ.

La Conferințele „Patru Luni până la "ȘOCUL" GDPR", „ZF Insurance – Calea către o creștere sănătoasă a pieței asigurărilor" și Summitul „ZF Digital 2018" s-a înregistrat o prezență numeroasă a reprezentanților mediului privat – companii de telecomunicații, companii de asigurări, entități din cadrul sistemului financiar-bancar etc., participarea interactivă la discuții arătând interesul pentru aplicarea regulilor de prelucrare stabilite de Regulament.

- **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.

Astfel, **secțiunea specială existentă pe pagina de internet a Autorității Naționale de Supraveghere, dedicată Regulamentului General privind Protecția Datelor**, creată încă din anul 2017, a fost în permanență actualizată cu documentele emise de Comitetul European pentru Protecția Datelor și îmbogățită cu alte informații sau documente, inclusiv Ghidul destinat operatorilor emis de instituția noastră.

De asemenea, a fost actualizată secțiunea „Legislație", fiind publicate atât Legea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, precum și Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului general privind protecţia datelor.

Totodată, în scopul popularizării reglementărilor specifice în materie, au fost postate pe pagina de internet a autorității deciziile administrative cu caracter normativ, emise de Autoritatea Națională de Supraveghere, necesare desfășurării în special a activității de soluționare a plângerilor și de efectuare a investigațiilor, precum și pentru abrogarea unor acte administrative emise sub imperiul Legii nr. 677/2001.

În vederea aducerii la cunoștință a activităţii instituţiei, 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 Naţională de Supraveghere.

Toate aceste mijloace și modalități au fost subsumate obiectivului de asigurare a unei informări adecvate a operatorilor, împuterniciților și publicului larg cu privire la noile reguli de prelucrare a datelor cu caracter personal, la obligațiile ce le revin, respectiv la drepturile de care beneficiază sub imperiul Regulamentului General privind Protecția Datelor și a legislației incidente.

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.

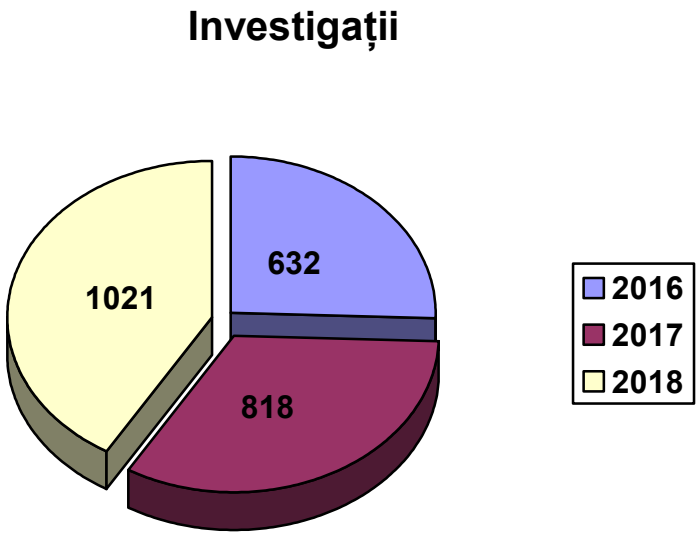
În anul 2018, s-a continuat activitatea intensă de monitorizare și control a regulilor de utilizare a datelor personale la nivelul operatorilor din sectorul public și privat. Astfel, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea prevederilor Legii nr. 677/2001, ale Legii nr. 506/2004, precum și a prevederilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE.

În perioada 1 ianuarie 2018 – 25 mai 2018, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile prelucrării datelor cu caracter personal în cadrul activităților desfășurate în scop de reclamă, marketing și publicitate, prelucrării datelor cu caracter personal colectate prin intermediul web-siteurilor/aplicațiilor on-line și prelucrării datelor cu caracter personal efectuate de operatorii care au ca obiect de activitate furnizarea de servicii de comunicații mobile.

Începând din data de 25 mai 2018, dată la care a fost pus în aplicare și în România Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 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, investigațiile din oficiu au avut ca obiect verificarea respectării prevederilor legale ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, potrivit art. 33 alin. (1) din RGPD, precum și ca urmare a sesizărilor transmise Autorității Naționale de Supraveghere.

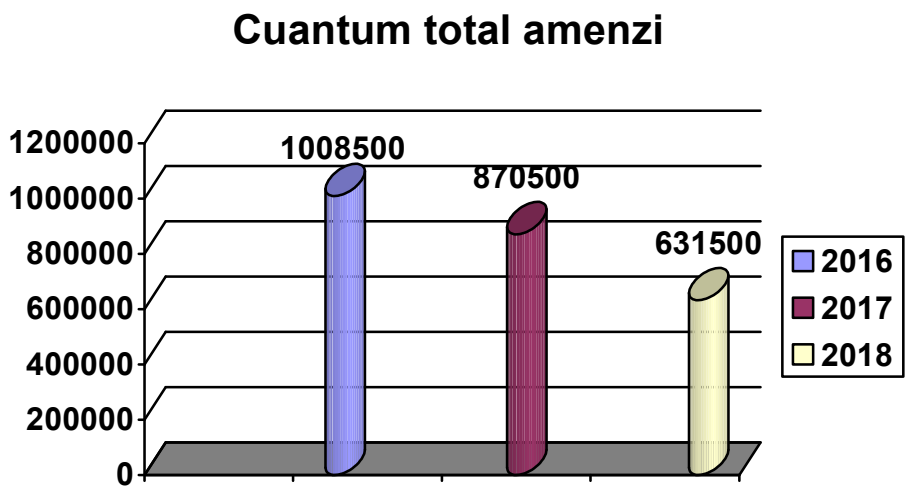
În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul unei creșteri exponențiale a numărului acestora (4822 plângeri și 200 sesizări), în anul 2018 au continuat să fie sesizate în principal încălcări ale legislației din domeniul financiar-bancar, cu precădere, cele care vizează prelucrarea 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 demarate de Autoritatea Națională de Supraveghere în anul 2018 a fost de **1021**, dintre care până la data de 25 mai 2018 au fost demarate 391 de investigații, iar începând cu 25 mai 2018 au fost 630 de investigații.



În urma investigațiilor efectuate au fost aplicate sancțiuni contravenționale constând în **56 amenzi și 124 avertismente**. De asemenea, au fost aplicate o serie de măsuri corective în baza dispozițiilor art. 58 alin. (2) lit c) și d) din Regulamentul General privind Protecția Datelor

Cuantumul total al amenzilor aplicate în 2018 a fost de **631.500 lei.**



Menționăm că, pe parcursul anului 2018, au fost întreprinse demersuri de către Autoritatea Națională de Supraveghere, destinate pregătirii punerii în aplicare a Regulamentului General privind Protecția Datelor, în acest context înscriindu-se și adoptarea de procedurii de efectuare a investigațiilor (Decizia nr. 161/2018) și, respectiv, a procedurii de primire și soluționare a plângerilor (Decizia nr. 133/2018)

Secțiunea a 2-a. Investigații din oficiu

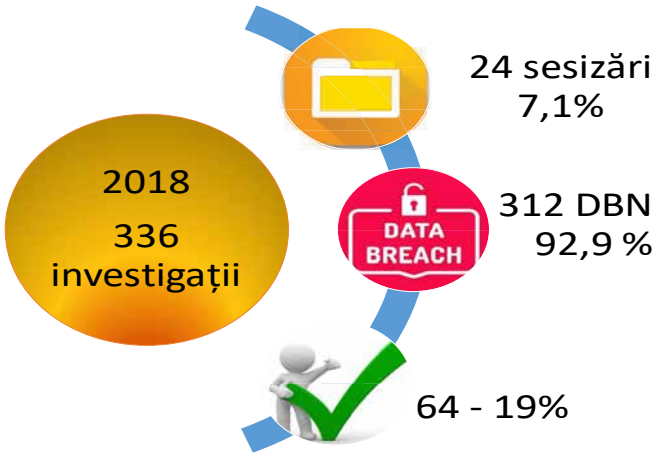
În anul 2018, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile în cadrul prelucrării datelor cu caracter personal, atât în sistemul public, cât și în cel privat.

Investigațiile din oficiu efectuate au avut ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001, a dispoziţiilor Legii nr. 506/2004, precum și a prevederilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecţia persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE.

Astfel, până la data de 25 mai 2018, au fost efectuate 60 de investigații din oficiu. Ulterior intrării în vigoare a Regulamentului General privind Protecția Datelor, au fost efectuate 64 de investigații din oficiu, ca urmare a notificării incidentelor de securitate a prelucrării datelor cu caracter personal, respectiv ca urmare a primirii de sesizări.

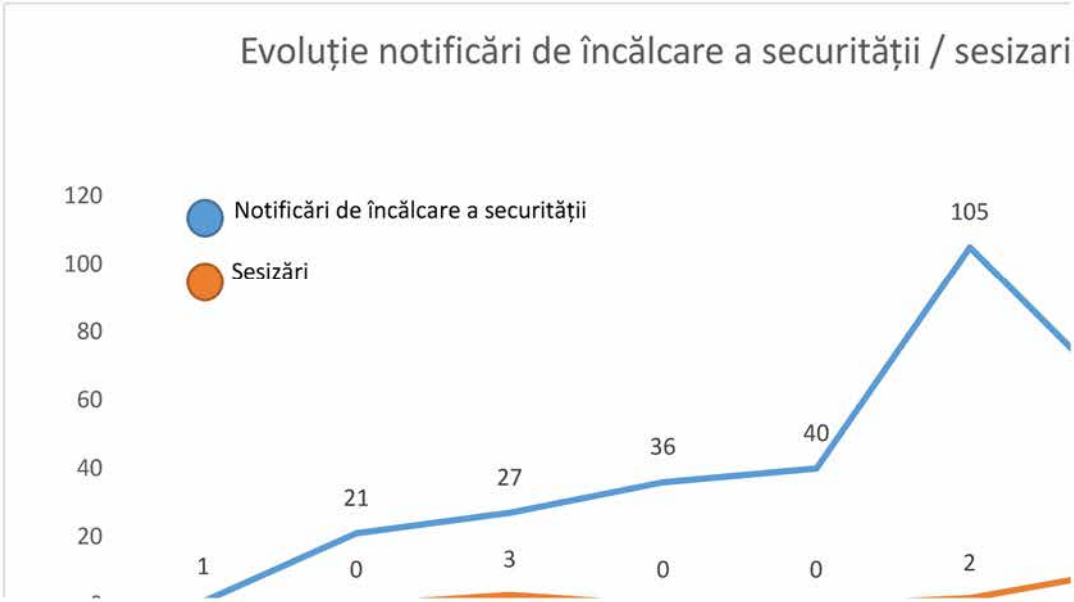
Începând cu data de 25 mai 2018, au fost demarate 336 de investigații din oficiu, în aplicarea Regulamentului General privind Protecția Datelor.

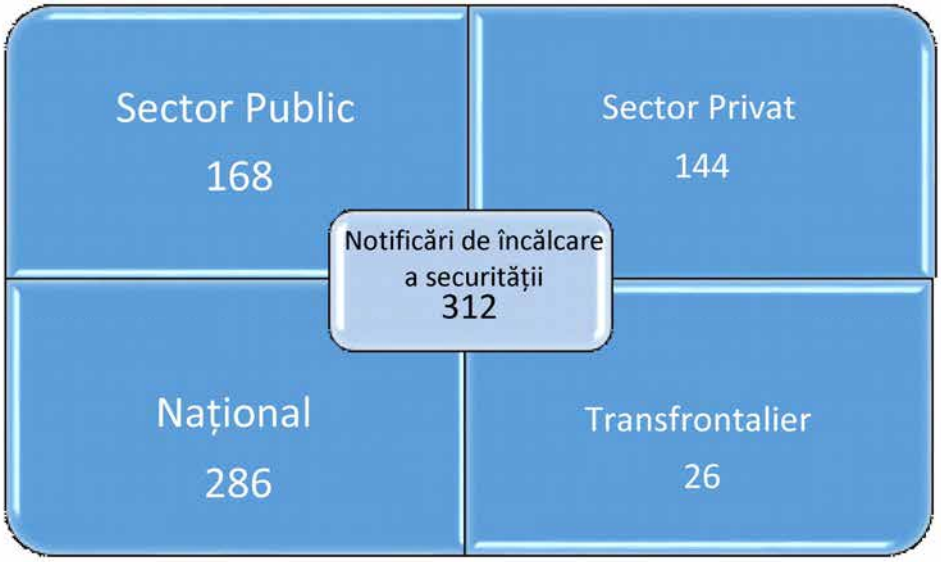
Dintre acestea, 64 de investigații au fost finalizate prin transmiterea de recomandări operatorilor de date cu caracter personal privind respectarea prevederilor Regulamentului General privind Protecția Datelor.



Autoritatea Națională de Supraveghere a primit un număr total de 312 notificări de încălcare a securității datelor cu caracter personal (DBN), precum și un număr total

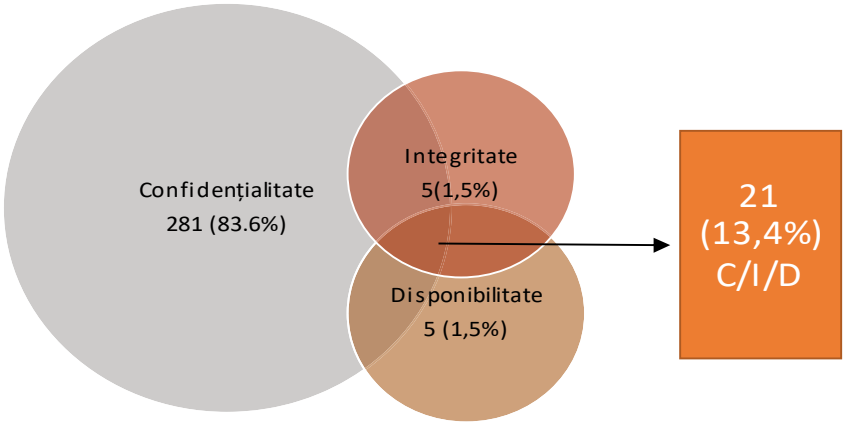
de 24 de sesizări privind posibilitatea încălcării prevederilor Regulamentului general privind protecția datelor în domeniul bancar, telecomunicații, publicații online etc., iar media lunară (mai-decembrie) a notificărilor de încălcare a securității a fost de 42 de notificări primite de Autoritatea Națională de Supraveghere.





În ceea ce privește notificările încălcărilor de securitate, 168 au vizat sectorul public și 144 sectorul privat. Totodată, 286 de notificări reprezintă incidente de securitate la nivel național.

Având în vedere clasificarea incidentelor de securitate prevăzută în „Ghidul privind notificarea încălcărilor de securitate", emis de Grupul de Lucru Articolul 29 și aprobat de Comitetul European pentru Protecția Datelor, aproximativ 83% (281 de incidente) dintre acestea au fost de tipul Confidențialitate. În unele cazuri, notificările de încalcare a securității datelor cu caracter personal (21) au fost clasificate, de către operatorii care au transmis notificările, ca fiind mixte (confidențialitate/integritate, confidențialitate/disponibilitate, integritate/disponibilitate, respectiv confidențialitate/integritate/disponibilitate).



I. Încălcarea dreptului de acces - FIȘĂ DE CAZ

Autoritatea Națională de Supraveghere s-a sesizat din oficiu cu privire la răspunsul comunicat de către o societate comercială unei persoane vizate (persoană fizică) ca urmare a exercitării de către aceasta a dreptului de acces la date, conform art. 13 din Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, modificată și completată.

Persoana vizată, fost angajat al operatorului, s-a adresat acestuia printr-o cerere prin care își exercita dreptul de acces la datele sale cu caracter personal, solicitând informații referitoare la: scopul prelucrării datelor sale cu caracter personal, destinatarii/categoriile de destinatari ai datelor, datele care fac obiectul prelucrării, orice informații disponibile cu privire la originea datelor, activitatea desfășurată de către persoana vizată, durata activității persoanei vizate, veniturile realizate, salariul

brut, încadrarea în grupe de muncă, vechime în muncă și în specialitate, conform contractului individual de muncă pe perioada în care aceasta a fost angajată.

Societatea a transmis un răspuns persoanei vizate, prin care i-a oferit informații generale cu privire la operațiunile de prelucrare a datelor efectuate, însă nu i-a furnizat informații cu privire la toate datele necesare, conform art. 13 alin. (1) din Legea nr. 677/2001.

În urma investigaţiei efectuate, operatorul a fost sancţionat contravențional pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001, raportat la art. 13 din aceeași lege, întrucât nu a comunicat persoanei vizate toate informațiile pe care avea obligația să i le comunice.

Totodată, Autoritatea Națională de Supraveghere a recomandat operatorului să transmită persoanei vizate un răspuns complet la cererea sa, cu respectarea art. 13 din Legea nr. 677/2001.

II. Utilizarea de tehnologii de plasare de informaţii, web-bug sau tracking code - FIȘĂ DE CAZ

Autoritatea Națională de Supraveghere a primit, la adresa de e-mail, mai multe plângeri care conțineau următorul text: „*NOTA! Mesajul, are ataşat un cod de urmărire şi raportare continuă a stării (TRAKING CODE) motiv pentru care vă rugăm să evitaţi posibilitatea de a nega faptul că acest mesaj a fost expediat la adresa Dumneavoastră de mail, respectiv că nu aţi primit mesajul*".

Ca urmare a verificărilor demarate la nivelul aplicației proprii de management al documentelor, s-a constatat că plângerile erau transmise de pe adrese de e-mail ale unor domenii de internet care conțineau „web-bug" sau „tracking pixel". Totodată, ca urmare a verificărilor efectuate, Autoritatea Națională de Supraveghere a constatat că, de la mai multe adrese de e-mail ale domeniilor de internet menționate anterior, au fost transmise e-mailuri care conțineau un „web-bug" sau „tracking pixel" (identificat sub denumirea de „tracking code") în corpul mesajelor primite și către alți operatori economici.

Față de cele de mai sus, Autoritatea Națională de Supraveghere s-a sesizat din oficiu referitor la utilizarea de web-bug sau tracking code – tehnologii de plasare de informaţii şi accesarea acestor informaţii din echipamentul terminal (staţii de lucru –

calculatoare), demarând o investigație la deținătorul domeniilor de internet ale adreselor de e-mail de la care au fost transmise plângerile.

Astfel, Autoritatea Națională de Supraveghere a solicitat informații referitoare la scopul utilizării de web-bug/tracking pixel/tracking code în cadrul comunicărilor electronice (e-mail); sursa acestui web-bug/tracking pixel/tracking code (dacă este dezvoltat de către deținătorul domeniilor sau de o terță parte), modul de funcționare, precum și o descriere a elementelor HTML ale acestui web-bug/tracking pixel/tracking code; data la care a început această prelucrare (colectare, urmărire și raportare continuă a stării), precum și, dacă este cazul, data încetării acestei prelucrări de informații prin aceste comunicări electronice; de câte ori s-a utilizat, la nivelul domeniilor deținute, această metodă de urmărire și raportare continuă a stării comunicațiilor electronice; modalitatea prin care s-au adus la cunoștința persoanelor vizate (utilizatori ai adreselor de e-mail) drepturile prevăzute de art. 12-18 din Legea nr. 677/2001; modalitatea de obținere a consimțământului persoanelor vizate privind această prelucrare/colectare (urmărire și raportare continuă a stării) prin aceste comunicări electronice; care este perioada de stocare a informațiilor colectate prin urmărirea și raportarea continuă a stării comunicațiilor electronice, precum și destinația acestor informații colectate.

Ca urmare a investigației efectuate, s-a constatat că operatorul investigat, la nivelul domeniilor proprii de Internet utilizate, servicii ale societății informaționale, a încălcat confidențialitatea comunicărilor, contrar dispozițiilor art. 4 alin. (2) din Legea nr. 506/2004, modificată și completată, care statuează că „Ascultarea, înregistrarea, stocarea şi orice altă formă de interceptare ori supraveghere a comunicărilor şi a datelor de trafic aferente sunt interzise, cu excepţia cazurilor următoare: a) se realizează de utilizatorii care participă la comunicarea respectivă; b) utilizatorii care participă la comunicarea respectivă şi-au dat, în prealabil, consimţământul scris cu privire la efectuarea acestor operaţiuni; c) se realizează de autorităţile competente, în condiţiile legii.”

De asemenea, s-a constatat că la nivelul domeniilor de Internet proprii, servicii ale societății informaționale, pentru informațiile stocate în echipamentele terminale ale utilizatorilor, operatorul nu a îndeplinit în mod cumulativ condițiile prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004, respectiv obținerea acordului utilizatorului

în cauză pentru modulele web-bug/tracking pixel/tracking code utilizate în corespondența electronică cu diferite adrese de e-mail și furnizarea informațiilor anterior exprimării acordului privind scopul general al procesării informațiilor stocate, durata de viață, informațiile stocate și accesate, precum și permiterea stocării și/sau accesului unor terți la informațiile stocate în echipamentul terminal al utilizatorului (stații de lucru, smartphones – mijloace automate de prelucrare a datelor cu caracter personal).

Precizăm că Grupul de lucru Articolul 29 (Grupul privind protecția datelor personale de pe lângă Comisia Europeană, în prezent Comitetul European pentru Protecția Datelor), în Avizul nr. 2/2010, subliniază că publicitatea comportamentală implică prelucrarea unor identificatori unici, indiferent dacă acest lucru se realizează prin utilizarea modulelor cookie sau a oricărui tip de dispozitive de identificare. Utilizarea acestor identificatori unici permite urmărirea utilizatorilor unui anumit calculator, chiar și în cazul în care adresele IP sunt șterse sau anonimizate. Cu alte cuvinte, acești identificatori unici permit ca persoanele vizate să fie „recunoscute" în vederea urmăririi comportamentului lor ca utilizatori în timp ce navighează pe diferite site-uri și, prin urmare, se poate considera că sunt date cu caracter personal.

Totodată, art. 5 alin. (3) din Directiva 2002/58/CE, astfel cum a fost modificată prin Directiva 2009/136/CE, a consolidat protecția utilizatorilor de rețele și servicii de comunicații electronice, introducând obligația operatorilor/furnizorilor de a obține consimțământul exprimat în cunoștință de cauză al utilizatorului (sau al abonatului) înainte de a stoca informații sau de a dobândi accesul la informațiile stocate în echipamentul terminal al acestuia. Cerința se aplică tuturor tipurilor de informații stocate sau accesate în echipamentul terminal al utilizatorului [...].

Față de cele de mai sus, în urma investigaţiei efectuate, operatorul reclamat a fost sancţionat contravențional pentru încălcarea art. 4 alin. (5) din Legea nr. 506/2004, modificată și completată, întrucât operatorul, la nivelul domeniilor proprii de Internet utilizate, servicii ale societății informaționale, pentru informațiile stocate în echipamentele terminale ale utilizatorilor nu a îndeplinit în mod cumulativ condițiile prevăzute de art. 4 alin. (5), lit. a) și b) din Legea nr. 506/2004, respectiv: a) obținerea acordului utilizatorului în cauză pentru modulele web-bug/tracking pixel/tracking code utilizate în corespondența electronică cu diferite adrese de email și

b) furnizarea informațiilor anterior exprimării acordului 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 (stații de lucru, smartphones, mijloace automate de prelucrare a datelor cu caracter personal), contravenție prevăzută de art. 13 alin. (1) lit. i) din Legea nr. 506/2004, modificată și completată. De asemenea, operatorul a fost sancționat pentru nerespectarea prevederilor art. 4 alin. (2) referitoare la interdicţia interceptării şi supravegherii comunicărilor şi datelor de trafic aferente, respectiv stocarea şi orice altă formă de interceptare ori supraveghere a comunicărilor şi a datelor de trafic aferente, întrucât, la nivelul domeniilor proprii de Internet, servicii ale societății informaționale, prin utilizarea modulelor web-bug/tracking pixel/tracking code, supraveghează e-mailurile transmise (comunicările transmise prin intermediul serviciilor de comunicații electronice), fără ca destinatarii acestora să-și fi dat în prealabil consimțământul scris cu privire la efectuarea acestor operațiuni, fiind colectate informaţii privind data la care a fost deschis respectivul e-mail, adresa IP de la care a fost deschis şi chiar dispozitivul folosit, contrar articolului 4, alineatul (2), din Legea nr. 506/2004, modificată și completată.

III. Accesul neautorizat la datele cu caracter personal ale unor persoane fizice de pe teritoriul României, prelucrate de către un operator care nu este stabilit în România - FIȘĂ DE CAZ

Autoritatea Națională de Supraveghere s-a sesizat din oficiu privind accesul neautorizat la datele cu caracter personal ale unor persoane fizice de pe teritoriul României/utilizatori din România, prelucrate de către un operator care nu este stabilit în România (Statele Unite ale Americii), prin intermediul unor aplicații disponibile doar pentru telefoane inteligente, oferite pe platforma electronică a operatorului.

Potrivit prevederilor art. 2 alin. (2) lit. c) și art. 2 alin. (3) din Legea nr. 677/2001, prevederile acestei legi se aplică și prelucrărilor de date cu caracter personal efectuate în cadrul activităţilor desfăşurate de operatori care nu sunt stabiliţi în România, prin utilizarea de mijloace de orice natură situate pe teritoriul României, cu excepţia cazului în care aceste mijloace nu sunt utilizate decât în scopul tranzitării pe

teritoriul României a datelor cu caracter personal care fac obiectul prelucrărilor respective. În acest caz operatorul îşi va desemna un reprezentant care trebuie să fie o persoană stabilită în România.

Față de cele de mai sus, investigația s-a desfășurat la reprezentantul operatorului, o societate comercială cu sediul în România, având în vedere că, potrivit prevederilor art. 2 alin. (3) din Legea nr. 677/2001, prevederile legii aplicabile operatorului sunt aplicabile şi reprezentantului acestuia, fără a aduce atingere posibilităţii de a introduce acţiune în justiţie direct împotriva operatorului.

Ca urmare a investigației efectuate, Autoritatea Națională de Supraveghere a fost informată că incidentul de încălcare a securității datelor cu caracter personal, de tip hacking, a presupus accesarea de informații privind aproximativ 57 de milioane de utilizatori din întreaga lume (aproximativ 32 de milioane de persoane dintre acestea se găsesc în afara Statelor Unite ale Americii, inclusiv aproximativ 30.000 de persoane din România). La nivelul Uniunii Europene, acest incident de încălcare a securității datelor cu caracter personal a afectat utilizatori din toate cele 28 de state membre.

Astfel, în mod ilegal au fost accesate date cu caracter personal și s-au efectuat copii ale acestora.

Pentru aproximativ toți utilizatorii, fișierele descărcate au inclus numele, adresele de e-mail și numerele de telefon mobil. În unele cazuri, fișierele includeau și alte informații colectate de la utilizatori sau create de operator în legătură cu utilizatorii, de exemplu ID-ul intern de utilizator; fișierul unui utilizator care a invitat un alt utilizator să se înregistreze în aplicație sau cu care utilizatorii au partajat călătorii dacă au optat pentru anumite programe; o serie de scurte observații privind șoferii (profile automate); anumite informații unice de localizare (date de geolocalizare), precum latitudinea și longitudinea corespunzătoare locului unde utilizatorul s-a înregistrat pentru prima oară în aplicație; precum și alte informații de cont, inclusiv token-urile de utilizator și parole de utilizator hash sau salted.

Aplicațiile oferite de platforma electronică a operatorului se subscriu serviciilor societății informaționale și reprezintă servicii de comunicații electronice care constau în întregime/în principal în transmiterea semnalelor prin reţelele de comunicaţii electronice, prin intermediul Internetului, privind prelucrările de date cu caracter

personal efectuate prin mijloace automate (aplicații/terminale mobile smartphone) pe teritoriul României.

Incidentul produs intră în categoria unei încălcări a securității datelor cu caracter personal, așa cum este definit de Legea nr. 506/2004, modificată și completată, respectiv distrugerea accidentală sau ilicită, pierderea, alterarea, divulgarea neautorizată ori accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate.

Față de cele de mai sus, în urma investigaţiei efectuate, operatorul a fost sancţionat contravențional pentru neîndeplinirea obligației de informare prevăzute la art. 3 alin. (6) din Legea nr. 506/2004, modificată și completată, întrucât operatorul nu a îndeplinit obligația de informare, prin notificarea fără întârziere către ANSPDCP a încălcării securității datelor cu caracter personal, precum și pentru neîndeplinirea obligației de informare prevăzute la art. 3 alin. (7) din Legea nr. 506/2004, modificată și completată, întrucât operatorul nu a îndeplinit obligația de informare, prin notificarea în mod individual, fără întârziere, a tuturor persoanelor vizate/utilizatori din România afectați de incidentul de securitate a datelor cu caracter personal.

Totodată, Autoritatea Națională de Supraveghere a solicitat operatorului investigat notificarea/informarea încălcării securității datelor cu caracter personal, în mod individual, a tuturor persoanelor vizate/utilizatori din România afectați de incidentul de securitate a datelor cu caracter personal.

Ca urmare a solicitării ANSPDCP, operatorul investigat a notificat în mod individual persoanele vizate afectate.

IV. Prelucrarea nelegală a datelor cu caracter personal ale unui abonat de către un partener contractual al operatorului - FIȘĂ DE CAZ

Autoritatea Națională de Supraveghere a efectuat o investigație la un furnizor de servicii de telefonie mobilă, referitor la prelucrarea nelegală a datelor cu caracter personal ale unei persoane fizice/abonat, de către un partener contractual al operatorului, în scopul emiterii unei facturi, prin accesarea ilegală a bonusului Phone credit acordat de către furnizorul de servicii de telefonie mobilă persoanei fizice în cauză.

Ca urmare a investigației efectuate, s-a constatat că incidentul s-a datorat unei erori umane de natură internă a unui angajat al partenerului contractual al operatorului, care avea calitatea de împuternicit pentru prelucrarea datelor cu caracter personal.

Față de cele de mai sus, operatorul investigat a fost sancționat contravențional pentru „Prelucrarea nelegală a datelor cu caracter personal", prevăzută de art. 32 din Legea nr. 677/2001, întrucât operatorul, prin împuternicitul său, a prelucrat datele cu caracter personal ale persoanei vizate/abonat, fără consimțământul acesteia, în scopul emiterii unei facturi prin accesarea bonusului acordat acesteia de către operator, precum și pentru „Neîndeplinirea obligațiilor privind confidențialitatea și aplicarea măsurilor de securitate", prevăzută de art. 33 din Legea nr. 677/2001, întrucât operatorul, prin împuternicitul său, nu a luat măsuri suficiente împotriva accesului neautorizat, al unui angajat al împuternicitului, la datele cu caracter personal ale persoanei vizate/abonat din aplicația de facturare a operatorului și folosirii acestora în vederea emiterii unei facturi în mod ilegal.

Ca urmare a constatărilor de mai sus, raportat la prevederile art. 2 lit. h) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, modificată şi completată, Autoritatea Națională de Supraveghere a apreciat că incidentul produs intră în categoria unei încălcări a securității datelor cu caracter personal așa cum este definită de legea sus-menționată, respectiv încălcarea securităţii având ca rezultat distrugerea accidentală sau ilicită, pierderea, alterarea, divulgarea neautorizată ori accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod în legătură cu furnizarea de servicii de comunicaţii electronice destinate publicului.

Astfel, operatorul investigat a fost sancționat contravențional și pentru neîndeplinirea obligaţiei de informare prevăzută la art. 3 alin. (6) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, modificată şi completată, întrucât acesta nu a îndeplinit obligația de informare, prin notificarea fără întârziere către Autoritatea Națională de Supraveghere a încălcării securității datelor cu caracter personal, deși operatorul avea cunoștință de acest incident de securitate, așa cum este definit de Legea nr. 506/2004, precum și de obligațiile legale aflate în sarcina sa.

Totodată, s-a recomandat operatorului să respecte prevederile Deciziei 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) 2013/611 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.

V. Verificarea respectării prevederilor legale referitoare la prelucrarea datelor cu caracter personal de către operatorii care au ca obiect de activitate furnizarea de servicii de comunicații mobile

Autoritatea Națională de Supraveghere a dispus efectuarea de investigații la mai multe entități care prelucrează date cu caracter personal având ca obiect principal de activitate „Activități de telecomunicații prin rețele fără cablu (exclusiv prin satelit)”. Autoritatea Națională de Supraveghere a controlat, până la data de 25 mai 2018, patru mari furnizori de servicii de comunicații mobile.

Referitor la entitățile controlate, specificăm că, în vederea realizării obiectului de activitate, acestea încheie cu clienți persoane fizice (abonați) contracte pentru furnizarea de servicii de telefonie mobilă, pentru clienții noi și clienții existenți (prelungire contract), și reziliază contracte în baza cererilor de reziliere.

Datele personale prelucrate în scopul încheierii de contracte pentru furnizarea de servicii de comunicații mobile, în general, sunt aceleași pentru toți operatorii controlați, și anume: nume, prenume, telefon, adresă de e-mail, cetățenie, serie și număr BI/CI, CNP, semnătură și adresă de domiciliu.

Pe lângă acestea, operatorii controlați colectează copii ale actelor de identitate ale persoanelor fizice, respectiv copii ale BI/CI/pașaport/permis de ședere. Colectarea acestor copii de acte de identitate se efectuează atât la punctele de lucru ale operatorilor, cât și la punctele de lucru ale împuterniciților.

În contracte există clauze referitoare la acordul clientului, unde se precizează că acesta își exprimă acordul cu privire la prelucrarea CNP și a copiei actului de identitate, însă nu se oferea clientului posibilitatea de a opta pentru o astfel de prelucrare.

În urma investigațiilor efectuate de Autoritatea Națională de Supraveghere, s-a constatat că toți operatorii controlați au prelucrat în mod excesiv date cu caracter personal ce intrau sub incidența art. 8 din Legea nr. 677/2001, modificată și completată, și au reținut prin colectare și stocare copii ale actelor de identitate ale persoanelor fizice cu care au încheiat contracte de furnizare de servicii de comunicații electronice, fără a avea consimțământul expres al acestor persoane fizice, în lipsa unui temei legal sau a unui aviz al Autorității Naționale de Supraveghere.

În temeiul prevederilor art. 4 alin. (1) lit. c), ale art. 5 și art. 8 din Legea nr. 677/2001 și ale art. 2 și art. 6 din Decizia ANSPDCP nr. 132/2011, coroborate cu prevederile art. 21 alin. (3) lit. d) şi ale art. 27 din Legea nr. 677/2001, raportate la art. 3 alin. (5) coroborat cu art. 13 din Legea nr. 102/2005, Președintele Autorităţii Naţionale de Supraveghere a emis decizii de ștergere/distrugere a datelor cu caracter personal privind codul numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală, inclusiv a copiilor după actele de identitate care le conțin, deja colectate de către operatorii investigați, fără consimțământul expres al persoanelor vizate, fără temei legal sau fără avizul Autorității Naționale de Supraveghere.

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

I. Prezentare generală

Pe parcursul anului 2018, Autoritatea Națională de Supraveghere a continuat să își îndeplinească una dintre principalele atribuții legale, legate de obiectivul pentru care a fost înființată, respectiv 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, prin soluționarea plângerilor și a sesizărilor ce vizează încălcarea acestui drept.

Aceste competențe au fost consolidate prin Regulamentul (UE) 2016/679, aplicabil din 25 mai 2018, și prin legislația națională de implementare a prevederilor acestuia, respectiv prin Legea nr. 102/2005, așa cum a fost modificată și completată prin Legea nr. 129/2018, precum și prin Legea nr. 190/2018.

Astfel, cadrul legislativ privind depunerea și soluționarea plângerilor la Autoritatea Națională de Supraveghere după data de 25 mai 2018 este asigurat în principal de art. 77 din Regulamentul General privind Protecția Datelor, conform căruia „orice persoană vizată are 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, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezentul regulament.” Potrivit acestor prevederi, autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul art. 78 din Regulamentul General privind Protecția Datelor.

Aceste dispoziții sunt implementate prin art. 20-21 din Legea nr. 102/2005, republicată, și puse în aplicare prin procedura de primire și soluționare a plângerilor, aprobată prin Decizia nr. 133/2018 a președintelui Autorității Naționale de Supraveghere. În cazul în care plângerea este depusă prin intermediul unui organism, al unei organizaţii, al unei asociaţii sau fundaţii fără scop patrimonial, acestea trebuie să dovedească faptul că au fost constituite legal, cu un statut ce prevede obiective de interes public, şi că sunt active în domeniul protecţiei drepturilor şi libertăţilor persoanelor vizate în ceea ce priveşte protecţia datelor lor cu caracter personal.

Condițiile necesare pentru depunerea plângerilor și pentru analizarea admisibilității acestora, precum și procedura de soluționare sunt făcute publice pe pagina de Internet a Autorității Naționale de Supraveghere, în cadrul unei secțiuni dedicate, unde este disponibil și un formular electronic pentru cei care doresc să folosească această modalitate de adresare a unei plângeri, așa cum prevede și art. 57 alin. (2) din Regulamentul General privind Protecția Datelor.

În Comunicarea Comisiei Europene către Parlamentul European şi Consiliu din 24 ianuarie 2018, intitulată „Protecţie sporită, noi oportunităţi – Orientările Comisiei privind aplicarea directă a Regulamentului general privind protecţia datelor de la 25 mai 2018”, s-a precizat că „În momentul adaptării legislaţiei lor naţionale, statele membre trebuie să ia în considerare faptul că orice măsuri naţionale care ar avea ca rezultat crearea unui obstacol în calea aplicării directe a regulamentului şi punerea în

pericol a aplicării simultane şi uniforme a acestuia în întreaga UE sunt contrare tratatelor."

În acest context, Legea nr. 677/2001, precum și deciziile emise anterior de Autoritatea Națională de Supraveghere au fost abrogate începând cu data de 25 mai 2018, când a fost pus în aplicare Regulamentul General privind Protecția Datelorîn toate statele membre ale Uniunii Europene, inclusiv în România. Modificările aduse Legii nr. 102/2005 prin Legea nr. 129/2018 au fost publicate în Monitorul Oficial nr. 503 din 19 iunie 2018, iar Decizia nr. 133/2018, în Monitorul Oficial nr. 600 din 13 iulie 2018.

De asemenea, Decizia nr. 161/2018 privind aprobarea procedurii de efectuare a investigațiilor, care conține inclusiv formularul de proces-verbal de constatare și sancționare a contravențiilor, a fost publicată în Monitorul Oficial nr. 892 din 23 octombrie 2018.

Printre alte dispoziții tranzitorii, art. VI din Legea nr. 129/2018 prevede următoarele:

„(1) Dispoziţiile Regulamentului general privind protecţia datelor se aplică plângerilor şi sesizărilor depuse şi înregistrate la Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal începând cu data aplicării acestuia, precum şi celor depuse înainte de 25 mai 2018 şi aflate în curs de soluţionare. Investigaţiile efectuate pentru soluţionarea acestora şi investigaţiile din oficiu, începute anterior datei de 25 mai 2018 şi nefinalizate la această dată, sunt supuse dispoziţiilor aceluiaşi regulament.

(2) Constatarea faptelor şi aplicarea măsurilor corective, inclusiv a sancţiunilor contravenţionale, după data de 25 mai 2018, se realizează în conformitate cu prevederile Regulamentului general privind protecţia datelor şi cu cele ale dispoziţiilor legale de punere în aplicare a acestuia, ale Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, precum şi cu cele aduse prin prezenta lege.

(3) În cazul în care Regulamentul general privind protecţia datelor şi dispoziţiile legale de punere în aplicare a acestuia prevăd o sancţiune mai gravă, contravenţia săvârşită anterior datei de 25 mai 2018 va fi sancţionată conform dispoziţiilor actelor

normative în vigoare la data săvârşirii acesteia. În situaţiile în care, potrivit Regulamentului general privind protecţia datelor şi dispoziţiilor legale de punere în aplicare a acestuia, fapta nu mai este considerată contravenţie, aceasta nu se mai sancţionează, chiar dacă a fost săvârşită înainte de data de 25 mai 2018."

Prin urmare, în anul 2018, activitatea de soluționare a plângerilor (și sesizărilor) desfășurată de Autoritatea Națională de Supraveghere a fost axată, în principal, pe două paliere: primirea, analizarea și soluționarea plângerilor, respectiv finalizarea investigațiilor începute pentru plângerile depuse sub regimul Legii nr. 677/2001, precum și primirea, analizarea, soluționarea și demararea investigațiilor în cazul plângerilor depuse după data de 25 mai 2018.

Printre considerentele pentru care plângerile și sesizările nu au putut fi reținute în vederea efectuării unor demersuri de către autoritate pot fi enumerate:

- neprezentarea dovezilor în susţinerea aspectelor reclamate sau a calității de reprezentant al persoanei vizate (ex. lipsa împuternicirii avocațiale sau a unui mandat emis conform dispozițiilor legale aplicabile);

- sesizarea unor fapte în legătură cu care Autoritatea Națională de Supraveghere nu deține competenţa legală materială (ex. aspecte care țin de aplicarea legislației din domeniul protecției drepturilor consumatorilor sau din domeniul dreptului penal);

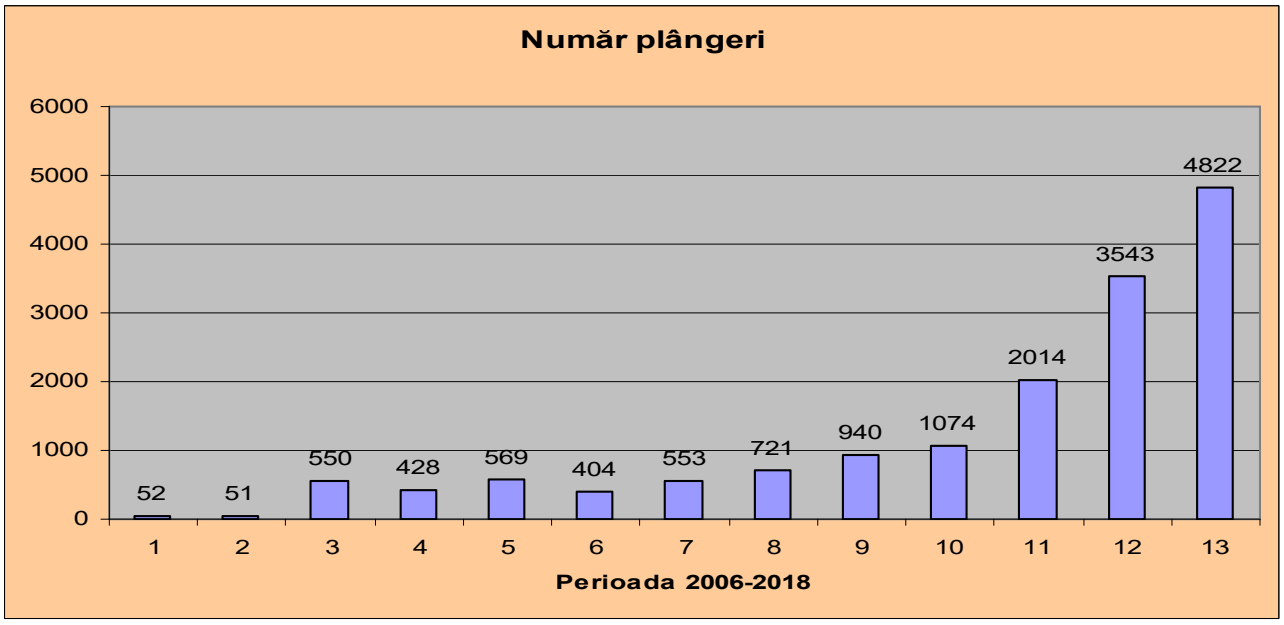
- imposibilitatea identificării exacte a entității reclamate (ex. neidentificarea certă a expeditorului unei comunicări comerciale electronice nesolicitate sau a deținătorului unui website).

În anul 2018, **numărul petițiilor** soluționate de Autoritatea Națională de Supraveghere **a crescut cu peste 30%** prin raportare la anul 2017. Astfel, au fost primite şi soluţionate un număr de **4822 plângeri** (față de **3543** în 2017), **176 sesizări, 33 de solicitări informații** și **80 de alte petiții**. Din conținutul acestora, se poate constata că această creștere considerabilă a numărului plângerilor primite în cursul anului 2018 este rezultatul unei mai bune cunoașteri a atribuţiilor legale ale Autorităţii Naționale de Supraveghere de către persoanele fizice, prin comparație cu perioada anterioară, precum și al creșterii încrederii petiționarilor în acțiunile Autorității de supraveghere pentru respectarea drepturilor și libertăților lor.

De asemenea, s-a constatat o creștere considerabilă a numărului plângerilor înregistrate după data de 25 mai 2018, în contextul publicității realizate cu privire la punerea în aplicare a Regulamentului General privind Protecția Datelor. Astfel, după data de 25 mai 2018 au fost înregistrate **2922 de plângeri și 120 de sesizări**. Din numărul total al acestora, în peste 700 de cazuri, petenții au adresat solicitările lor prin utilizarea formularului electronic de plângere, pus la dispoziție pe site-ul instituției după această dată.

Subliniem astfel că, în perioada 2006-2018, a avut loc o evoluție exponențială a numărului plângerilor care au fost adresate Autorității Naționale de Supraveghere, creșterea înregistrată fiind **de peste 6 ori față de anul 2013**, respectiv, **de peste 90 de ori față de primul an de activitate**.

Numărul plângerilor în perioada 2006-2018



Pentru soluţionarea plângerilor şi sesizărilor primite, în anul 2018 au fost efectuate **625 de investigații, din care 604 de investigații în scris.** De asemenea, în **82 cazuri** investigațiile au fost finalizate prin încheierea unor procese-verbale de constatare/sancționare la sediul instituției.

Astfel, în anul 2018 au fost **efectuate** investigații pentru soluționarea unui număr de peste **1800 de plângeri considerate admisibile**. De asemenea, pe

parcursul anului 2018 au fost **finalizate** investigațiile pentru soluționarea plângerilor admisibile din peste **1100 de cazuri**, inclusiv pentru cele primite anterior acestui an. În cazul plângerilor considerate admisibile potrivit Regulamentului General privind Protecția Datelor și Legii nr. 102/2005, Autoritatea Națională de Supraveghere a întreprins în mod constant demersuri de informare a petenților cu privire la evoluția sau rezultatul investigațiilor, pe tot parcursul celor șapte luni care au urmat datei de 25 mai 2018.

În urma investigaţiilor efectuate pentru soluționarea plângerilor și sesizărilor, au fost aplicate sancţiuni contravenţionale, reprezentate de **38 de amenzi**, **cuantumul** total al amenzilor aplicate anterior datei de 25 mai 2018 fiind de **223.000** lei. În cursul anului 2018 au fost aplicate în total 120 de avertismente, dintre care un avertisment a fost stabilit după aplicarea Regulamentului General privind Protecția Datelor.

De asemenea, au fost aplicate **7 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c) și d) din Regulamentul General privind Protecția Datelor.

Plângerile şi sesizările primite au vizat o gamă largă de aspecte, însă în anul 2018, cele mai multe dintre plângeri au vizat prelucrarea datelor personale în următoarele domenii: sectorul financiar-bancar, monitorizarea spaţiilor publice sau private prin mijloace de supraveghere video, sectorul comunicaţiilor electronice, dezvăluirea datelor către diverse entități, diseminarea datelor pe Internet, utilizarea fișierelor de tip cookies.

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 (de exemplu: drepturile de informare, acces, intervenție, opoziție, dreptul de a fi uitat), încălcarea principiilor de prelucrare a datelor cu caracter personal, precum și încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date.

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.

Având în vedere dispozițiile Regulamentului General privind Protecția Datelor care impun cooperarea cu alte autorități de supraveghere din statele membre ale Uniunii Europene, în cazul prelucrărilor transfrontaliere, în 18 cazuri Autoritatea Națională de Supraveghere a recurs la mecanismele prevăzute de art. 56 și 61 din Regulament, în vederea obținerii de informații necesare pentru desfășurarea propriilor investigații, în scopul identificării unei autorități de supraveghere principale, determinate de sediul principal/unic al operatorilor care realizează prelucrări cu o componentă transfrontalieră, în sensul art. 4 pct. 23 din Regulamentul General privind Protecția Datelor sau pentru a obține acordul autorității principale pentru tratarea unui caz local, în sensul art. 56 alin. (2) din Regulament. În situațiile în care autoritățile similare au acceptat să soluționeze cazurile în calitate de autoritate principală, au fost transmise documentele traduse în limba engleză către acestea și petenții respectivi au fost informați în mod corespunzător. Totodată, Autoritatea Națională de Supraveghere din România a transmis informații și documente solicitate de alte autorități din Uniunea Europeană, în legătură cu soluționarea plângerilor depuse în statele respective.

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

1. Prelucrarea datelor personale de către operatori din sectorul financiar-bancar

În anul 2018, numărul plângerilor care au avut ca obiect transmiterea datelor personale către biroul de credit a continuat să ocupe o poziție importantă în numărul total al celor primite de Autoritatea Națională de Supraveghere.

Astfel, în sectorul financiar-bancar, operatorii reclamați sunt, în principal, bănci, instituţii financiare nebancare, societăți de recuperări creanțe și societăți care dețin sisteme de evidență de tipul birourilor de credit. Principalul motiv de nemulţumire a persoanelor vizate, care a determinat sesizarea Autorității Naționale de Supraveghere, a fost legat de raportarea datelor personale către sisteme de evidenţă de tip birou de credit, fără respectarea prevederilor Legii nr. 677/2001 şi ale Deciziei Președintelui ANSPDCP nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate

în sisteme de evidenţă de tipul birourilor de credit, în vigoare din luna februarie 2008 (acte normative abrogate de la data de 25 mai 2018).

De asemenea, petenții au fost nemulțumiți de faptul că operatorii din sectorul financiar-bancar le-au încălcat dreptul de acces, în sensul că nu au răspuns solicitărilor lor, nu au transmis răspunsul la adresa de corespondență solicitată sau nu le-au fost furnizate toate informațiile solicitate.

O parte dintre petenți au reclamat faptul că datele lor cu caracter personal au fost prelucrate fără consimțământ, fiind deschise conturi bancare în numele lor sau fiind interogate datele de la biroul de credit fără acordul lor expres.

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 investigaţiile desfăşurate, s-a constatat nerespectarea condițiilor legate de prelucrarea datelor personale în cadrul biroului de credit, cu referire la: tipul de informaţii raportate de către bănci și instituțiile financiare nebancare, modalitatea şi termenul de realizare a informării prealabile impuse de Legea nr. 677/2001 şi de Decizia nr. 105/2007, termenul și frecvența raportărilor în cursul unei luni.

În ceea ce privește activitatea de soluționare a plângerilor, anul 2018 s-a remarcat printr-un efort ridicat de analizare și soluționare a unui număr semnificativ de cazuri în care petenții au reclamat transmiterea datelor personale în baza de date a biroului de credit.

Dificultatea acestor cazuri a fost determinată de complexitatea și numărul foarte mare de prelucrări de date ce au necesitat verificări din partea Autorității Naționale de Supraveghere, prelucrări derulate pe o perioadă de până la 4 ani, dosarele verificate cuprinzând în anumite situații sute de file.

Majoritatea cazurilor analizate au fost soluționate favorabil, datele negative ale petenților fiind șterse din baza de date a Biroului de Credit de către participanții care le-au transmis, acest rezultat datorându-se eforturilor reprezentanților Autorității Naționale de Supraveghere de a face înțelese și respectate, de către operatorii din sectorul financiar-bancar, prevederile legislației în domeniul protecției datelor cu caracter personal.

În cazurile în care, în urma investigațiilor efectuate, s-a constatat că băncile/instituțiile financiare nebancare nu au dat curs în mod voluntar cererilor formulate de petenți sau recomandărilor adresate cu ocazia acestor investigații, Autoritatea Națională de Supraveghere a dispus 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.

FIȘĂ DE CAZ

O bancă a refuzat să dea curs cererilor de exercitare a dreptului de intervenție depuse de mai mulți petenți privind ștergerea datelor lor negative transmise la Biroul de Credit fără respectarea dispozițiilor legale în vigoare, respectiv fără informarea lor prealabilă cu privire la suma restantă și raportarea datelor în acest sistem.

Ca atare, s-a dispus sancționarea contravențională a respectivei bănci, pentru „prelucrarea nelegală a datelor cu caracter personal", în baza art. 32 din Legea nr. 677/2001, pentru încălcarea prevederilor art. 14 din Legea nr. 677/2001 raportate la art. 12 și art. 4 alin. (1) lit. a) din aceeaşi lege, coroborate cu art. 8, art. 9 și art. 12 din Decizia nr. 105/2007.

FIȘĂ DE CAZ

Prin petiţiile sale, o petentă a reclamat, printre altele, că datele sale cu caracter personal au fost prelucrate de către o bancă și raportate în mod eronat la Biroul de Credit fără înştiinţare prealabilă și fără o informare corespunzătoare.

Petenta a susținut că s-a adresat băncii și și-a exercitat dreptul de intervenție, dar operatorul i-a răspuns formal, arătând că răspunsul se află la sediul unei sucursale.

În cadrul investigației efectuate, s-a constatat că banca i-a transmis petentei un e-mail prin care era informată că, deoarece se solicită informații de natura secretului bancar, răspunsul se află în original la sediul unei agenții din Timișoara, iar în cazul în care dorește să i se comunice răspunsul la o altă adresă, este necesar să contacteze

banca (cu precizarea că informațiile confidențiale pot fi transmise titularului, după o identificare prealabilă).

Față de cele de mai sus, s-a constatat că operatorul nu a prezentat dovezi că a comunicat un răspuns la cererea petentei la adresa solicitată, astfel încât nu a respectat opțiunea acesteia prevăzută de art. 14 alin. (3) din Legea nr. 677/2001.

În baza acestor constatări, banca a fost sancţionată contravenţional conform art. 32 din Legea nr. 677/2001, pentru încălcarea art. 14 alin. (3) din această lege.

FIȘĂ DE CAZ

Prin petiția transmisă, petentul a reclamat faptul că o bancă a refuzat să răspundă la cererea sa prin care și-a exercitat dreptul de acces, conform art. 15 din Regulamentul General privind Protecția Datelor, cu privire la precizarea entităților cărora le-au fost dezvăluite datele sale cu caracter personal, invocând faptul că nu poate preciza destinatarii datelor din motive de confidențialitate.

În cadrul investigației efectuate, banca ne-a comunicat adresele transmise petentului, în care acestuia i se precizau categoriile de destinatari ai datelor sale cu caracter personal.

Autoritatea de supraveghere a revenit și a informat banca că, potrivit Ghidului privind transparența în temeiul RGPD, emis de actualul Comitet European pentru Protecția Datelor (WP 260/2017) și față de solicitarea petentului, este justificată cererea acestuia de a i se preciza destinatarii cărora le-au fost dezvăluite datele sale cu caracter personal, și nu indicarea generică a unor categorii de destinatari către care banca „poate dezvălui" date cu caracter personal, pentru a nu-i fi îngrădită astfel posibilitatea exercitării drepturilor sale în relația cu aceste entități.

Ca urmare, banca a achiesat la acest punct de vedere și a răspuns solicitării petentului cu privire la indicarea destinatarilor către care au fost transmise datele personale ale acestuia, sens în care a fost informat și petiționarul.

2. *Prelucrarea datelor personale prin mijloace de supraveghere video*

În anul 2018, plângerile 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 Autorităţii Naționale de Supraveghere pentru apărarea acestora.

Plângerile adresate instituției noastre având ca obiect instalarea sistemelor de supraveghere video au fost îndreptate împotriva asociaţiilor de proprietari sau diverselor categorii de angajatori care au instalat un sistem de supraveghere video la locul de muncă.

FIŞĂ DE CAZ

Printr-o petiţie s-a sesizat o posibilă încălcare a dispoziţiilor Legii nr. 677/2001 de către o asociație de proprietari, în sensul că aceasta a instalat un sistem de supraveghere video la scara pe care o administrează, pe holuri și în lift, fără respectarea prevederilor legale.

Ca urmare a efectuării investigației, a reieșit că decizia de a instala un sistem de supraveghere video în cadrul asociației a fost votată în adunarea generală a proprietarilor, în scopul supravegherii spațiilor comune, pentru protecția proprietarilor și a bunurilor din condominiu. Cu privire la accesarea imaginilor înregistrate, s-a precizat că această operațiune se poate face doar de către persoanele anume desemnate, în cazuri justificate și în mod securizat; imaginile au fost dezvăluite doar organelor de poliție, în cadrul unor anchete.

Întrucât s-a constatat că asociația de proprietari nu a realizat informarea persoanelor vizate în conformitate cu prevederile art. 12 din Legea nr. 677/2001, deşi avea această obligaţie încă de la data instalării camerelor de supraveghere, aceasta a fost sancționată pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001.

FIȘĂ DE CAZ

Prin petițiile înregistrate, Autoritatea Națională de Supraveghere a fost sesizată că o Direcţie Generală de Asistenţă Socială şi Protecţia Copilului prelucrează imaginea prin intermediul sistemului de supraveghere video instalat fără respectarea tuturor dispozițiilor legale.

În urma investigației efectuate, s-a constatat că Direcția prelucra imaginea angajaților și a minorilor instituționalizați, fără respectarea dispozițiilor legale în vigoare la acea dată și, ca urmare, operatorul a fost sancționat pentru contravențiile prevăzute de art. 31, art. 32 raportat la art. 12, respectiv art. 32 raportat la art. 4 din Legea nr. 677/2001.

De asemenea, s-a dispus operatorului, printre altele, suspendarea prelucrării datelor angajaților (imaginii) captate/colectate prin intermediul camerelor de supraveghere instalate în bucătărie și spălătorie, informarea persoanelor vizate potrivit art. 12 din Legea nr. 677/2001, luarea măsurilor necesare în vederea respectării prevederilor Legii nr. 272/2004 privind protecția și promovarea drepturilor copilului în situația în care se prelucrează și date cu caracter personal ale minorilor (imaginea).

FISA DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că i-a fost încălcat dreptul la viaţa privată cu privire la prelucrarea datelor cu caracter personal de către o societate comercială, respectiv un hipermarket, la care petentul era angajat, prin intermediul unui sistem de supraveghere video instalat în incinta în care acesta își desfășura activitatea.

Totodată, petentul și-a exprimat nemulțumirea față de răspunsul primit de la operator la cererea prin care și-a exercitatat dreptul de acces la date.

Din răspunsurile transmise Autorității naționale de supraveghere a rezultat faptul că angajații operatorului (inclusiv petentul) nu au fost informați clar cu privire la scopurile utilizării sitemului de supraveghere, precum și drepturile de care beneficiază.

În temeiul art. 58 alin. (2) lit. b) și d) din RGPD, raportat la art. 14 alin. (11), art. 15 alin. (1) și (3) și art. 16 alin. (5) din Legea nr. 102/2005, precum și la art. 12 din Legea nr. 190/2018 coroborat cu art. 7 din OG nr. 2/2001, s-au dispus următoarele măsuri:

Avertisment **-** pentru nesocotirea dreptului de informare, drept prevăzut de art. 13 din RGPD, întrucât operatorul nu a prezentat dovezi că a realizat informarea persoanelor vizate, angajați ai acestei societăți comerciale, conform prevederilor legale, cu privire la prelucrarea datelor lor prin sistemul de supraveghere video;

Măsuri corective constând în informarea adecvată a persoanelor fizice (inclusiv angajații societății) ale căror date personale le prelucrează prin sistemul de supraveghere video instalat în magazinele proprii în conformitate cu prevederile art. 13 din RGPD;

Recomandări:

- să stabilească o perioadă de stocare a datelor cu caracter personal, raportat la scopul în care sunt prelucrate și în concordanță cu dispozițiile legale în vigoare;

- să furnizeze persoanelor vizate informaţii privind acţiunile întreprinse în urma unor cereri în temeiul articolelor 15-22, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care persoana vizată solicită un alt format.

3. Dezvăluirea datelor personale către diverse entități/terțe persoane

În anul 2018, o pondere însemnată în numărul plângerilor și sesizărilor adresate Autorităţii Naționale de Supraveghere a fost reprezentată de petițiile prin care s-au semnalat situații diverse de încălcare a dispozițiilor legale privind condiţiile în care date personale au fost dezvăluite publicului larg (prin publicarea pe Internet, de exemplu), către terțe persoane neautorizate sau către diverse entităţi de drept public şi privat, fără să fi fost obţinut în prealabil acordul persoanelor vizate, fără să existe un alt temei legal sau fără informarea acestora.

De asemenea, Autoritatea Națională de Supraveghere a continuat să primească în anul 2018 plângeri care au vizat nerespectarea de către Google a „dreptului de a fi uitat”, urmare a refuzului acestei companii de a da curs cererilor prin care se solicita dezindexarea de pe Internet a rezultatelor căutărilor asociate numelui unei persoane.

Din investigațiile efectuate în anul 2018 s-a constatat faptul că, în anumite cazuri, dezvăluirea ilegală a datelor personale s-a produs ca urmare a neadoptării de

către operatori a măsurilor de securitate și confidențialitate necesare pentru a preveni accesul unor persoane neautorizate la date, datorate în special necunoașterii regulilor de protecție a datelor personale aplicabile în activitatea pe care o desfășoară.

FIȘĂ DE CAZ

Un petent a sesizat Autoritatea Națională de Supraveghere cu privire la faptul că angajatorul i-a prelucrat ilegal datele cu caracter personal, conținute într-un raport medical de medicina muncii, prin dezvăluirea acestui document către fosta soție, fără consimțământul său. Petentul a reclamat faptul că angajatorul a depus ulterior în instanță acest document, în cadrul unui proces care avea ca obiect obținerea unui program de vizitare a unui minor și exercitarea în comun a autorității părintești.

În cadrul investigației efectuate, s-a constatat că angajatorul a dezvăluit anumite date medicale ale petentului, fără a avea consimțământul său.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a sancționat contravențional operatorul pentru fapta prevăzută de art. 32 din Legea nr. 677/2001, pentru încălcarea prevederilor art. 5 din aceeași lege.

FIȘĂ DE CAZ

Prin petiția transmisă, petentul a reclamat faptul că o asociație ar fi prelucrat ilegal date cu caracter personal prin dezvăluirea acestora pe site-ul său.

În fapt, petentul a susţinut că asociația a postat pe forum o plângere penală formulată împotriva mai multor persoane, plângere ce cuprindea nume şi prenume, adresa de domiciliu și CNP – ul persoanelor vizate, fără ca aceste date să fie anonimizate.

Din verificările efectuate, s-a constatat că documentul ce conținea datele cu caracter personal fusese vizualizat de 115 persoane.

Ca urmare a investigației efectuate la asociație, a fost identificată pe site-ul acesteia plângerea penală formulată de un membru al asociației împotriva a 21 de persoane, plângere postată la solicitarea acestuia. Reprezentanții operatorului au declarat că datele cu caracter personal ale persoanelor vizate nu au fost anonimizate,

din neatenție. În urma demersurilor efectuate de Autoritatea Națională de Supraveghere, documentul respectiv a fost eliminat de pe site.

Față de constatări, operatorului i-a fost aplicată o sancțiune contravențională în baza art. 32, raportat la art. 5 și 8, din Legea nr. 677/2001, în vigoare la data săvârșirii faptei.

FIȘĂ DE CAZ

Mai mulți petiționari au sesizat Autoritatea Națională de Supraveghere cu privire la faptul că datele lor personale au fost dezvăluite, fără acordul lor, de către o autoritate publică unui dezvoltator imobiliar, prin transmiterea către acest terț a copiilor petițiilor adresate de petenți autorității. Petițiile dezvăluite de autoritatea publică către terț cuprindeau numele, prenumele, adresa de domiciliu și adresa de e-mail, aparținând petenților, precum și aspecte referitoare la o construcție care urma a fi edificată la o adresă apropiată de domiciliul lor.

În cadrul investigației efectuate, operatorul a susținut că a dezvăluit datele petenților în baza unui temei legal, respectiv Ordinul care aproba metodologia de informare şi consultare a publicului cu privire la elaborarea sau revizuirea planurilor de amenajare a teritoriului şi de urbanism. Din analizarea actului normativ menționat a reieșit că operatorul nu a respectat prevederile acestuia, deoarece autorităţile competente cu aprobarea planului de amenajare a teritoriului şi de urbanism au obligația de a notifica iniţiatorul PUD numai cu privire la eventualele obiecţii primite şi de a solicita acestuia modificarea propunerilor sau răspunsul motivat de refuz, cu acordarea unui termen de transmitere a acestui răspuns.

Astfel, întrucât în prevederile legale susmenționate nu se precizează că autoritatea competentă cu aprobarea planului urbanistic de detaliu dezvăluie iniţiatorului PUD datele cu caracter personal ale persoanelor vizate care au făcut obiecții la acel plan, operatorul a fost sancționat contravențional pentru încălcarea art. 5 alin. (1) și (2) din Legea nr. 677/2001, pentru dezvăluirea ilegală a datelor personale ale petenților către un terț.

FISA DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la o posibilă încălcare a prevederilor legale privind prelucrarea datelor sale cu caracter personal de către deținătorul unui website care a transmis un mesaj comercial nesolicitat conținând toate adresele de e-mail vizibile ale destinatarilor, inclusiv adresa petentului.

În urma investigației efectuate, s-a constatat o încălcare a prevederilor legale prin modul în care operatorul a diseminat adresele de e-mail ale mai multor persoane, inclusiv adresa de e-mail a petentului.

În plus, a rezultat că operatorul de date reclamat nu a realizat informarea persoanelor vizate cu privire la scopul prelucrării datelor lor personale.

Pentru faptele constatate, în temeiul art. 58 alin. (2) lit. c) și d) din RGPD, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005 și art. 12 din Legea nr. 190/2018, s-a dispus aplicarea mai multor măsuri corective împotriva operatorului reclamat, și anume:

- să ia măsuri pentru informarea adecvată a persoanelor fizice ale căror date personale le prelucrează raportat la scopul prelucrării;

- să nu mai disemineze adresele de e-mail ale persoanelor care au calitatea de persoane vizate ale acestei societăți comerciale, în lipsa unui temei legal;

- transmiterea de mesaje comerciale prin mijloace de comunicare elctronică să se efectueze numai cu consimţământul expres prealabil al utilizatorului.

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

Respectarea drepturilor persoanelor vizate reglementate de Legea nr. 677/2001, respectiv de Regulamentul General privind Protecția Datelor (după data de 25 mai 2018), în special a dreptului la informare, a dreptului de acces la date, a dreptului de intervenţie/rectificare/ștergere a datelor şi a dreptului de opoziţie, deși reprezintă o obligație esențială a operatorilor de date, a constituit obiectul multor plângeri adresate Autorității Naționale de Supraveghere și în anul 2018.

Astfel, ca urmare a investigaţiilor efectuate, s-a constatat că de multe ori operatorii nu cunosc obligaţiile care le incumbă potrivit reglementărilor legale

susmenţionate ori le ignoră cu bună-ştiinţă, respectiv transmit persoanelor vizate răspunsuri incomplete sau/şi fără respectarea termenului de 15 zile (o lună, în baza Regulamentului General privind Protecția Datelor) prevăzut de dispozițiile legale referitoare la protecția datelor cu caracter personal. 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 prevederile legale referitoare la protecția datelor cu caracter personal.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o companie de telefonie mobilă, în sensul că aceasta i-a încălcat dreptul de acces la datele cu caracter personal. Petentul s-a adresat operatorului cu o cerere prin care solicita informații referitoare la prelucrarea datelor sale cu caracter personal, scopul prelucrării, datele prelucrate, destinatarii către care au fost dezvăluite datele, sursa de colectare a datelor și eventuale mecanisme automate, în situația în care acesta le utilizează. De asemenea, petentul a solicitat să i se comunice care sunt drepturile de care beneficiază în baza Legii nr. 677/2001.

Urmare a cererii depuse, i s-a comunicat că are posibilitatea exprimării în mod gratuit a opțiunii în legătură cu primirea unor informații comerciale referitoare la oferte și programe de loialitate inițiate de operator, menționându-i-se totodată că va înceta prelucrarea datelor sale cu caracter personal la încetarea serviciilor, dacă nu se înregistrează debite restante.

Având în vedere că operatorul nu a răspuns solicitărilor efective ale petentului, la finalizarea demersurilor întreprinse, acesta a fost sancționat contravențional pentru că a încălcat dreptul de acces, întrucât nu i-a răspuns petentului în termenul legal de 15 zile și nu i-a comunicat toate informațiile solicitate prin cererea sa.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a prevederilor Legii nr. 677/2001 de către o autoritate publică. Petentul a susținut că operatorul i-a încălcat dreptul prevăzut de art. 13 din Legea nr. 677/2001.

Petentul s-a adresat operatorului printr-o cerere prin care își exercita dreptul de acces la datele sale cu caracter personal și a fost nemulțumit că acesta nu i-a transmis toate informațiile solicitate, și anume, scopul concret al accesării datelor și categoriile de date prelucrate cu ocazia accesării.

În cadrul investigației s-a constatat că datele cu caracter personal ale petentului (CNP, nume și prenume) au fost accesate neautorizat într-o bază de date constituită la nivel național, la o anumită dată, de către un utilizator al operatorului.

De asemenea, s-a constatat că operatorul nu a transmis petentului toate informațiile pe care avea obligația să le transmită, în conformitate cu prevederile art. 13 din Legea nr. 677/2001, la cererea de exercitare a dreptului de acces la date, inclusiv informații cu privire la scopul concret al accesării datelor sale cu caracter personal și categoriile de date prelucrate cu ocazia accesării.

În urma investigaţiei efectuate, operatorul reclamat a fost sancționat pentru săvârşirea contravenţiei prevăzute de art. 33 din Legea nr. 677/2001, întrucât nu a adoptat suficiente măsuri de securitate şi confidenţialitate pentru a proteja datele personale ale petentului (nume, prenume, CNP) împotriva accesului neautorizat, aşa cum era prevăzut de art. 19 şi art. 20 din Legea nr. 677/2001, fapt care a permis accesarea ilegală a datelor acestuia, într-o bază de date constituită la nivel național, de către un utilizator al operatorului.

Totodată, operatorul a fost sancţionat pentru contravenţia prevăzută de art. 32 din Legea nr. 677/2001, întrucât a încălcat dreptul de acces la date, prin faptul că nu a transmis petentului, în termen de 15 zile, toate informațiile pe care avea obligația să le transmită, în conformitate cu prevederile art. 13 din Legea nr. 677/2001, la cererea de exercitare a dreptului de acces la date, inclusiv informații cu privire la scopul concret al accesării datelor sale cu caracter personal și categoriile de date prelucrate cu ocazia accesării.

FIȘĂ DE CAZ

Un petent ne-a sesizat cu privire la refuzul Google de a da curs cererii de ștergere a unor adrese URL care figurau pe Internet ca fiind asociate unui site.

Petentul s-a adresat Google arătând că informațiile publicate sunt false și se încearcă discreditarea sa de către un blogger. Conform informațiilor furnizate de petent

şi verificate de instituţia noastră, s-a constatat că site-ul reclamat este un blog personal pe care sunt postate şi informaţii privind unele călătorii efectuate de petent, fiind folosit un ton denigrator la adresa acestuia, dar și alte informații de natură personală care îl priveau pe petent (fără ca acesta să joace un rol în viața publică).

Faţă de situaţia prezentată, Autoritatea Națională de Supraveghere a solicitat Google LLC să dea curs cererii petentului cu privire la adresa URL susmenţionată, în cel mai scurt termen posibil.

Solicitarea s-a realizat având în vedere atât Decizia Curţii de Justiţie a Uniunii Europene în cauza Costeja, din 13 mai 2014, cât şi Ghidul pentru aplicarea Hotărârii Curţii de Justiţie a Uniunii Europene privind <Google Spania şi INC V. Agencia Española de Proteccion de Datos (AEPD) Mario Costeja Gonzales> C-131/12, adoptat pe 26 noiembrie 2014 de către Grupul de lucru Art. 29 din care face parte și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal din România.

Google LLC nu a transmis un răspuns la adresa Autorității Naționale de Supraveghere, ci a solicitat instanței de judecată pronunțarea unei hotărâri prin care să se dispună anularea adresei ANSPDCP. Curtea de Apel București a hotărât respingerea cererii formulate de reclamanta Google Inc. în contradictoriu cu Autoritatea Națională de Supraveghere, ca inadmisibilă.

Față de cele de mai sus, instituția noastră a solicitat din nou operatorului să ia măsuri pentru soluționarea plângerii petentului.

În cadrul investigației efectuate, Google LLC a refuzat să dea curs solicitării instituției noastre, considerând că nu sunt întrunite condițiile prevăzute de lege pentru eliminarea URL-ului din rezultatele căutării.

De asemenea, s-a constatat că Google LLC (fosta Google Inc.) nu și-a desemnat un reprezentant pe teritoriul României, conform art. 2 alin. (3) din Legea nr. 677/2001, cu toate că notificase la Autoritatea Națională de Supraveghere, încă din anul 2015, faptul că prelucrează date prin intermediul serviciilor de căutare web și că transferă date în SUA.

Față de constatări, operatorului i-au fost aplicate sancțiuni contravenționale în baza art. 31 și art. 32 raportat la art. 14 și art. 15 din Legea nr. 677/2001, în vigoare la data constatării faptei.

5. Transmiterea de comunicări comerciale prin mijloace de comunicație electronică

În cursul anului 2018, 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 poşta electronică. Majoritatea acestora au privit aspecte legate de protecţia vieţii private în sectorul comunicaţiilor electronice prin primirea de mesaje comerciale nesolicitate prin poşta electronică, fără consimţământul expres şi neechivoc al destinatarului în acest sens.

În vederea soluţionării plângerilor considerate admisibile, Autoritatea Națională de Supraveghere a efectuat o serie de investigaţii pentru a verifica existenţa consimţământului persoanei vizate de a primi mesaje comerciale pe adresa sa de poştă electronică sau prin SMS. În unele cazuri investigate, s-a constatat că expeditorii mesajelor comerciale nu au respectat prevederile legale sub aspectul obţinerii consimțământului prealabil şi al respectării opţiunii persoanelor vizate de a nu mai primi mesaje comerciale nesolicitate.

FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a dispoziţiilor legale de către o societate care i-a transmis prin SMS, la numărul personal de telefon, mesaje comerciale prin care își promova activitatea, după exercitarea dreptului de opoziție de către petent și comunicarea unui răspuns că a fost dezabonat.

În urma investigaţiei efectuate, s-a constatat că operatorul colecta datele persoanelor fizice incluse în baza de date a societății fie ca urmare a efectuării unor comenzi on-line de către acestea, fie în urma realizării unor campanii de marketing prin diverse mijloace, respectiv radio și televiziune, urmate de contactarea telefonică a operatorului de către potențialii clienți. Cu aceste ocazii, operatorul solicita persoanelor vizate să își dea acordul pentru prelucrarea datelor, inclusiv pentru a fi informate cu privire la ofertele operatorului și „campaniile de marketing”.

Cu toate acestea, operatorul nu a ținut seama de exprimarea opoziției petiționarului de a nu mai primi mesaje comerciale și i-a transmis, prin SMS, astfel de

mesaje ulterior cererii adresate de acesta și comunicării răspunsului că a luat act de solicitarea sa.

Astfel, întrucât operatorul i-a transmis petentului mesaje prin SMS, prin care își promova activitatea, ulterior opoziției manifestate de acesta și nu a putut prezenta nicio dovadă certă a obținerii în prealabil a consimțământului expres al acestuia în vederea primirii de comunicări comerciale prin poșta electronică, a fost sancționat contravențional pentru nerespectarea prevederilor referitoare la comunicările nesolicitate, contravenţie prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004.

FIȘĂ DE CAZ

Prin petiţia sa, un petent ne-a sesizat faptul că a primit mesaje comerciale nesolicitate, pe adresa sa de e-mail, în conținutul mesajelor fiind promovate produse comercializate de un site. De asemenea, petentul a susținut că s-a adresat operatorului prin intermediul poștei electronice, solicitând eliminarea datelor sale din baza de date a societății, dar nu a primit răspuns.

Ca urmare a investigației efectuate la această societate, s-a constatat faptul că, în ceea ce privește mesajele comerciale primite de petent pe adresa sa de e-mail, societatea nu a putut face dovada obținerii consimțământului său expres și prealabil pentru primirea de comunicări comerciale prin mijloace de comunicație electronică. De asemenea, s-a constatat faptul că operatorul nu a răspuns la cererea petentului.

Față de constatări, operatorului i-au fost aplicate sancțiuni contravenționale în baza art. 13 alin. (1) lit. q) din Legea nr. 506/2004 și a Legii nr. 677/2001 în vigoare la data săvârșirii faptei.

FIȘĂ DE CAZ

O petentă ne-a sesizat faptul că o anumită societate i-a transmis un mesaj comercial de tip SMS prin care era promovată activitatea acesteia, deși și-a exprimat dezacordul în acest sens. Petenta a mai menționat în petiția sa și faptul că s-a adresat societății prin e-mail, solicitând să i se șteargă datele personale, dar societatea a continuat să îi trimită mesaje comerciale la numărul personal de telefon. Urmare a investigației efectuate, s-a constatat că societatea a transmis mesaje promoționale cu oferte, pe numărul de telefon al petentei, fără a prezenta o dovadă certă a obținerii în

prealabil a consimțământului expres al acesteia în vederea primirii de comunicări comerciale prin telefon, încălcând astfel prevederile art. 12 alin. (1) din Legea nr. 506/2004.

În urma investigației efectuate, față de cele constatate, societatea a fost sancționată pentru săvârșirea contravenției de „Nerespectare a prevederilor art. 12 referitoare la comunicările nesolicitate", contravenţie prevăzută de art. 13 alin. (1) lit. q) din Legea nr. 506/2004.

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

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

În anul 2018, o parte din plângerile și sesizările ce au fost adresate Autorității Naţionale de Supraveghere au avut ca obiect fie dezvăluirea datelor personale către terțe persoane, fie accesarea neautorizată a datelor personale (inclusiv de către angajații proprii), ca urmare a faptului că operatorii în cauză (comercianți, 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.

FIȘĂ DE CAZ

Autoritatea Națională de Supraveghere a fost sesizată de către un petent cu privire la faptul că i-au fost dezvăluite datele cu caracter personal ale altei persoane, în cadrul unei operațiuni de deschidere cont bancar.

În cadrul investigației s-a constatat că, din eroare, odată cu furnizarea documentelor aferente deschiderii unui cont curent, reprezentantul operatorului bancar i-a înmânat petentului un exemplar de cerere deschidere cont emisă pe numele altei persoane, dezvăluind, fără temei legal, datele cu caracter personal ale acesteia.

La finalizarea demersurilor întreprinse, Autoritatea Națională de Supraveghere a sancționat operatorul pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001, întrucât a dezvăluit fără consimțământ datele cu caracter personal (nume, prenume, CNP, serie și număr CI, număr cont) ale unei persoane fizice, precum și pentru săvârşirea contravenţiei prevăzute de art. 33 din Legea nr. 677/2001, întrucât nu a luat măsuri tehnice și organizatorice împotriva dezvăluirii datelor personale ale unei persoane vizate către un terț.

FIȘĂ DE CAZ

Un petent a sesizat un incident de securitate la o societate comercială al cărei angajat a fost, în sensul că puteau fi accesate de către orice angajat al acestei societăți datele cu caracter personal colectate și stocate pe serverul acestui operator, aparținând unui număr de peste 5000 de persoane fizice (solicitanți, foști angajați, parteneri etc.).

În cadrul investigației efectuate, s-a constatat faptul că, la data incidentului, unele foldere, care conțineau și date cu caracter personal ale angajaților, erau accesibile tuturor angajaților din societate. Acest fapt s-ar fi datorat unei erori în stocarea informațiilor financiare și personale ale angajaților, iar din dovezile disponibile, nu au existat indicii cu privire la transferarea datelor în afara companiei sau la utilizarea necorespunzătoare a acestora.

Întrucât operatorul nu a luat măsuri suficiente împotriva dezvăluirii și/sau accesului neautorizat la datele personale ale angajaților, fapt care a făcut posibil ca datele cu caracter personal ale acestora, colectate și stocate pe serverul societății, să poată fi accesate fără drept, a fost sancționat contravențional pentru „neîndeplinirea obligaţiilor privind confidenţialitatea şi aplicarea măsurilor de securitate", conform art. 33 din Legea nr. 677/2001, pentru încălcarea art. 20 din Legea nr. 677/2001.

CAPITOLUL AL V-LEA

ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

La nivel internațional, în anul 2018, Autoritatea Naţională de Supraveghere a participat la o serie de grupuri de lucru, conferinţe și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei, în domeniul protecţiei datelor cu caracter personal, implicându-se în activitatea desfăşurată în cadrul acestora.

În calitate de membru al Grupului de Lucru Articolul 29, devenit Comitetul European pentru Protecția Datelor odată cu intrarea în vigoare a Regulamentului (UE) 2016/679, Autoritatea Națională de Supraveghere s-a implicat în pregătirea pentru noul cadru legislativ în domeniul protecției datelor, care a devenit aplicabil pe întreg teritoriul Uniunii Europene începând cu data de 25 mai 2018.

Reprezentanții Autorității Naţionale de Supraveghere au participat în 2018 la o serie de reuniuni şi diverse grupuri de lucru la nivel european, printre care:

- Grupul de Lucru Articolul 29, devenit Comitetul European pentru Protecția Datelor – organism al Uniunii Europene (înființat în temeiul art. 68 din Regulamentul General privind Protecția Datelor), care reuneşte toate autoritățile Uniunii Europene, precum şi Autoritatea Europeană pentru Protecţia Datelor. De asemenea, Autoritatea Naţională de Supraveghere a participat, prin membrii săi, la următoarele subgrupuri de lucru: BTLE, Cooperare, Calcul amenzi, eGuvernare, Enforcement, Financial Matters, IT users, Key provisions, Social Media, Tehnologie, Transferuri Internaţionale,
- Comitetul Europol şi Organismul comun de control în domeniul vamal,
- Grupul de coordonare comună VIS, Grupul de coordonare comună SIS II şi Grupul de coordonare comună Eurodac.

Grupul de Lucru Articolul 29, respectiv Comitetul European pentru Protecția Datelor

În cursul anului 2018, Grupul de Lucru Articolul 29 și, ulterior, Comitetul European pentru Protecția Datelor și-au exprimat, în principal, poziția față de:

- propunerile Comisiei Europene privind stabilirea unui cadru pentru interoperabilitate între sistemele informatice ale Uniunii Europene în domeniul

frontierelor și vizelor, precum și al poliției și al cooperării judiciare, azilului și migrației,

- propunerile Comisiei Europene referitoare la ordinele europene de divulgare și de păstrare a probelor electronice în materie penală,
- proiectul de Decizie al Comisiei Europene privind protecția adecvată a datelor cu caracter personal în Japonia.

În anul 2018, Comitetul European pentru Protecția Datelor a adoptat un număr de 27 de avize pe marginea proiectelor autorităților naționale de protecția datelor privind listele de operațiuni pentru care este necesară realizarea evaluării impactului asupra protecției datelor, în conformitate cu art. 35 alin. (4) din Regulamentul General privind Protecția Datelor și, totodată, a emis o serie de orientări cu privire la aplicarea Regulamentului General privind Protecția Datelor.

Documentele au fost adoptate fie sub formă de avize, fie sub formă de ghiduri/orientări pentru interpretarea și aplicarea Regulamentului General privind Protecția Datelor, astfel:

➢ avizul referitor la propunerile Comisiei Europene privind stabilirea unui cadru pentru interoperabilitate între sistemele informatice ale Uniunii Europene în domeniul frontierelor și vizelor, precum și al poliției și al cooperării judiciare, azilului și migrației

În decembrie 2017, Comisia Europeană a prezentat două proiecte de regulamente privind interoperabilitatea între sistemele de informare europene existente și viitoare în domeniul controlului la frontiere, al migrației, al protecției internaționale, precum și al cooperării polițienești și judiciare. Scopul general este de a conecta toate aceste sisteme prin formarea unei noi arhitecturi de sistem. Interoperabilitatea preconizată a acelor sisteme ar trebui să pună la dispoziția autorităților naționale toate datele disponibile privind resortisanții țărilor terțe în cadrul îndeplinirii atribuțiilor lor. Obiectivele cheie urmăresc să faciliteze verificarea identității, să detecteze folosirea mai multor identități și să combată astfel frauda de identitate. În opinia Grupului de Lucru Articolul 29, propunerile privind interoperabilitatea nu vizează completarea bazelor de date centralizate existente și viitoare ale Uniunii Europene cu funcții suplimentare de încrucișare, ci urmăresc dezvoltarea unei noi arhitecturi a sistemului care să aibă cel puțin trei baze de date suplimentare;

- avizul privind propunerile Comisiei Europene referitoare la ordinele europene de divulgare și de păstrare a probelor electronice în materie penală

În aprilie 2018, Comisia Europeană a prezentat o propunere de regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală și o propunere de directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul obținerii de probe în cadrul procedurilor penale. Prin aceste propuneri legislative, Comisia Europeană dorește să îmbunătățească cooperarea dintre autoritățile statelor membre și furnizorii de servicii, inclusiv cei care își au sediul în afara Uniunii Europene, și să propună soluții pentru problema reprezentată de stabilirea și asigurarea respectării jurisdicției în spațiul cibernetic. Grupul de Lucru Articolul 29 a atras atenția asupra limitării drepturilor la protecția datelor și la viața privată în ceea ce privește datele prelucrate de furnizorii de telecomunicații și de societățile informaționale, în special atunci când acestea sunt prelucrate ulterior de autoritățile de aplicare a legii, a reamintit necesitatea de a asigura coerența oricărui instrument al Uniunii Europene cu Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică și cu Directiva UE privind ordinul european de anchetă (OEA) și a recomandat să se clarifice normele procedurale respective care reglementează accesul la probe electronice la nivel național și la nivelul Uniunii Europene, pentru a se asigura că noul instrument nu ar conferi autorităților de aplicare a legii noi competențe pe care acestea nu le-ar avea la nivel intern;

- avizul privind proiectul de Decizie al Comisiei Europene privind protecția adecvată a datelor cu caracter personal în Japonia

Comitetul European privind Protecția Datelor a acordat o atenție deosebită acestei decizii privind nivelul de protecție adecvat, fiind prima în acest sens de la intrarea în vigoare a Regulamentului General privind Protecția Datelor, care va constitui un precedent pentru viitoarele transpuneri privind nivelul de protecție adecvat, precum și pentru revizuirea deciziilor de acest fel adoptate în temeiul Directivei 95/46/CE;

- avizul privind proiectele de liste de operațiuni pentru care este necesară realizarea evaluării impactului asupra protecției datelor, în conformitate cu art. 35 alin. (4) din Regulamentul General privind Protecția Datelor;

- ghidul privind consimțământul în temeiul Regulamentului (UE) 2016/679

Documentul oferă o analiză aprofundată a noțiunii de consimțământ definită de Regulamentul General privind Protecția Datelor, cu accent pe cerințele pentru obținerea și dovedirea consimțământului valabil, oferind instrucțiuni practice pentru a asigura conformitatea cu noile dispoziții. Avizele cu privire la consimțământ emise anterior de Grupul de Lucru Articolul 29 sunt în continuare relevante, în cazul în care sunt conforme cu noul cadru juridic, întrucât majoritatea elementelor-cheie ale consimțământului rămân aceleași în temeiul Regulamentului General privind Protecția Datelor. Prin urmare, un consimțământ obținut anterior datei de 25 mai 2018 este în continuare valabil, în măsura în care respectă condițiile impuse de Regulamentul General privind Protecția Datelor. În practică, Regulamentul General privind Protecția Datelor ridică standardul în ceea ce privește punerea în aplicare a mecanismelor de obținere a consimțământului și introduce cerințe noi, care impun operatorilor să modifice mecanismele de obținere a consimțământului;

- ghidul privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679

Regulamentul General privind Protecția Datelor introduce obligația de notificare a unei încălcări a securității datelor cu caracter personal către autoritățile naționale de supraveghere competente și, în anumite cazuri, de informare a persoanelor ale căror date cu caracter personal au fost afectate de încălcare. Documentul adoptat explică cerințele obligatorii de notificare și comunicare în caz de încălcare a securității, așa cum este prevăzut în Regulamentul General privind Protecția Datelor, și unele dintre măsurile pe care operatorii și persoanele împuternicite de operatori le pot lua pentru a îndeplini aceste noi obligații. De asemenea, ghidul oferă exemple de diverse tipuri de încălcări, indicând cine ar trebui să fie notificat în diferite ipoteze;

- ghidul privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679

Regulamentul General privind Protecția Datelor vizează în mod expres procesul decizional individual automatizat, inclusiv crearea de profiluri. Disponibilitatea pe scară largă a datelor cu caracter personal pe internet și pe baza dispozitivelor conectate în cadrul internetului obiectelor, precum și capacitatea de a stabili corelații și de a crea legături pot permite determinarea, analizarea și previzionarea unor aspecte ale

personalității, comportamentului, intereselor și obiceiurilor unei persoane. Regulamentul General privind Protecția Datelor introduce noi dispoziții menite să abordeze riscurile pe care crearea de profiluri și procesul decizional individual automatizat le generează, în special, dar nu exclusiv, la adresa vieții private. Documentul își propune să clarifice aceste dispoziții, conținând, în același timp, recomandări de bune practici pe baza experienței dobândite în statele membre ale Uniunii Europene.

- ghidul asupra transparenței în temeiul Regulamentului (UE) 2016/679

Documentul oferă îndrumări practice cu privire la noua obligație de transparență privind prelucrarea datelor cu caracter personal în temeiul Regulamentului General privind Protecția Datelor. Aceste orientări, ca și celelalte ghiduri ale Grupului de Lucru Articolul 29, sunt destinate a fi, în general, aplicabile și relevante pentru operatorii de date, indiferent de specificațiile sectoriale, industriale sau de reglementările specifice fiecărui operator de date;

- ghidul privind derogările prevăzute la articolul 49 din Regulamentul (UE) 2016/679

Documentul oferă îndrumări în ceea ce privește aplicarea art. 49 din Regulamentul General privind Protecția Datelor, în legătură cu derogările aplicabile în contextul transferurilor de date cu caracter personal către țări terțe. Atunci când se aplică art. 49, trebuie avut în vedere faptul că, în conformitate cu art. 44, exportatorul de date care transferă date cu caracter personal către țări terțe sau organizații internaționale trebuie să îndeplinească și condițiile prevăzute de celelalte dispoziții ale Regulamentului General privind Protecția Datelor. Art. 49 alin. (1) prevede că, în absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în anumite condiții. În cazul în care nivelul de protecție nu este adecvat, exportatorul de date ar trebui să ofere garanții adecvate. Prin urmare, exportatorii de date ar trebui, în primul rând, să depună eforturi pentru a identifica posibilitățile de încadrare a transferului utilizând unul dintre mecanismele prevăzute la art. 45 și art. 46 din Regulamentul General privind Protecția Datelor și, numai în absența acestora, să utilizeze derogările prevăzute la art. 49 alin. (1). Prin urmare, derogările prevăzute la art. 49 constituie

excepții de la principiul general conform căruia datele cu caracter personal pot fi transferate către țări terțe numai în cazul în care se oferă un nivel corespunzător de protecție în țara terță sau în cazul în care au fost prezentate garanții adecvate, iar persoanele vizate se bucură de drepturi opozabile și efective pentru a beneficia în continuare de drepturile lor fundamentale și de garanții;

- ghidul privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul General privind Protecția Datelor

În cadrul instituirii mecanismelor de certificare și a sigiliilor și mărcilor din domeniul protecției datelor, art. 43 alin. (1) din Regulamentul General privind Protecția Datelor impune statelor membre să se asigure că organismele de certificare care emit certificarea în temeiul art. 42 alin. (1) sunt acreditate fie de autoritatea de supraveghere competentă, fie de organismul național de acreditare, fie de ambele entități. Dacă acreditarea este efectuată de organismul național de acreditare în conformitate cu ISO/IEC 17065/2012, cerințele suplimentare stabilite de autoritatea de supraveghere competentă trebuie, de asemenea, aplicate. Scopul ghidului este de a oferi îndrumări privind interpretarea și punerea în aplicare a dispozițiilor art. 43 din Regulamentul General privind Protecția Datelor, venind în sprijinul statelor membre, autorităților de supraveghere și organismelor naționale de acreditare cu finalitatea de a institui o bază de referință coerentă și armonizată pentru acreditarea organismelor de certificare care emit certificarea în conformitate cu Regulamentul General privind Protecția Datelor.

La sfârșitul anului 2018, Comitetul European pentru Protecția Datelor a adoptat următoarele ghiduri disponibile spre consultare publică și trimitere de propuneri:

- ghidul privind certificarea și identificarea criteriilor de certificare în conformitate cu art. 42 și 43 din Regulamentul (UE) 2016/679

Obiectivul principal al documentului este de a identifica principalele cerințe și criteriile care pot fi relevante pentru toate tipurile de mecanisme de certificare emise în conformitate cu art. 42 și 43 din Regulamentul General privind Protecția Datelor. În acest scop, ghidul analizează raționamentul certificării ca instrument de responsabilitate, explică conceptele cheie ale dispozițiilor privind certificarea din art. 42

și 43, domeniul de aplicare a ceea ce poate fi certificat în conformitate cu art. 42 și 43 și scopul certificării;

- ghidul privind aplicabilitatea teritorială a Regulamentului General privind Protecția Datelor

Art. 3 din Regulamentul General privind Protecția Datelor reflectă intenția legiuitorului de a asigura o protecție globală a drepturilor persoanelor vizate din Uniunea Europeană și de a stabili, în ceea ce privește cerințele de protecție a datelor, condiții de concurență echitabile pentru companiile active pe piețele Uniunii Europene, în contextul fluxurilor de date la nivel mondial. Acesta definește domeniul de aplicare teritorial al Regulamentului pe baza a două criterii principale: criteriul „sediu", și criteriul „direcționare" . În cazul în care unul dintre aceste două criterii este îndeplinit, dispozițiile relevante ale Regulamentului General privind Protecția Datelor se vor aplica prelucrării datelor cu caracter personal de către operatorul sau persoana împuternicită în cauză. În aceste linii directoare, Comitetul European pentru Protecția Datelor stabilește și clarifică criteriile de determinare a domeniului de aplicare teritorial al Regulamentului General privind Protecția Datelor. O astfel de interpretare comună este, de asemenea, esențială pentru operatori și persoanele împuternicite de operatori, atât în cadrul Uniunii Europene, cât și în afara Uniunii Europene, astfel încât aceștia să poată evalua dacă le sunt aplicabile dispozițiile Regulamentului General privind Protecția Datelor.

În cadrul primei reuniuni plenare, Comitetul European pentru Protecția Datelor a aprobat Orientările referitoare la Regulamentul General privind Protecția Datelor adoptate de predecesorul său, Grupul de Lucru Articolul 29.

Comitetul Consultativ al Convenţiei 108 al Consiliului Europei

În luna mai 2018, Consiliul Europei a adoptat Protocolul modificat care actualizează Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, cunoscută sub numele de „Convenția 108".

Această reglementare a Consiliului Europei, care a reprezentat singurul instrument internațional obligatoriu din punct de vedere juridic privind protecția vieții

private și a datelor cu caracter personal, a fost modernizată, după o îndelungată perioadă de analiză și negocieri.

Modernizarea Convenției 108 abordează provocările la adresa vieții private rezultate din utilizarea noilor tehnologii de informare și comunicare și, în același timp, consolidează mecanismul de aplicare pentru a asigura implementarea eficientă a acesteia.

În ceea ce privește aderarea la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, a fost primită solicitarea de aderare din partea statului Kazahstan.

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

Un număr mare de autorități naționale competente sunt desemnate pentru a avea acces la Sistemul de Informații privind Vizele (VIS), având posibilitatea de a utiliza sistemul în scopuri specifice. Astfel, există întotdeauna riscuri de abuzuri ale sistemului care pot avea consecințe importante asupra persoanelor vizate ale căror date sunt introduse în VIS. Pentru a evita astfel de abuzuri, personalul autorităților naționale competente trebuie să beneficieze de o formare specifică referitoare la protecția datelor. În acest sens, Grupul de coordonare comună VIS a decis să analizeze instruirea în domeniul protecției datelor a personalului acestor autorități, prin adoptarea unui chestionar și transmiterea acestuia, spre completare, autorităților naționale competente să aibă acces la datele introduse în VIS.

În ceea ce privește sistemul Eurodac, pentru a continua verificarea modului în care sunt soluționate, în practică, cererile de exercitare a drepturilor persoanelor vizate, Grupul de Coordonare Comună Eurodac a redactat un chestionar. Acest chestionar a urmărit două obiective: să aibă o imagine de ansamblu asupra procedurilor existente pentru exercitarea drepturile persoanelor vizate și să identifice cele mai bune practici și posibile îmbunătățiri. În acest scop, chestionarul a fost împărțit în șapte secțiuni referitoare la dreptul la informare, dreptul de acces, cererile de exercitare a drepturilor persoanelor vizate, procedurile de acordare a dreptului la rectificare, procedurile de acordare a dreptului la ștergere, cooperarea autorităților

competente în vederea asigurării drepturilor de protecție a datelor și mecanismele de recurs.

În anul 2018, Comitetul de Cooperare Europol a adoptat Planul de Activitate al Comitetului de Cooperare Europol pentru perioada 2018-2020 care vizează, printre altele, următoarele activități: promovarea și facilitarea exercitării drepturilor persoanelor vizate, supravegherea activităților la nivel național și european, revizuirea, până în anul 2021, a acordurilor de cooperare cu state terțe de către Comisia Europeană, actualizarea Manualului pentru Unitățile Naționale Europol și monitorizarea revizuirii Regulamentului (CE) nr. 45/2001.

A 40ª Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private

În anul 2018, cea de-a 40ª Conferință Internaţională a Comisarilor din domeniul Protecţiei Datelor şi a Vieţii Private a fost organizată de Autoritatea Europeană pentru Protecția Datelor, în colaborare cu Autoritatea pentru Protecţia Datelor din Bulgaria. În cadrul conferinței au fost adoptate următoarele rezoluții și declarații:

- rezoluția privind colaborarea dintre autoritățile pentru protecția datelor personale și autoritățile pentru protecția consumatorilor în scopul asigurării unei protecții adecvate a persoanelor într-o economie digitală
- rezoluția privind platformele de tip e-learning
- rezoluția privind viitorul Conferinței Internaționale
- declarația privind etica și protecția datelor în ceea ce privește inteligența artificială.

Conferinţa de primăvară a autorităţilor europene pentru protecţia datelor

În anul 2018, Conferința de primăvară a autorităților europene pentru protecția datelor cu caracter personal a fost organizată de Autoritatea pentru Protecția Datelor din Albania. Subiectele dezbătute au vizat următoarele aspecte:

- îmbunătățirea cooperării în domeniul supravegherii: rolul autorităților pentru protecția datelor;
- aplicabilitatea teritorială a Regulamentului General privind Protecția Datelor;

- revizuirea Convenției 108;
- protecția datelor cu caracter personal în cadrul activităților polițienești și judiciare în materie penală;
- influența standardelor europene asupra altor sisteme – dezvoltarea convergenței la nivel internațional în jurul unui set comun de standarde de protecție a datelor care sunt împărtășite de sistemul european;
- provocările protecției datelor în cadrul activităților umanitare.

Misiuni de evaluare Schengen

Un capitol important în activitatea Autorității Naționale de Supraveghere în plan internațional îl reprezintă participarea la misiunile de evaluare Schengen în domeniul protecţiei datelor.

Misiunile Schengen se referă la evaluarea și monitorizarea aplicării *acquis-ului* Schengen, respectiv analizarea modului de implementare a regulilor de protecție a datelor cu caracter personal, asigurându-se astfel că statele membre aplică reglementările Schengen în mod eficient și în conformitate cu principiile și normele fundamentale. La finalul fiecarei misiuni de evaluare se întocmește un raport pe baza răspunsurilor transmise de statul evaluat la chestionarul standard[1] și a informațiilor furnizate de autoritățile statului respectiv pe durata vizitei de evaluare. Acest raport conține, printre altele, constatări și evaluări privind cadrul normativ aplicabil, autoritatea pentru protecția datelor, drepturile persoanelor vizate, cooperarea internațională.

În anul 2018, misiunile de evaluare Schengen în domeniul protecției datelor au vizat statele Elveția, Finlanda și Estonia.

Contribuții pe marginea documentelor transmise de alte autorități/instituții, din perspectiva protecției datelor cu caracter personal

În cursul anului 2018, Autoritatea Națională de Supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții, printre care menționăm:

[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

- propunerile de Regulament ale Parlamentului European și ale Consiliului privind crearea unui cadru pentru interoperabilitatea dintre sistemele Uniunii Europene de informații – Autoritatea Națională de Supraveghere a atras atenția asupra riscului extinderii utilizării unui anumit sistem dincolo de scopul pentru care a fost inițial destinat, menționând faptul că o astfel de inițiativă care ar putea permite o utilizare ulterioară a datelor cu caracter personal ar avea un impact deosebit asupra persoanelor fizice. Totodată, autoritatea a apreciat că, prin crearea unui „depozit" („common identity repository") ar putea apărea efectul de dublare a datelor cu caracter personal și, ca atare, a subliniat necesitatea respectării principiilor de protecție a datelor cu caracter personal, în special cel al minimizării datelor, care presupune ca datele cu caracter personal să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. Referitor la accesul autorităților de aplicare a legii la date colectate în scopuri administrative, Autoritatea Națională de Supraveghere a precizat faptul că un astfel de acces, spre exemplu la Sistemul de Informații privind Vizele (VIS) ori Sistemul Eurodac, se poate realiza numai cu respectarea anumitor garanții în vederea limitării impactului nejustificat asupra persoanelor fizice ale căror date cu caracter personal sunt prelucrate. Așadar, un astfel de acces trebuie justificat și, totodată, necesită o analiză aprofundată pentru a se evalua dacă sunt respectate principiile necesității și proporționalității. Autoritatea Națională de Supraveghere a evidențiat, totodată, importanța demonstrării necesității și proporționalității interoperabilității sistemelor și necesitatea respectării cerințelor impuse de Regulamentul (UE) 2016/679, care includ principiile de protecție a datelor *privacy by design* și *privacy by default*, precum și obligația de a implementa măsuri tehnice și organizatorice pentru a asigura securitatea și confidențialitatea datelor cu caracter personal.

- propunerea de Regulament de coordonare a sistemelor de securitate socială – Autoritatea Națională de Supraveghere a subliniat necesitatea includerii de mențiuni referitoare la exercitarea tuturor drepturilor de care beneficiază persoanele vizate în temeiul Regulamentului General privind Protecția Datelor, spre exemplu dreptul la rectificare, dreptul la ștergere etc. Autoritatea Națională de Supraveghere a atras atenția asupra faptului că, potrivit principiului responsabilității din Regulamentul General privind Protecția Datelor, operatorii trebuie să respecte principiile de prelucrare

a datelor cu caracter personal („legalitate, echitate şi transparenţă", „limitări legate de scop", „reducerea la minimum a datelor", „exactitate", „limitări legate de stocare", precum și „integritate şi confidenţialitate") și să demonstreze că, în fapt, respectă aceste principii, sens în care s-a considerat ca fiind necesară stabilirea unei perioade maxime de păstrare a datelor cu caracter personal, prin raportare la scopul în care sunt prelucrate.

- propunerea de Directivă a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2017/1132 în ceea ce privește utilizarea instrumentelor și a proceselor digitale în contextul dreptului societăților comerciale (Directiva Digitalizare) – Cu toate că Regulamentul (UE) 2016/679 nu acoperă prelucrarea datelor referitoare la persoanele juridice, Autoritatea Națională de Supraveghere a menționat aspectele reținute de Curtea de Justiție a Uniunii Europene în legătură cu denumirea unei persoane juridice: „faptul că această informație este furnizată ca parte a unei activități profesionale nu înseamnă că ea nu poate să fie caracterizată ca un set de date cu caracter personal" și „[...] persoanele juridice se pot prevala de protecția articolelor 7 și 8 din Cartă în ceea ce privește o astfel de identificare în măsura în care denumirea persoanei juridice identifică una sau mai multe persoane fizice" (*Cauzele Conexate C-92/09 și C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*). În ceea ce privește accesibilitatea datelor, Autoritatea Națională de Supraveghere a subliniat faptul că accesul la datele cu caracter personal trebuie să fie însoțit de măsuri corespunzătoare și eficiente de prevenire a prelucrării ilegale a datelor cu caracter personal. Referitor la pierderea dreptului de a exercita o funcție de conducere, Autoritatea Națională de Supraveghere a atras atenția asupra faptului că schimbul de informații privind pierderea dreptului de a exercita o funcție de conducere ar putea implica un schimb de date privind condamnări penale și infracțiuni, considerate categorii speciale de date cu caracter personal. Astfel, în conformitate cu art. 10 din Regulamentul (UE) 2016/679, *„prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni se efectuează numai sub controlul autorității de stat sau atunci când prelucrarea este autorizată de legislația Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate*".

➢ proiecte de Convenții/Acorduri de securitate socială între România și state terțe – Față de propunerile de Convenții/Acorduri de securitate socială între România și state terțe, Autoritatea Națională de Supraveghere a precizat că Regulamentul General privind Protecția Datelor stabilește, în cuprinsul art. 49, faptul că, în absenţa unei decizii privind nivelul de protecţie adecvat sau a unor garanţii adecvate, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o ţară terţă sau o organizaţie internaţională poate avea loc numai atunci când transferul este necesar din considerente importante de interes public ori când transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă. Potrivit aceloraşi prevederi, interesul public este recunoscut în dreptul Uniunii sau în dreptul statului membru sub incidenţa căruia intră operatorul. În absenţa unei decizii privind nivelul de protecţie adecvat, dreptul Uniunii sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o ţară terţă sau o organizaţie internaţională. Legat de acest aspect, Autoritatea Națională de Supraveghere a recomandat ca, în contextul negocierii de acorduri/memorandumuri încheiate de Guvernul României și Guverne ale unor state terțe, care vizează și prelucrarea datelor cu caracter personal, să fie avute în vedere dispoziții mai detaliate privind modalitatea de transmitere a datelor, pentru asigurarea protejării drepturilor și intereselor legitime ale persoanelor vizate și a conformității cu Regulamentul General privind Protecția Datelor.

Astfel, pentru garantarea drepturilor persoanelor fizice cu privire la prelucrarea datelor lor personale de către autoritățile competente ale părților contractante, Autoritatea Națională de Supraveghere a recomandat introducerea, în cadrul convenției/acordului, a unui capitol distinct care să conțină prevederi exprese privind respectarea principiilor de protecţie a datelor cu caracter personal instituite prin Regulamentul General privind Protecția Datelor, cu referire inclusiv, dar fără a se limita la:

- categoriile de date – asigurarea că datele personale sunt adecvate, relevante şi limitate la cele strict necesare prin raportare la scopul în care sunt colectate şi ulterior prelucrate; prelucrarea categoriilor speciale de date numai în condițiile expres prevăzute de lege;

- drepturile persoanelor vizate – asigurarea condiţiilor de exercitare a tuturor drepturilor de care beneficiază persoana vizată în conformitate cu dispozițiile Regulamentului General privind Protecția Datelor; menționarea căilor de atac administrative și judiciare în situaţia în care drepturile persoanei vizate sunt încălcate;
- transparenţa – obligaţia autorităților competente ale părților contractante de a furniza persoanei vizate informaţii privind identitatea operatorului, scopul prelucrării și temeiul juridic al acesteia, categoriile de destinatari, drepturile de care beneficiază persoana vizată şi modalitatea de exercitare a acestor drepturi;
- perioada de stocare a datelor – păstrarea datelor personale strict pe durata necesară îndeplinirii obiectivului pentru care au fost colectate; menționarea perioadei de stocare a datelor personale de către autoritățile competente ale părților contractante, dar și a modalității de ştergere sau distrugere a datelor la încheierea acesteia;
- securitatea datelor – instituirea de măsuri tehnice şi organizatorice împotriva prelucrării neautorizate sau ilegale a datelor personale, precum şi împotriva pierderii sau distrugerii accidentale a datelor personale, inclusiv prin mijloace de control al accesului la date; accesarea datelor personale doar de către personalul autorizat etc; includerea obligației de informare reciprocă în cazul unei încălcări a securității datelor cu caracter personal, precum și a autorității de supraveghere, după caz;
- supravegherea – menționarea autorităţii de supraveghere responsabile pentru controlul legalităţii prelucrărilor de date cu caracter personal, în baza acordului.

În ceea ce privește confidențialitatea datelor, Autoritatea Națională de Supraveghere a evidențiat faptul că, potrivit art. 24 din Regulamentul (UE) 2016/679, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul (UE) 2016/679. Respectivele măsuri se revizuiesc și se actualizează periodic.

În concluzie, Autoritatea Națională de Supraveghere a apreciat că aceste Convenții/Acorduri de securitate socială aflate în negociere între România și state terțe necesită includerea de dispoziții referitoare la măsurile tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, astfel încât să răspundă exigențelor Regulamentului (UE) 2016/679.

CAPITOLUL VI

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

În anul 2018, Autoritatea Națională de Supraveghere a soluţionat **7.114** solicitări din partea operatorilor de date cu caracter personal, reprezentate de notificări şi cereri prin care se solicita punctul de vedere sau clarificarea unor aspecte privind prelucrările de date cu caracter personal efectuate.

În concordanță cu prevederile Legii nr. 677/2001, au fost soluţionate **5066** notificări privind prelucrări de date cu caracter personal, dintre care **4757** efectuate pe teritoriul României şi **309** transferuri de date către entităţi din străinătate.

Din cele **309** notificări cu transferuri de date către entităţi din străinătate, în **231** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terţe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield).

Totodată, au fost notificate **78** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, în baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules).

În urma analizării transferurilor de date în străinătate către state terţe, a fost emis un număr de **5** autorizaţii de transfer.

În acelaşi timp, Autoritatea Națională de Supraveghere a soluționat **1185** solicitări ale operatorilor privind diverse aspecte referitoare la: obligația operatorilor de a mai notifica prelucrările de date după aplicarea Regulamentului (UE) 2016/679, modalitatea prin care operatorii pot comunica autorității de supraveghere responsabilul cu protecția datelor, necesitatea efectuării unor cursuri de protecția datelor de către responsabilul cu protecția datelor, obligația operatorilor de a menționa pe documentele prin care colectează date cu caracter personal a numărului de notificare acordat anterior aplicării Regulamentului, programul de audiențe al autorității de supraveghere,

informații despre documente emise de Autoritatea Națională de Supraveghere sau de Comitetul European pentru Protecția Datelor.

De asemenea, au fost analizate și soluționate **856** puncte de vedere privind aspecte referitoare la aplicarea Regulamentului (UE) 2016/679.

Precizăm că un număr de **7225** de operatori au comunicat Autorității Naționale de Supraveghere responsabilii cu protecția datelor desemnați, în temeiul art. 37 alin. (7) din Regulamentul (UE) 2016/679, prin intermediul formularului on-line de declarare a responsabilului cu protecția datelor, pus la dispoziția operatorilor pe site-ul instituției noastre la secțiunea „Responsabilul cu protecția datelor”.

Secțiunea 1- Activitatea de înregistrare a prelucrărilor de date

Deși, prin Decizia președintelui Autorității Naționale de Supraveghere nr. 200/2015 au fost reglementate expres cazurile pentru care este necesară notificarea autorității, operatorii de date cu caracter personal au notificat Autorității Naționale de Supraveghere prelucrările pe care le efectuează potrivit obiectului lor de activitate, inclusiv prelucrările efectuate în scopul îndeplinirii atribuţiilor lor legale.

Autoritatea Națională de Supraveghere a informat aceste entităţi că au calitatea de operator şi, implicit, obligaţia de a respecta legislaţia din domeniul protecţiei datelor, în special cu privire la dispozițiile art. 12, 19 şi 20 din Legea nr. 677/2001, modificată şi completată, fiind însă scutite de obligaţia de a notifica.

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

- prelucrarea datelor care permit localizarea geografică a persoanelor fizice prin mijloace de comunicații electronice (monitorizarea/securitatea persoanelor şi/sau bunurilor publice/private prin utilizarea GPS-ului);
- prelucrarea datelor cu caracter personal prin mijloace electronice, având ca scop monitorizarea şi/sau evaluarea unor aspecte de personalitate, precum competenţa profesională, credibilitatea, comportamentul sau alte asemenea (crearea şi utilizarea de profiluri ale persoanelor vizate în vederea transmiterii unor newsletter-uri, semnalarea încălcării codurilor de conduită în mediul privat - whistleblowing);

- prelucrarea datelor cu caracter personal ale minorilor efectuată prin intermediul internetului sau al mesageriei electronice (publicarea rezultatelor la diferite concursuri şcolare şi extraşcolare, postarea unor imagini din tabere școlare);
- prelucrarea datelor efectuată prin mijloace de supraveghere video în scopul monitorizării/securităţii persoanelor, spaţiilor şi/sau bunurilor publice/private;
- prelucrarea datelor cu caracter personal având ca scop verificarea și montarea tahografelor ori descărcarea de date din tahografele digitale.

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

- verificarea condițiilor de prelucrare a datelor cu caracter personal în scopul „rapoarte de credit și colectare debite/recuperare creanțe”;
- verificarea modului în care se obține consimțământul persoanelor vizate pentru prelucrarea efectuată în scopul întocmirii Registrului Național al Pacienților Infectați cu Hepatita C;
- verificarea modalității de informare a persoanelor vizate.

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

Din cele **309** notificări cu transferuri de date către entităţi din străinătate, în **231** au fost declarate transferuri către state din Uniunea Europeană, din Zona Economică Europeană și către state terţe cu nivel de protecție adecvat al datelor recunoscut de Comisia Europeană (inclusiv în Statele Unite ale Americii, către entităţi care au aderat la principiile Privacy Shield), precum şi transferuri către state terţe efectuate în temeiul art. 30 din Legea nr. 677/2001, modificată şi completată.

Totodată, au fost notificate **78** de transferuri de date în străinătate în temeiul art. 29 alin. (4) din Legea nr. 677/2001, modificată şi completată, în baza contractelor cu clauze standard şi a regulilor corporatiste obligatorii (Binding Corporate Rules).

De asemenea, Autoritatea Națională de Supraveghere a avut calitatea de autoritate co-reviewer în analizarea a două seturi de reguli corporatiste obligatorii (Binding Corporate Rules).

În anul 2018, dintre domeniile care au vizat transferurile de date către state terţe, efectuate în baza prevederilor art. 29 alin. 4 din Legea nr. 677/2001, modificată şi completată, respectiv efectuate în baza clauzelor contractuale standard și a regulilor corporatiste obligatorii, menționăm următoarele:

- resurse umane; administrarea și gestionarea relațiilor de lucru de la recrutare până la rezilierea contractului; monitorizarea și asigurarea respectării obligațiilor ulterioare rezilierii după încetarea raporturilor de muncă; încurajarea planificării și dezvoltării carierei; administrarea și gestionarea programului anual de compensare prin bonusuri al societății și a programului pe termen lung de compensare prin bonusuri; administrarea și prelucrarea statelor de salarii și de plată;
- gestiune economico-financiară și administrativă; bugetul angajaților și analiza profitabilității; reevaluări salariale; modificări în termenii și condițiile de angajare; revizuirea și stabilirea plăților compensatorii; facturarea și condițiile de plată;
- marketing;
- administrarea computerizată pentru adrese de e-mail și alte activități similare în legătură cu persoanele angajate;
- scopuri de afaceri;
- dezvoltarea și îmbunătățirea produselor și serviciilor;
- 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 terţe, în temeiul Legii nr. 677/2001, Autoritatea Națională de Supraveghere a emis un număr de **5 autorizaţii de transfer**.

Secțiunea a 3-a - Solicitări primite de la operatori

În cursul anului 2018, au fost analizate **856** de solicitări primite de la operatori privind, în principal, aspecte referitoare la aplicarea Regulamentului General privind Protecția Datelor.

Principalele informații solicitate de operatorii de date cu caracter personal sau împuterniciții acestora s-au referit la:

- obligațiile operatorilor sau persoanelor împuternicite,
- activitatea responsabilului cu protecția datelor,
- necesitatea efectuării evaluării impactului asupra datelor,
- transferul datelor în state terțe,
- notificarea breșelor de securitate,
- principiile de prelucrare.

Prezentăm mai jos câteva situații supuse spre analiză Autorităţii Naționale de Supraveghere cu privire la aplicarea Regulamentului (UE) 2016/679:

1) Mai mulți operatori au solicitat informații cu privire la necesitatea notificării prelucrărilor de date după aplicarea Regulamentului General privind Protecția Datelor.

Autoritatea Națională de Supraveghere a informat operatorii că, potrivit acestui Regulament, operatorii nu mai au obligația de notificare a prelucrărilor de date.

În acest context, Autoritatea a recomandat operatorilor să aibă în vedere prevederile Capitolului IV din Regulament, care reglementează obligațiile pe care le au operatorii de date cu caracter personal, precum și persoanele împuternicite.

De asemenea, au fost recomandate o serie de ghiduri adoptate și date publicității de Grupul de Lucru Art. 29 (în prezent Comitetul European pentru Protecția Datelor) disponibile la adresa de internet a Autorității Naționale de Supraveghere.

2) O societate care are ca obiect de activitate prestări de servicii informatice a solicitat un punct de vedere cu privire la măsurile de securitate pe care trebuie să le

implementeze pentru clienții săi, în contextul aplicării Regulamentului General privind Protecția Datelor.

În ceea ce privește aspectele referitoare la securitatea prelucrărilor de date, Autoritatea Națională de Supraveghere a precizat că atât operatorul, cât și persoana împuternicită de acesta trebuie să asigure confidenţialitatea și securitatea prelucrării, prin adoptarea de măsuri tehnice și organizatorice adecvate, după caz: pseudonimizarea și criptarea datelor cu caracter personal; capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea și rezistenţa continue ale sistemelor și serviciilor de prelucrare; capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util, în cazul în care are loc un incident de natură fizică sau tehnică; un proces pentru testarea, evaluarea și aprecierea periodice ale eficacităţii măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

De asemenea, a fost informat operatorul și cu privire la consacrarea, în art. 5 din Regulamentul General privind Protecția Datelor, principiului responsabilității, potrivit căruia operatorii de date cu caracter personal nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrare a datelor („legalitate, echitate şi transparenţă”, „limitări legate de scop”, „reducerea la minimum a datelor”, „exactitate”, „limitări legate de stocare”, precum și „integritate şi confidenţialitate”), dar este necesar ca aceștia să poată demonstra respectarea principiilor menționate.

3) O persoană fizică a solicitat punctul de vedere al Autorității Naționale de Supraveghere cu privire la necesitatea obținerii consimțământului tuturor proprietarilor dintr-un condominiu pentru supravegherea video a holului de acces și pentru instalarea unei camere în fața liftului.

Autoritatea Națională de Supraveghere a precizat că prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune atât prevederilor Regulamentului General privind Protecția Datelor, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

Astfel, s-a precizat că, potrivit art. 6 din Regulamentul menționat mai sus, prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una din condițiile prevăzute la alin. (1):

a) când persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale pentru unul sau mai multe scopuri specifice;

b) când prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

d) când prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) când prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

f) când prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Autoritatea a menționat că, în situația în care instalarea unui sistem de supraveghere video este necesară în vederea realizării unui interes legitim al asociaţiei de proprietari (asigurarea pazei şi protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor de utilitate publică, precum și a împrejmuirilor afectate acestora), hotărârea de a instala un astfel de sistem trebuie adoptată în cadrul adunării generale a asociaţiei de proprietari.

De asemenea, Autoritatea Națională de Supraveghere a adus la cunoștință persoanei faptul că, potrivit art. 48 alin. (1) din Legea nr. 196/2018 privind înființarea, organizarea şi funcţionarea asociaţiilor de proprietari şi administrarea condominiilor, „Adunarea generală poate adopta hotărâri, dacă majoritatea proprietarilor membri ai asociației de proprietari sunt prezenți personal sau prin reprezentanți care au o împuternicire scrisă și semnată de către proprietarii în numele cărora votează.

În același timp, s-a atras atenția asupra prevederilor alin. (3) al art. 48 din același act normativ, potrivit cărora hotărârile Adunării Generale a Asociației de Proprietari pot fi adoptate prin votul majorităţii acestora.

4) O persoană fizică a solicitat Autorității Naționale de Supraveghere punctul de vedere cu privire la retragerea consimțământului acordat unei instituții financiar-bancare.

Autoritatea Națională de Supraveghere a adus la cunoștință acesteia prevederile art. 7 din Regulamentul (UE) 2016/679, potrivit cărora:

- în cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal;

- în cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nicio parte a respectivei declaraţii care constituie o încălcare a prezentului regulament nu este obligatorie;

- persoana vizată are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia;

- atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Totodată, Autoritatea Națională de Supraveghere a precizat că, în situația în care consimțământul este retras, operatorul are obligația de a șterge, fără întârzieri nejustificate, toate datele cu caracter personal ale persoanei vizate care și-a exercitat dreptul prevăzut la art. 17 alin. (1) lit. b) din Regulament („dreptul la ștergerea datelor”). De asemenea, s-a subliniat că prevederile de mai sus nu se aplică în măsura în care prelucrarea este necesară:

- pentru exercitarea dreptului la liberă exprimare și la informare;

- pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului;

- din motive de interes public în domeniul sănătății publice, în conformitate cu art. 9 alin. (2) lit. h) și i) și cu art. 9 alin. (3);

- în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice;

- pentru constatarea, exercitarea sau apărarea unui drept în instanță.

În același timp, s-a evidențiat că prelucrările de date efectuate trebuie precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din Regulament, care obligă operatorul să furnizeze persoanei vizate o serie de informații stabilite expres.

CAPITOLUL VII

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfăşurării activităţii, Autorității Naționale de Supraveghere i s-a alocat prin Legea nr. 2/2018 - Legea bugetului de stat pe anul 2018 - un buget în sumă de 6.436.000 lei, diminuat în conformitate cu prevederile ordonanțelor de rectificare a bugetului de stat nr. 78/2018 și nr. 101/2018 și în urma anulărilor de credite realizate în luna decembrie 2018, conform reglementărilor Legii nr. 500/2002 privind finanțele publice, rezultând următoarea sinteză:

Denumire indicator	Cod	Buget iniţial 2018 - mii lei -	Buget actualizat la 31.12.2018 - mii lei -	Execuție bugetară la 31.12.2018 - mii lei -	Execuţie bugetară la 31.12.2018 (%)
Total cheltuieli	51.01	6.436	4.735	4.602	97,19
Titlul I Cheltuieli de personal	10	5.524	3.837	3.835	99,95
Titlul II Bunuri şi servicii	20	812	806	764	94,85
Cheltuieli de capital Titlul X Active nefinanciare	71	100	90	3	2,84

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.

În cursul anului 2018 au existat restricții privind ocuparea, prin concurs sau examen, a posturilor vacante sau temporar vacante din instituţiile şi autorităţile publice, precum și realizarea unor achiziții, aspecte care au avut impact asupra execuției bugetare a anului 2018.

Creditele definitive aprobate au asigurat realizarea obiectivelor propuse, ținând cont de solicitările permanente privind eficiența utilizării fondurilor publice și restricțiile menționate mai sus.

În ceea ce priveşte modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorităţii Naționale de Supraveghere a constituit un procent de 81% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 3.835.233 lei (prin ocuparea unor posturi temporar, prin detaşare), înregistrându-se în continuare un deficit major de personal (15 posturi neocupate, 5 posturi ocupate temporar prin detașare, reprezentând 40% din numărul total de 50 de posturi – exclusiv demnitarii – prevăzute de Legea nr. 102/2005). Majoritatea cheltuielilor de personal au fost aferente plăţilor efectuate pentru munca salariată a angajaţilor din compartimentele de specialitate.

Cheltuielile aferente titlului Bunuri și servicii în anul 2018 au avut o pondere de 17% în bugetul instituției, iar din acestea, cheltuielile cu pondere mai importantă au fost:

- 32% costuri de închiriere și cheltuieli cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI
- 34% bunuri și servicii pentru întreținere și funcționare (curățenie, abonament program legislativ, servicii de actualizare informatică etc.)

În anul 2018, cheltuielile cu bunuri și servicii au crescut cu 16% față de anul 2017.

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

În ceea ce privește Titlul X Active nefinanciare, în anul 2018, Autoritatea Naţională 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 întocmirea situaţiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare.

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

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

Toate documentele care intră sub incidenţa controlului financiar preventiv propriu au fost verificate şi vizate pentru conformitate/încadrare în limitele bugetare.

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