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

# R A P O R T  A N U A L

## 2012

*Raportul de activitate este prezentat Senatului României, în temeiul art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, publicată în Monitorul Oficial al României nr. 391 din 9 mai 2005, cu modificările şi completările ulterioare.*

*Bucureşti*

## CUPRINS

# CAPITOLUL I
# PREZENTARE GENERALĂ

Raportul de activitate al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea de Supraveghere) pe anul 2012 este structurat pe şapte capitole, după cum urmează:

**Capitolul I** asigură o prezentare a structurării raportului pe principalele aspecte.

În cuprinsul **Capitolului II** sunt prezentate iniţiativele luate la nivelul Uniunii Europene în vederea reformării cadrului legal privind protecţia datelor cu caracter personal.

Activitatea în domeniul reglementării, avizării şi consultării este inclusă în **Capitolul III**, *c*are evidenţiază, în principal, implementarea reglementărilor existente în domeniul protecţiei datelor cu caracter personal, avizarea proiectelor actelor normative referitoare la aspecte privind protecţia datelor, precum şi clarificarea problemelor semnalate de diverşi operatori. Aceasta s-a concretizat în emiterea a **două decizii cu caracter normativ**, **51 de avize** şi **832 de opinii**.

Prin petiţiile adresate autorităţii, persoanele fizice şi operatorii de date au solicitat informaţii referitoare la incidenţa legislaţiei privind protecţia datelor asupra activităţii desfăşurate de operatori, necesitatea depunerii notificării, prelucrarea datelor cu caracter special, legalitatea dezvăluirii unor date, transferul acestora în străinătate.

În secţiunea referitoare la reprezentarea în faţa instanţelor de judecată, sunt prezentate dosarele relevante aflate pe rolul instanţelor judecătoreşti în care Autoritatea de Supraveghere a fost parte şi sunt evidenţiate problemele care au determinat naşterea acestor litigii, respectiv contestarea proceselor-verbale de către operatorii cărora li s-au aplicat sancţiuni.

Este de subliniat faptul că, în general, instanţele de judecată au interpretat legislaţia privind protecţia datelor personale într-o manieră similară celei în care Autoritatea de Supraveghere a înţeles să aplice dispoziţiile legale şi să sancţioneze faptele comise de operatori.

**Capitolul IV** constă într-o analiză a activităţii de control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor înregistrate.

Această activitate constă în verificarea modalităţii în care operatorii din România efectuează operaţiuni de prelucrare a datelor cu caracter cu scopul de a cunoaşte cum sunt aplicate dispoziţiile Legii nr. 677/2001. Activitatea de control se realizează prin investigaţii din oficiu şi pe baza plângerilor ori sesizărilor înregistrate. În urma investigaţiilor, au fost aplicate sancţiuni contravenţionale constând în avertismente şi amenzi.

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

În cazurile considerate ca fiind întemeiate, au fost aplicate sancţiuni contravenţionale şi, după caz, s-a dispus, prin decizia preşedintelui Autorităţii de Supraveghere, încetarea prelucrării sau ştergerea datelor.

**Capitolul V** referitor la activitatea de relaţii externe a Autorităţii de Supraveghere, menţionează participarea redusă a reprezentanţilor instituţiei la grupurile de lucru specifice în domeniul protecţiei datelor cu caracter personal.

**Capitolul VI** privind activitatea de supraveghere a prelucrărilor de date cu caracter personal prezintă analizarea formularelor transmise de operatorii de date, persoane fizice şi juridice, care au avut obligaţia depunerii acestora. Au fost înregistrate un număr total de **11592** de notificări privind prelucrări de date realizate atât pe teritoriul României, cât şi în statele membre, ori transferuri în state terţe.

**Capitolul VII** privind resursele materiale şi financiare conţine informaţii referitoare la creditele bugetare puse la dispoziţie şi sumele cheltuite pentru fiecare articol al clasificaţiei bugetare. În anul 2012, restricţiile existente în execuţia bugetară au avut ca efect renunţarea la efectuarea unor achiziţii de bunuri şi a investigaţiilor din oficiu pe teren în teritoriu.

# CAPITOLUL AL II-LEA

## INIŢIATIVE LA NIVELUL UNIUNII EUROPENE ÎN VEDEREA REFORMĂRII CADRULUI LEGAL PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL

În data de 25 ianuarie 2012, Comisia Europeană a abordat comunicarea cu tema *"Protecţia vieţii private într-o lume interconectată. Un cadru european privind protecţia datelor pentru secolul 21"*. Printre obiectivele importante ale acestei iniţiative se numără modernizarea sistemului curent de protecţie a datelor personale, îmbunătăţirea şi simplificarea legislaţiei existente, precum şi consolidarea încrederii cetăţenilor europeni în mediul digital şi, în consecinţă, stimularea dezvoltării economiei digitale pe piaţa unică a Uniunii Europene, dar şi dincolo de graniţele sale.

Pachetul legislativ propus de Comisia Europeană cuprinde următoarele iniţiative**:**

- un proiect de regulament care va înlocui Directiva 95/46/EC privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- un proiect de directivă privind protecţia datelor procesate în scopul prevenirii, detectării, investigării şi punerii sub urmărire a infracţiunilor şi a altor activităţi judiciare.

România susţine, de principiu, adoptarea noului pachet legislativ privind protecţia datelor. În acest context, protecţia efectivă a datelor cu caracter personal în întreaga Uniune necesită consolidarea şi detalierea nu numai a drepturilor persoanelor vizate, ci şi a obligaţiilor celor care prelucrează/procesează date cu caracter personal. În mod firesc, acest fapt conduce la o sporire a sarcinilor administrative care revin operatorilor de date cu caracter personal, sarcini care ar putea îngreuna desfăşurarea activităţilor marilor corporaţii, dar mai ales a întreprinderilor mici şi mijlocii. Tocmai de aceea, Autoritatea de Supraveghere consideră că este esenţial să se identifice cele mai bune soluţii pentru a asigura un echilibru just între protecţia datelor cu caracter personal şi sarcinile administrative ale operatorilor de date cu caracter personal.

În acelaşi timp, pornind de la necesitatea asigurării unei protecţii adecvate a dreptului la viaţă privată al fiecărei persoane, Autoritatea de Supraveghere s-a pronunţat în favoarea consolidării drepturilor persoanelor fizice ale căror date personale sunt utilizate, atât în domeniul public, cât şi în cel privat, inclusiv în ceea ce priveşte stabilirea unor noi drepturi, cum sunt dreptul de a fi uitat şi dreptul la portabilitate, în concordanţă cu evoluţiile tehnologice ale societăţii contemporane.

***<u>Secţiunea I – Proiectul Regulamentului Parlamentului European şi al Consiliului privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date</u>***

Referitor la natura instrumentului juridic**,** Comisia Europeană a optat pentru un regulament, deoarece aplicabilitatea directă a acestui tip de instrument juridic face posibilă reducerea actualei fragmentări legislative a cadrului juridic al Uniunii, oferind, în acelaşi timp, o mai mare securitate juridică cetăţenilor europeni.

Cu toate acestea, unele state membre s-au pronunţat în favoarea reglementarii cadrului general de protecţie a datelor prin Regulament, iar altele în favoarea reglementării prin Directivă. Această din urmă opinie a fost împărtăşită şi de Autoritatea de Supraveghere în cadrul discuţiilor la reuniunile Grupului de Lucru art. 29 de pe lângă Comisia Europeană, considerându-se că o directivă conferă mai multă libertate statelor membre şi permite o reglementare la nivel naţional în acord cu instituţiile de drept român.

Referitor la rolul Comisiei Europene, menţionăm că un aspect problematic pentru statele membre este cel referitor la *numărul mare de acte delegate şi acte de implementare conferite Comisiei Europene* în temeiul articolelor 290 şi 291 din Tratatul privind Funcţionarea Uniunii Europene. Statele membre, inclusiv România, au criticat numărul mare de referiri la actele delegate ale Comisiei în cuprinsul propunerii de Regulament, aspect de natură să aducă în discuţie asigurarea independenţei autorităţilor naţionale, în condiţiile intervenţiei semnificative a executivului european.

Cât priveşte actele delegate şi actele de implementare, urmare a dezbaterilor din cadrul Consiliilor de miniştri, cazurile în care Comisia adoptă astfel de acte au fost reduse, statele membre optând fie pentru eliminarea definitivă a actelor delegate (actul delegat nu este oportun situaţiei reglementate), fie pentru înlocuirea actului delegat cu prevederi concrete în textul regulamentului. Argumentul predominant a fost faptul că prea multe acte delegate conduc la incertitudine în aplicarea instrumentului.

Cu toate acestea**,** Autoritatea de Supraveghere şi-a exprimat îngrijorarea faţă de numărul mare de cazuri rămase, întrucât o parte dintre acestea nu îşi au locul în proiectul de regulament, specificul naţional impunând o reglementare la nivel intern, pentru o implementare eficientă a actului comunitar.

Referitor la creşterea sarcinilor birocratice ale operatorilor, în special impactul instrumentului şi al reglementărilor asupra micro-întreprinderilor şi IMM-urilor, România a semnalat că vor creşte obligaţiile întreprinderilor şi costurile pentru acestea. În sensul celor de mai sus, majoritatea statelor membre au susţinut introducerea abordării bazate pe riscurile implicate de anumite prelucrări de date.

O altă componentă ce conduce la creşterea sarcinilor administrative ce revin operatorilor este reprezentată de prevederile referitoare la instituirea atât a unor proceduri, cât şi a unor politici privind respectarea drepturilor persoanelor vizate din cuprinsul Regulamentului.

Un element de noutate este şi cel referitor la notificarea autorităţilor naţionale de supraveghere de către operatorii la care apare o încălcare a condiţiilor de securitate a prelucrării datelor. În această privinţă, Autoritatea de Supraveghere susţine ca notificarea să fie efectuată doar în cazul încălcărilor importante ale securităţii datelor personale, de natură să afecteze persoanele fizice. Corelat cu acest aspect, s-a instituit în sarcina operatorilor şi obligaţia de informare a persoanelor fizice ale căror date sunt implicate în încălcarea de securitate semnalată autorităţii naţionale de supraveghere. În această privinţă, Autoritatea de Supraveghere opinează că ar trebui să fie lăsat la aprecierea autorităţilor naţionale de supraveghere dacă se impune informarea persoanelor implicate, pentru a evita alarmarea acestora în situaţii minore, eventual deja remediate de operator.

Un alt aspect foarte important este cel referitor la numirea conducerii autorităţii de supraveghere (art. 48 pct. 1 din regulament). România a susţinut ca aceasta să se efectueze numai de către Parlament (nu şi de către Guvern) pentru autorităţile de la nivel naţional, în vederea asigurării unei reale independenţe a autorităţilor naţionale de protecţia datelor.

O altă problematică privind independenţa autorităţii de supraveghere se referă la autoritatea financiară independentă (prevăzută la art. 47 pct. 7 din regulament) competentă să efectueze controlul financiar al Autorităţii, fără însă a afecta independenţa acesteia. Autoritatea de Supraveghere apreciază că sunt necesare clarificări asupra identităţii acesteia, în condiţiile în care, în prezent, în România, controlul financiar asupra bugetului Autorităţii se exercită şi de Ministerul Finanţelor Publice subordonat executivului.

O nouă prevedere propusă se referă la transmiterea proiectelor de decizii ale autorităţilor naţionale de protecţia datelor către Comitetul European pentru Protecţia Datelor (European Data Protection Board) şi Comisia Europeană, în anumite cazuri. Aceasta ridică problema relaţiei de subordonare a autorităţilor naţionale independente de protecţia datelor faţă de organisme europene, respectiv executivul Uniunii Europene. Autoritatea de Supraveghere consideră că acest aspect ar trebui reanalizat, prin raportare la dispoziţiile Constituţiei României, luând în considerare faptul că, în sistemul de drept românesc, actele administrative emise de Autoritatea de Supraveghere pot fi supuse numai controlului judecătoresc.

În ceea ce priveşte termenele instituite în relaţiile de cooperare dintre autorităţile naţionale de protecţie a datelor, subliniem dezechilibrul existent în resursele umane şi

financiare de care dispune fiecare autoritate la nivelul statelor membre, în condiţiile în care se impun termene extrem de scurte de acţiune în cazuri preconizat complexe. Astfel, în textul proiectului de regulament, se prevede termenul de *o lună* în care autoritatea de supraveghere solicitată trebuie să acţioneze, la cererea unei alte autorităţi de protecţia datelor dintr-un stat membru. Considerăm acest termen prea scurt în condiţiile în care Autoritatea de Supraveghere se confruntă cu serioase dificultăţi în ceea ce priveşte resursele umane şi financiare de care dispune, în situaţia actuală în care primeşte noi competenţe prin mai multe acte normative cu putere de lege (Legea nr. 238/2009, Legea nr. 141/2010, Legea nr. 271/2010, proiectul ordonanţei de urgenţă privind modificarea Legii nr. 506/2004, propunerea legislativă privind reţinerea datelor de trafic).

Referitor la consimţământul persoanelor vizate, o particularitate o reprezintă solicitarea consimţământului părinţilor în cazul copiilor sub 13 ani, în contextul în care, în sistemul de drept românesc, capacitatea restrânsă de exerciţiu se dobândeşte la vârsta de 14 ani. Ca atare, Autoritatea de Supraveghere consideră că, în ceea ce priveşte vârsta minorilor, trebuie să fie inserate prevederi care să facă trimitere la legea naţională aplicabilă în materie a statului membru.

Legat de includerea unor noi drepturi în proiectul Regulamentului, cum sunt dreptul de a fi uitat şi dreptul la portabilitatea datelor, în concordanţă cu evoluţiile tehnologice ale societăţii contemporane, Autoritatea de Supraveghere îşi exprimă satisfacţia faţă de aceste reglementări.

În ceea ce priveşte adoptarea instituţiei ofiţerului pentru protecţia datelor, prin proiectul Regulamentului, subliniem că acesta este un element de noutate absolută în peisajul juridic din România şi va implica o schimbare semnificativă în activitatea operatorilor care, până în prezent, notificau prelucrările de date efectuate la Autoritatea de Supraveghere. Sub acest aspect, România a propus scăderea pragului de salariaţi instituit ca o condiţie pentru desemnarea ofiţerului de protecţie a datelor, la nivelul operatorilor.

În legătură cu extinderea categoriilor de date speciale, Autoritatea de Supraveghere a propus, în cadrul consultărilor interministeriale organizate de Ministerul Afacerilor Europene, includerea în sfera acestora şi a „datelor biometrice”, motivat de faptul că prelucrarea lor nu se poate efectua decât în condiţiile asigurării unui caracter adecvat raportat la scopul prelucrării şi al instituirii unor măsuri de securitate şi confidenţialitate sporite, într-o manieră similară abordării de la nivelul Consiliului Europei, în contextul revizuirii Convenţiei 108.

Referitor la cuantumul sancţiunilor, România a considerat că acesta este excesiv şi disproporţionat faţă de prejudiciul care ar putea fi creat prin nerespectarea condiţiilor impuse de regulament. În acest sens, apreciem că s-ar impune o abordare mai puţin rigidă, oferindu-se

autorităţilor de supraveghere o independenţă mai mare, care să le permită luarea în considerare a diverselor circumstanţe ale comiterii actelor ilicite. În aceste condiţii, poate fi luată în calcul reglementarea posibilităţii aplicării unei sancţiuni pecuniare, precum cele avute în vedere în cadrul proiectului de instrument, fără a fi condiţionată de aplicarea unei atenţionări iniţiale rămase fără rezultat.

***Secţiunea a II-a – Proiectul de Directivă privind protecţia datelor procesate în scopul prevenirii, detectării, investigării şi punerii sub urmărire a infracţiunilor şi a altor activităţi judiciare***

În comunicarea Comisiei Europene privind „O abordare globală a protecţiei datelor cu caracter personal în Uniunea Europeană", aceasta a precizat că Uniunea Europeană are nevoie de o politică mai cuprinzătoare şi mai coerentă privind dreptul fundamental la protecţia datelor cu caracter personal.

În acest context, se arăta faptul că Decizia-cadru 2008/977/JAI are un domeniu de aplicare limitat, deoarece se aplică doar în cazul prelucrării datelor la nivel transfrontalier şi nu în cazul activităţilor de prelucrare realizate de către poliţie şi autorităţile judiciare exclusiv la nivel naţional. Acest fapt poate crea dificultăţi pentru poliţie şi alte autorităţi competente în domeniul cooperării judiciare în materie penală şi al cooperării poliţieneşti. Acestea nu reuşesc întotdeauna să facă distincţie cu uşurinţă între prelucrarea exclusiv la nivel naţional şi cea la nivel transfrontalier sau să prevadă dacă anumite date personale pot face obiectul unui schimb transfrontalier într-o etapă ulterioară. În plus, ca urmare a naturii şi conţinutului său, decizia-cadru lasă legislaţiilor naţionale ale statelor membre o amplă marjă de manevră privind punerea în aplicare a dispoziţiile sale. De asemenea, decizia-cadru nu include niciun mecanism sau grup consultativ similar Grupului de Lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal care să sprijine interpretarea comună a dispoziţiilor sale, şi nici nu prevede competenţe de executare pentru Comisie în vederea asigurării unei abordări comune în punerea sa în aplicare.

Asigurarea unui nivel omogen şi ridicat de protecţie a datelor cu caracter personal ale persoanelor fizice şi facilitarea schimbului de date cu caracter personal între autorităţile competente ale statelor membre sunt esenţiale pentru a se garanta eficacitatea cooperării judiciare în materie penală şi a cooperării poliţieneşti. În acest scop, nivelul de protecţie a drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, identificării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor trebuie să fie echivalent în toate

statele membre. Protecţia efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea drepturilor persoanelor vizate şi a obligaţiilor celor care prelucrează date cu caracter personal, ci şi competenţe echivalente pentru monitorizarea şi asigurarea conformităţii cu normele în materie de protecţie a datelor cu caracter personal în statele membre.

În consecinţă, scopul propunerii este de a asigura un nivel ridicat şi coerent de protecţie a datelor în acest domeniu, sporind astfel încrederea reciprocă între autorităţile poliţieneşti şi cele judiciare din diferitele state membre şi facilitând libera circulaţie a datelor şi cooperarea între aceste autorităţi.

În privinţa acestei propuneri, România a formulat rezerve de examinare care s-au referit, printre altele, la extinderea domeniului de aplicare al Directivei cu activitatea de menţinere şi asigurare a ordinii publice, în vederea unei reglementări unitare şi exhaustive a protecţiei datelor în context poliţienesc.

De asemenea, s-a considerat că termenul de 5 ani pentru negocierea acordurilor internaţionale care prevăd transferul de date personale este prea scurt pentru desfăşurarea tuturor formalităţilor necesare pentru un asemenea demers. Mai mult, unele acorduri au fost încheiate cu dificultate, astfel încât renegocierea lor este practic imposibilă, în special dacă aceste acorduri sunt multilaterale.

# CAPITOLUL AL III-LEA
## ACTIVITATEA DE REGLEMENTARE, AVIZARE ŞI CONSULTARE

### ***Secţiunea 1 – Acte cu caracter normativ emise de Autoritatea de Supraveghere***

Pe parcursul anului 2012, în vederea promovării intereselor persoanelor vizate, Autoritatea de Supraveghere a continuat implementarea reglementărilor existente în domeniul protecţiei datelor cu caracter personal şi a contribuit la îmbunătăţirea cadrului de reglementare în acest domeniu de activitate prin emiterea următoarelor acte cu caracter normativ:

- ***Decizia nr. 23 din 26 martie 2012 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal***

Această decizie a fost emisă în aplicarea prevederilor art. 22 alin. (9) din Legea nr. 677/2001, conform cărora Autoritatea de Supraveghere poate stabili cazuri în care notificarea nu este necesară. Emiterea acestei decizii s-a întemeiat pe faptul că anumite prelucrări de date nu sunt susceptibile de a afecta, cel puţin aparent, drepturile persoanelor vizate, în cazul utilizării lor regulate.

Stabilirea scutirilor de la notificare a vizat, în principal, situaţiile în care prelucrarea datelor cu caracter personal este efectuată de persoanele fizice sau de entităţile private care desfăşoară o activitate independentă, autorizată în baza unei legi speciale, în scopul îndeplinirii atribuţiilor lor legale; situaţiile în care prelucrarea datelor cu caracter personal este efectuată de autorităţile administraţiei publice locale, precum şi de autorităţile administraţiei publice de la nivel judeţean şi al municipiului Bucureşti, în scopul îndeplinirii atribuţiilor lor legale.

De asemenea, s-a stabilit că nu este necesară notificarea în cazul în care prelucrarea datelor cu caracter personal este efectuată în scopul împrumuturilor de cărţi, opere cinematografice, artistice, alte opere audiovizuale; când prelucrarea datelor cu caracter personal este efectuată în scopul gestionării bazei de date deţinute de Arhivele Naţionale, când prelucrarea datelor cu caracter personal este efectuată în scopul intermedierii tranzacţiilor imobiliare, precum şi în cazul în care prelucrarea datelor cu caracter personal referitoare la propriii membri este efectuată de partidele politice, cu condiţia ca datele să nu fie dezvăluite unor terţi fără consimţământul persoanei vizate.

- ***Decizia nr. 52 din 31 mai 2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video***

Decizia sus-menţionată a fost emisă luând în considerare documentele elaborate la nivelul Grupului de Lucru Art. 29 şi al altor organisme europene în legătură cu prelucrarea datelor cu caracter personal prin mijloace de supraveghere video, în care se subliniază potenţialele riscuri referitoare la respectarea dreptului la viaţă privată şi a dreptului la protecţia datelor cu caracter personal, precum şi necesitatea respectării principiului proporţionalităţii datelor prelucrate raportat la scopul propus.

De asemenea, la adoptarea acestei reglementări s-a avut în vedere faptul că anumite entităţi publice sau private utilizează sisteme de supraveghere video în mod excesiv, atât pentru a controla accesul angajaţilor la locul de muncă, cât şi pentru a monitoriza corectitudinea şi eficienţa activităţii desfăşurate, ceea ce poate aduce atingere vieţii private a acestora, precum şi pentru a controla deplasarea persoanelor, bunurilor şi accesul în anumite spaţii.

Având în vedere că utilizarea mijloacelor de supraveghere video poate aduce atingere dreptului la viaţă privată al individului, consfinţit de art. 26 din Constituţia României, republicată, prin utilizarea nelegitimă, neadecvată sau excesivă a acestora, Autoritatea de Supraveghere a reglementat, prin intermediul acestei decizii, modalitatea de aplicare a regulilor generale de prelucrare a datelor cu caracter personal prin mijloace de supraveghere video.

***<u>Secţiunea a 2-a – Avizarea actelor normative</u>***

În temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, Autoritatea de Supraveghere a emis avize asupra unui număr de **51** de proiecte de acte normative elaborate de diverse instituţii şi autorităţi publice care includeau aspecte privind prelucrarea datelor cu caracter personal.

Din compararea cifrelor statistice cu cele din anul precedent se constată o uşoară reducere a numărului de proiecte de acte normative transmise spre avizare Autorităţii de Supraveghere. Cu toate acestea, Autoritatea de Supraveghere a formulat un număr mare de observaţii referitoare la actele normative supuse avizării cu privire la protecţia drepturilor şi libertăţilor persoanelor. Acest aspect demonstrează necunoaşterea în totalitate a cerinţelor existente în acest domeniu de activitate.

Faţă de conţinutul proiectelor actelor normative transmise Autorităţii de Supraveghere în cursul anului 2012, au fost emise o serie de avize negative, avize favorabile fără observaţii, precum şi avize favorabile cu observaţii şi propuneri, după cum urmează:

***1. Avize negative***

Argumentele care au justificat ca Autoritatea de Supraveghere să emită avize negative au fost diverse. Printre acestea menţionăm necorelarea dispoziţiilor propuse cu principiile şi reglementările constituţionale, cu actele juridice ale Uniunii Europene, cu tratatele la care România este parte ori cu legislaţia cadru în materie, precum şi generarea unor paralelisme în reglementare.

Toate aceste aspecte au făcut imposibilă emiterea unui aviz favorabil, Autoritatea de Supraveghere propunând reformularea respectivelor proiecte de acte normative.

Dintre reglementările asupra cărora Autoritatea de Supraveghere a emis avize negative, exemplificăm următoarele:

- propunerea legislativă privind colectarea şi stocarea datelor necesare identificării clienţilor serviciilor de comunicaţii electronice furnizate prin intermediul cartelelor preplătite (Bp.680/2011);
- proiectul Legii privind reţinerea datelor generate sau prelucrate, de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii;
- propunerea Direcţiei pentru politici fiscale şi bugetare locale din cadrul Ministerului Administraţiei şi Internelor de completare a art. 11 din Ordonanţa Guvernului nr. 92/2003 privind Codul de procedură fiscală, republicată, cu completările şi modificările ulterioare;
- proiectul Ordonanţei de urgenţă pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- proiectul de lege privind adoptarea Ordonanţei de urgenţă nr. 13 din 24 aprilie 2012 pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;
- proiectul de lege pentru modificarea şi completarea Legii nr. 334/2006 privind finanţarea activităţii partidelor politice şi a campaniilor electorale.

***2. Avize favorabile, fără observaţii***

În anul 2012, Autoritatea de Supraveghere a emis avize favorabile, fără observaţii, pentru proiectele de acte normative care respectau rigorile constituţionale şi reglementările în materie, dintre care enumerăm:

- proiectul de Hotărâre a Guvernului privind stabilirea măsurilor necesare pentru aplicarea Regulamentului (UE) nr. 211/2011 al Parlamentului European şi al

Consiliului din 16 februarie 2011 privind iniţiativa cetăţenească;

- proiectul de Lege pentru modificarea şi completarea Legii 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;
- proiectul Ordonanţei Guvernului privind instituirea cadrului pentru implementarea sistemelor de transport inteligente în domeniul transportului rutier şi pentru interfeţele cu alte moduri de transport;
- proiectul de Lege pentru modificarea şi completarea Legii nr. 290/2004 privind cazierul judiciar;
- proiectul de Hotărâre pentru aprobarea normelor metodologice de aplicare a prevederilor referitoare la cardul naţional de asigurări sociale de sănătate din Legea nr. 95/2006 privind reforma în domeniul sănătăţii.

### *3. Avize favorabile cu observaţii şi propuneri*

În cadrul avizelor favorabile emise în anul 2012, Autoritatea de Supraveghere a formulat numeroase observaţii şi propuneri care au avut ca scop asigurarea unei reglementări complete şi redactarea clară a textelor legale, în scopul înţelegerii şi aplicării corecte a acestora.

În acest context, precizăm faptul că majoritatea observaţiilor şi propunerilor formulate de către Autoritatea de Supraveghere au fost însuşite de către iniţiatori. Dintre proiectele de acte normative asupra cărora Autoritatea a formulat propuneri, exemplificăm:

- proiectul de Regulament privind cooperarea administrativă prin intermediul Sistemului de informare al pieţei interne;
- propunerea legislativă privind comunicaţiile electronice (Plx. 238/2012);
- proiectul de lege pentru modificarea şi completarea Legii nr. 76/2002 privind sistemul asigurărilor pentru şomaj şi stimularea ocupării forţei de muncă şi pentru modificarea Legii nr. 116/2002 privind prevenirea şi combaterea marginalizării sociale;
- proiectul Legii privind organizarea şi funcţionarea sistemului de sănătate din România;
- proiectul Ordinului ministrului administraţiei şi internelor privind evidenţa permiselor de conducere reţinute şi a sancţiunilor aplicate conducătorilor de vehicule sau tramvaie;

- proiectul Ordonanţei de urgenţă a Guvernului pentru modificarea şi completarea unor acte normative privind evidenţa persoanelor, actele de identitate ale cetăţenilor români, precum şi actele de rezidenţă ale cetăţenilor statelor membre ale Uniunii Europene şi Spaţiului Economic European rezidenţi în România;
- proiectul Legii privind exercitarea activităţilor şi practicilor de medicină complementară şi/sau alternativă, precum şi înfiinţarea, organizarea şi funcţionarea Colegiului Practicienilor de Medicină Complementară şi/sau alternativă din România.

Autoritatea de Supraveghere a efectuat, în activitatea sa, propuneri pentru îmbunătăţirea conţinutului proiectelor transmise spre avizare. Observaţiile şi propunerile, atât de ordin general, cât şi punctual, la normele juridice transmise, au fost determinate de acelaşi gen de probleme care s-au manifestat şi în anii trecuţi, dintre care menţionăm:

**a) <u>Neconformitate cu prevederile Constituţiei</u>**

În acest context, exemplificăm ***proiectul Legii privind reţinerea datelor generate sau prelucrate, de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii.***

În primul rând, proiectul sus-menţionat conţinea, în cea mai mare parte, prevederi identice cu cele ale Legii nr. 298/2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, declarată neconstituţională de Curtea Constituţională prin Decizia nr. 1258/2009; în acest sens, propunerea nu clarifica aspectele de neconstituţionalitate constatate de Curtea Constituţională în privinţa încălcării dreptului la viaţă intimă, familială şi privată.

De asemenea, Autoritatea de Supraveghere a făcut obiecţii privind accesul la date al organelor de stat cu atribuţii în domeniul siguranţei naţionale, prin raportare la prevederile art. 4 din Directiva nr. 2006/24/CE, conform cărora statele membre vor adopta măsuri pentru a se asigura că datele stocate vor fi folosite doar de către autorităţile naţionale competente, în cazuri specifice şi potrivit legislaţiei naţionale.

O altă obiecţie rezidă în lipsa unei proceduri clare de solicitare şi comunicare a datelor reţinute de furnizori către autorităţile competente.

În plus, proiectul nu conţinea prevederi referitoare la alocarea resurselor financiare şi umane necesare îndeplinirii noilor competenţe stabilite în sarcina Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Faţă de aceste reglementări, Autoritatea de Supraveghere **nu a avizat** proiectul Legii privind reţinerea datelor generate sau prelucrate, de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii.

Cu toate acestea, a fost adoptată şi publicată *Legea nr. 82/2012 privind reţinerea datelor generate sau prelucrate, de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii,* textul acesteia fiind similar cu cel al Legii nr. 298/2008 a cărei neconstituţionalitate a fost declarată de Curtea Constituţională (Decizia Curţii Constituţionale nr. 1258 din 8 octombrie 2009).

**b) <u>Emiterea actelor normative fără anticiparea consecinţelor aplicării soluţiilor preconizate.</u>**

Sub aspectul susmenţionat, indicăm ***proiectul Ordonanţei de urgenţă pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.***

Astfel, raportat la prevederile art. 4 alin. (4) din Directiva 2009/136/CE care indică existenţa mai multor autorităţi naţionale, stabilirea (de către Ministerul Comunicaţiilor şi Societăţii Informaţionale - MCSI) unei singure autorităţi naţionale (Autoritatea de Supraveghere), nespecializată în domeniul comunicaţiilor electronice şi securităţii tehnologice, cu excluderea implicării autorităţilor cu competenţe legale exprese absolut necesare în procesul de implementare a directivei (ANCOM, MCSI, CERT-RO), poate să aibă ca rezultat o blocare a activităţii Autorităţii de Supraveghere, ca urmare şi a competenţelor primite în anul 2010 şi, implicit, împiedicarea realizării principalului obiectiv al instituţiei noastre, cel de apărare a vieţii private a persoanelor fizice, stabilit prin Legea nr. 102/2005.

Totodată, nu au fost efectuate menţiuni privind impactul financiar asupra bugetului general consolidat, deşi actul normativ supus avizării are consecinţe bugetare şi impact asupra activităţii Autorităţii, raportat la resursele financiare şi umane ale acesteia.

Contrar observaţiilor transmise de Autoritatea de Supraveghere, a fost adoptată *Ordonanţa de urgenţă nr. 13 din 24 aprilie 2012* pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

În forma în vigoare, dispoziţiile Ordonanţei de urgenţă nr. 13/2012 nu sunt în acord cu prevederile Directivei 2002/58/CE, modificată prin Directiva 2009/136/CE, fiind de natură a institui un regim prin care Autorităţii de Supraveghere i se impune să îndeplinească atribuţii contrare rolului său de apărare a dreptului la viaţă privată al persoanelor fizice, garantat de art. 26 din Constituţia României, republicată.

Prin prevederile Ordonanţei de urgenţă a Guvernului nr. 13/2012 s-au transferat fără corespondent în Directiva 2009/136/EC către Autoritatea de Supraveghere competenţe de reglementare în domeniul comunicaţiilor electronice, deşi în România, prin legea de transpunere a Directivei 21/2002 s-a stabilit că Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii (ANCOM) este autoritatea naţională de reglementare în domeniul comunicaţiilor electronice.

Mai mult, cu toate că ANCOM este abilitată prin Legea nr. 506/2004 cu efectuarea controlului asupra furnizorilor de servicii din domeniul comunicaţiilor electronice, prin sancţionarea mai multor contravenţii, prin Ordonanţa de urgenţă nr. 13/2012 au fost transferate aceste competenţe la Autoritatea de Supraveghere, fără corespondent în Directiva 2009/136/EC**.**

Totodată, deşi atribuţiile Autorităţii de Supraveghere pot fi exercitate numai pentru protejarea drepturilor persoanelor fizice, Ordonanţa de urgenţă a Guvernului nr. 13/2012 a stabilit în sarcina sa obligaţii de protejare şi a persoanelor juridice, ceea ce pune în discuţie aspecte de constituţionalitate.

Un aspect important este acela că, deşi competenţele ANCOM au fost transferate la Autoritatea de Supraveghere, nu s-a prevăzut, concomitent, preluarea personalului de specialitate de la ANCOM sau alocarea de personal şi resurse pentru Autoritatea de Supraveghere de la bugetul de stat.

Faţă de aceste dispoziţii, Autoritatea de Supraveghere **a avizat negativ** proiectul Ordonanţei de urgenţă pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

**c) <u>Contradicţii cu reglementările interne şi comunitare existente în domeniul protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal</u>**

Sub acest context, exemplificăm ***propunerea legislativă privind colectarea şi stocarea datelor necesare identificării clienţilor serviciilor de comunicaţii electronice furnizate prin intermediul cartelelor preplătite,*** această propunere venind în contradicţie cu:

- principiile statuate de Convenţia Consiliului Europei nr. 108/1981 pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal;

- prevederile Directivei 95/46/CE a Parlamentului European şi a Consiliului pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;

- dispoziţiile Directivei 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice şi de modificare a Directivei 2002/58/CE (aceasta din urmă fiind cea privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice);

- dispoziţiile Directivei 2009/136/CE privind serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice, ale Directivei 2002/58/CE privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice şi ale Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autorităţile naţionale însărcinate să asigure aplicarea legislaţiei în materie de protecţie a consumatorului;

- punctul 5.5 din Raportul de evaluare a Directivei privind reţinerea datelor (Directiva 2006/24/CE), adoptat de Comisia Europeană în aprilie 2011.

În plus, propunerea legislativă încalcă dreptul persoanelor vizate la viaţă privată (art. 26 din Constituţia României, republicată).

Astfel, prelucrarea codului numeric personal se realizează în condiţiile prevăzute de art. 8 din Legea nr. 677/2001 şi cele ale Deciziei nr. 132/2011, însă, aşa cum erau elaborate prevederile propunerii legislative susmenţionate, sunt grav încălcate principiile proporţionalităţii şi stocării datelor prevăzute de Directiva 95/46/CE şi de Legea nr. 677/2001.

Prin instituirea obligaţiei de comunicare a datelor de identificare în sarcina clienţilor (persoane vizate, potrivit Legii nr. 677/2001) care au achiziţionat deja un serviciu de orice tip de la furnizorii de servicii de comunicaţii electronice, anterior intrării în vigoare a legii propuse, Autoritatea de Supraveghere a apreciat că aceasta contravine principiului neretroactivităţii legii, statuat de art. 15 alin. (2) din Constituţia României, republicată.

În acelaşi timp, impunerea, de către furnizorii de servicii de comunicaţii electronice furnizate prin intermediul cartelelor preplătite, a obligaţiei utilizatorilor de a se identifica sau de a comunica date cu caracter personal (nume, prenume, cod numeric personal) constituie o restrângere a drepturilor acestora, prin condiţionarea exercitării de acte/fapte de comerţ, nu numai de dovedirea identităţii persoanelor în cauză, ci şi de condiţionarea prestării unor servicii de comunicaţii de prelucrarea anumitor date cu caracter personal.

De asemenea, prin propunerea legislativă susmenţionată se aduce atingere libertăţii consumatorului de a lua decizii la achiziţionarea de servicii de comunicaţii preplătite, dat fiind că, prin obligarea identificării, poate fi influenţată opţiunea consumatorului cu privire la achiziţionarea sau nu a serviciului respectiv.

Faţă de conţinutul proiectului, Autoritatea de Supraveghere **a avizat negativ** *propunerea legislativă privind colectarea şi stocarea datelor necesare identificării clienţilor serviciilor de comunicaţii electronice furnizate prin intermediul cartelelor preplătite.*

Un alt proiect cu privire la care Autoritatea de Supraveghere a emis **aviz cu observaţii** este ***propunerea legislativă privind comunicaţiile electronice***.

În acest context, s-a apreciat că proiectul de act normativ care transpune, printre altele, Directiva 2009/136/CE şi Directiva 2009/140/CE, trebuie să preia în noua reglementare legală şi prevederile referitoare la protecţia datelor cu caracter personal din aceste acte normative comunitare, cu precădere cele din Directiva 2009/136/CE.

Totodată, s-a subliniat că activităţile desfăşurate în contextul comunicaţiilor electronice presupun efectuarea de operaţiuni de colectare şi prelucrare a unor categorii diferite de date cu caracter personal. Acest fapt are implicaţii directe asupra drepturilor fundamentale ale persoanelor fizice şi poate conduce la atingeri aduse dreptului la viaţă privată a cetăţenilor, în ceea ce priveşte protecţia datelor lor cu caracter personal.

Faţă de textul prezentat, Autoritatea de Supraveghere a apreciat necesară definirea clară a rolului şi a responsabilităţilor tuturor entităţilor din sectorul public şi privat implicate în procesul de implementare a actului normativ privind comunicaţiile electronice, în vederea stabilirii calităţii acestora de operatori sau împuterniciţi, potrivit definiţiilor date de Legea nr. 677/2001.

În acest context, Autoritatea de Supraveghere a considerat că se impune luarea în considerare a principiilor de protecţie a datelor încă de la crearea sistemelor, bazelor de date, registrelor abonaţilor şi chiar a aplicaţiilor informatice utilizate, în special prin stabilirea persoanelor autorizate, după caz a autorităţilor şi instituţiilor publice sau private, care vor avea acces la date, în scopuri legitime şi cu respectarea tuturor garanţiilor adecvate pentru respectarea drepturilor persoanelor vizate.

Referitor la modalităţile de comunicare electronică a datelor, Autoritatea de Supraveghere a subliniat că o comunicare de acest tip se poate expune la o serie de riscuri cum ar fi pierderea, distrugerea etc., chiar accidentală. Or, la alegerea modalităţilor de transmitere a datelor sau a documentelor ce conţin date cu caracter personal, trebuie să se aibă în vedere faptul că operatorii au obligaţia de a aplica măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

S-a atras atenţia şi asupra nerespectării prevederilor Legii nr. 677/2001 privind consimţământul dat pentru prelucrarea datelor cu caracter personal, în contextul stabilirii prin această propunere legislativă a obligaţiilor pe care furnizorii de servicii de comunicaţii electronice destinate publicului le au faţă de abonaţii la serviciile de telefonie destinate publicului la momentul dezvăluirii datelor acestora furnizorilor de servicii de informaţii privind abonaţii sau de registre ale abonaţilor, desemnaţi conform normelor legale în vigoare de către ANCOM.

De asemenea, referitor la prevederile capitolului „Supraveghere, control şi sancţiuni" din propunerea legislativă, Autoritatea de Supraveghere a considerat că, prin forma textului propunerii, sunt create premisele unor suprapuneri de atribuţii între ANCOM şi Autoritatea de Supraveghere.

***<u>Secţiunea a 3-a – Opinii emise în diverse chestiuni privind protecţia datelor</u>***

În anul 2012, atât persoanele vizate, cât şi operatorii au solicitat un număr de **832** de opinii cu privire la condiţiile legale de prelucrare a datelor cu caracter personal.

În continuare, prezentăm unele dintre cele mai semnificative cazuri supuse analizei Autorităţii de Supraveghere.

- ***Condiţiile legale care trebuie respectate la prelucrarea datelor angajaţilor în situaţia implementării sistemelor de supraveghere video***

Prelucrarea datelor cu caracter personal prin utilizarea unor *sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor* se supune atât prevederilor Legii nr. 677/2001, modificată şi completată, Deciziei nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

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

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

În ceea ce priveşte însă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, menţionăm că aceasta *nu este permisă*, cu excepţia situaţiilor prevăzute expres de lege sau a avizului Autorităţii Naţionale de Supraveghere.

Cu alte cuvinte, regula supravegherii video în interiorul birourilor este interzicerea efectuării acestei prelucrări, excepţiile fiind situaţiile expres prevăzute într-un act normativ care obligă angajatorul la instituirea sistemelor de supraveghere video (de ex. în clădirile băncilor).

Întrucât implementarea unui astfel de sistem de videosupraveghere poate afecta drepturile angajaţilor, în plus faţă de dispoziţiile Legii nr. 677/2001 şi ale art. 8 din Decizia nr. 52/2012, trebuie respectate şi cele prevăzute de Codul muncii. În acest sens, anterior implementării unui astfel de sistem se impune o justificare temeinică a luării acestei măsuri concomitent cu consultarea sindicatului sau a reprezentanţilor salariaţilor.

În acest context, situaţia concretă în care se intenţionează instalarea sistemelor de supraveghere video în birouri se prezintă detaliat de către operator Autorităţii de Supraveghere, cu menţionarea scopului, legitimităţii prelucrării, măsurilor de securitate etc. urmând ca autoritatea să decidă în consecinţă.

Referitor la activitatea de instalare de către unele societăţi a sistemelor de supraveghere video, la sediul altor firme, aceasta presupune prestarea unor servicii, în cadrul cărora societăţile în discuţie pot avea calitatea de împuterniciţi, potrivit definiţiei date de art. 3 lit. f) din Legea nr. 677/2001, modificată şi completată, dacă prelucrează datele personale (înregistrările video) pe seama beneficiarului (operatorul), în baza instrucţiunilor primite de la acesta (art. 20 alin. 5 din Legea nr. 677/2001).

- ***Condiţiile de prelucrare a codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare* în contextul Deciziei nr. 132/2011**

Prevederile art. 5 din Decizia nr. 132/2011 stabilesc obligaţia operatorului de a respecta principiul caracterului adecvat, pertinent şi neexcesiv al prelucrării datelor şi de a asigura o serie de garanţii adecvate atunci când se face aplicarea art. 2 lit. c) din aceeaşi decizie.

În consecinţă, colectarea copiilor documentelor de identitate contravine principiului proporţionalităţii, statuat în art. 4 alin. (1) lit. c) al Legii nr. 677/2001, modificată şi completată, generând un dezechilibru între interesele, drepturile şi libertăţile persoanei vizate şi interesele operatorului.

Referitor la durata de stocare a datelor, aceasta trebuie să fie pe perioada strict necesară îndeplinirii scopului, după care datele vor fi şterse sau distruse, după caz. Aceasta este una dintre măsurile pe care operatorul le ia în cazul aplicării art. 2 lit. c) din Decizia nr. 132/2011, însă şi art. 4 alin. (1) lit. e) din Legea nr. 677/2001. Conform acestor dispoziţii legale, datele prelucrate (indiferent de natura lor) trebuie stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate.

În acest sens, fiecare operator de date trebuie să poată justifica necesitatea stabilirii unei anumite perioade de păstrare a datelor, cu excepţia situaţiilor în care acestea sunt stabilite prin acte normative.

- ***Condiţiile legale pentru dezvăluirea datelor personale de către o autoritate publică***

Legea nr. 677/2001 stabileşte condiţiile în care datele cu caracter personal pot fi prelucrate, inclusiv dezvăluite. Potrivit dispoziţiilor acestei legi, regula generală care guvernează prelucrarea datelor personale este *consimţământul* persoanei în cauză, dat în mod expres şi neechivoc.

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

Printre cazurile de excepţie reglementate de art. 5 alin. (2) din Legea nr. 677/2001 se numără şi cele în care prelucrarea (inclusiv dezvăluirea) este necesară în vederea executării unui contract la care persoana vizată este parte, prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale a operatorului sau este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze drepturile şi libertăţile fundamentale ale persoanei vizate.

Prin urmare, regula dezvăluirii datelor este aceea a existenţei consimţământului persoanei vizate dat în mod expres şi neechivoc.

Datele pot fi dezvăluite fără consimţământul persoanei vizate numai în măsura în care solicitările pot fi încadrate în sfera excepţiilor de la consimţământ.

În situaţia în care există *interes legitim* din partea solicitantului datelor (art. 5 alin. 2 lit. e) din Legea nr. 677/2001), acesta trebuie temeinic justificat şi dovedit, concomitent cu respectarea drepturilor persoanelor vizate de către instituţia în evidenţa căreia se află datele solicitate (în special dreptul de informare şi dreptul de opoziţie, potrivit art. 12 şi 15 din Legea nr. 677/2001) şi care urmează să fie dezvăluite.

Pe cale de consecinţă, fiecare solicitare se impune a fi analizată prin raportare, în principal, la calitatea solicitantului (societate bancară, de asigurări, executor judecătoresc, organe fiscale etc.), în vederea încadrării acesteia în unul dintre cazurile de legitimitate a prelucrării (inclusiv dezvăluirii) datelor, prevăzute de art. 5 din Legea nr. 677/2001, modificată şi completată, astfel cum au fost prezentate mai sus.

- ***Prelucrarea datelor prin intermediul sistemelor de pontaj/control acces cu tehnologie biometrică***

Datele prelucrate prin intermediul sistemelor de pontaj/control acces cu tehnologie biometrică sunt considerate date cu caracter personal.

Referitor la prelucrarea datelor biometrice (amprente digitale), precizăm că, potrivit dispoziţiilor art. 4 din Legea nr. 677/2001, datele cu caracter personal destinate a face obiectul prelucrării *trebuie să fie prelucrate cu bună-credinţă* şi în conformitate cu dispoziţiile legale în vigoare*, colectate în scopuri determinate, explicite şi legitime, să fie adecvate, pertinente şi neexcesive* prin raportare la scopul în care sunt colectate şi ulterior prelucrate.

Aceste date cu caracter personal nu pot fi prelucrate de operatori *decât cu stricta respectare a prevederilor art. 4, art. 5 şi art. 7 din Legea nr. 677/2001,* modificată şi completată, şi a dispoziţiilor Deciziei nr. 11/2009 privind stabilirea categoriilor de operaţiuni de prelucrare a datelor cu caracter personal, susceptibile de a prezenta riscuri speciale pentru drepturile şi libertăţile persoanelor.

În ceea ce priveşte prelucrarea datelor biometrice ale angajaţilor, Autoritatea de Supraveghere apreciază că operaţiunile de prelucrare a acestor date prezintă riscuri speciale pentru drepturile şi libertăţile persoanelor, astfel încât colectarea şi prelucrarea acestora este excesivă prin raportare la scopul urmărit şi la mijloacele utilizate.

În sensul celor de mai sus, Autoritatea de Supraveghere a recomandat constant folosirea unei soluţii alternative la sistemul de control acces persoane şi pontaj bazat pe amprentarea angajaţilor, eventual a unui sistem bazat pe utilizarea unui cod asociat altor date de identificare ale angajaţilor.

- ***Condiţiile legale care trebuie respectate la prelucrarea datelor personale de către societăţi de payroll şi resurse umane***

Mai mulţi operatori de date cu caracter personal, dar şi împuterniciţi au solicitat sprijinul Autorităţii de Supraveghere pentru a clarifica dacă au obligaţia de a notifica prelucrările de date cu caracter personal în scopul raportării la Inspectoratul Teritorial de Muncă.

Autoritatea de supraveghere a comunicat faptul că notificarea prelucrării datelor cu caracter personal nu este necesară când prelucrarea datelor cu caracter personal referitoare la propriii angajaţi şi la colaboratorii externi este efectuată de entităţile de drept public şi de drept privat, în vederea îndeplinirii unor obligaţii legale (Decizia nr. 100/2007 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal).

Totodată, s-a adus la cunoştinţa operatorilor faptul că excepţiile de la obligaţia de a notifica nu exonerează operatorii de îndeplinirea celorlalte obligaţii care le revin potrivit dispoziţiilor legale aplicabile în domeniul protecţiei datelor cu caracter personal (informarea persoanelor vizate, confidenţialitatea şi securitatea prelucrărilor).

Autoritatea de Supraveghere a formulat în răspunsurile transmise recomandări în privinţa analizării necesităţii notificării prelucrărilor de date cu caracter personal ce nu se încadrează în situaţiile de excepţie de la obligaţia notificării, stabilite de Autoritatea de Supraveghere prin deciziile emise.

- ***Condiţiile legale care trebuie respectate la prelucrarea datelor în situaţia unei societăţi care desfăşoară activităţi de tip slotmachine***

Autoritatea de Supraveghere a fost sesizată de reprezentantul unei societăţi care desfăşoară activităţi de tip slotmachine cu privire la calitatea de operator, dar şi la necesitatea de a notifica în cazul existenţei acestei calităţi.

Raportat la aspectele sesizate, Autoritatea de Supraveghere a comunicat faptul că în măsura în care activitatea desfăşurată presupune prelucrări de date cu caracter personal ale persoanelor premiate, societatea în discuţie se supune reglementărilor stabilite de Legea nr. 677/2001, modificată şi completată, având calitatea de operator.

Totodată s-a comunicat că deşi, ca regulă, prelucrările de date efectuate de operatori trebuie declarate prin depunerea notificării, există şi situaţii de excepţie de la această obligaţie, de strictă interpretare şi aplicare, stabilite de dispoziţiile art. 22 alin. (2) din Legea nr. 677/2001, modificată şi completată şi cele ale Deciziilor nr. 90/2006, nr. 100/2007 şi nr. 23/2012 ale preşedintelui Autorităţii de Supraveghere, pentru prelucrările efectuate în scopurile vizate de acestea. Prin urmare, numai în măsura în care se prelucrează date în scopurile prevăzute în textele dispoziţiilor legale de mai sus, nu este necesară depunerea notificării.

- ***Condiţiile legale care trebuie respectate la prelucrarea datelor în scop de colectare debite/recuperare creanţe, istoric al creditării unor persoane fizice sau întreprinderi în scopul analizării solvabilităţii acestora şi furnizarea de informaţii către instituţii financiare***

Mai mulţi operatori, dar şi împuterniciţi au solicitat sprijinul Autorităţii de Supraveghere pentru a li se clarifica dacă este în sarcina lor obligaţia notificării prelucrărilor de date cu caracter personal în scop de colectare debite/recuperare creanţe, constituirea istoricului creditării unor persoane fizice sau întreprinderi, scopul final fiind analizarea solvabilităţii acestora şi furnizarea de informaţii către instituţii financiare.

Autoritatea de Supraveghere le-a comunicat acestora faptul că, în situaţia în care, potrivit dispoziţiilor legale in vigoare, în activitatea de prestare a serviciilor de acest gen se prelucrează date cu caracter personal ale persoanelor fizice care se înregistrează într-un sistem propriu de evidenţă, aceste societăţi au calitatea de operator de date cu caracter personal, cu drepturile şi obligaţiile stabilite în sarcina lor, inclusiv obligaţia de a notifica (cu excepţiile prevăzute de lege).

În schimb, dacă aceştia prelucrează datele primite de la clienţi, iar după îndeplinirea contractului de prestare servicii, respectiv la încheierea prelucrării datelor, toate informaţiile sunt returnate acestora, entităţile în discuţie au calitatea de împuterniciţi. În acest sens, trebuie să respecte obligaţiile specifice împuternicitului, respectiv cele prevăzute la art. 19 şi 20 din Legea nr. 677/2001.

Prin urmare, societăţilor în cauză li s-a recomandat stabilirea propriei calităţi, de operator sau împuternicit, în funcţie de activităţile efectiv desfăşurate, prin raportare la definiţiile date de Legea nr. 677/2001, modificată şi completată, urmând ca în funcţie de calitatea avută să se poată stabili în sarcina lor obligaţiile specifice.

- ***Condiţiile legale care trebuie respectate la prelucrarea datelor în situaţia unui transfer de date cu caracter personal ale angajaţilor în state membre ale Uniunii Europene***

Autorităţii de Supraveghere i s-a solicitat opinia cu privire la existenţa obligaţiei de notificare în temeiul Legii nr. 677/2001 în sarcina unei societăţi din România care prelucrează şi transmite într-o ţară din Uniunea Europeană datele propriilor angajaţi, în scop de resurse umane.

Societăţii mai sus menţionate i s-a comunicat că, în situaţia în care desfăşoară o activitate de prelucrare a datelor care implică şi comunicarea acestora către un destinatar situat într-un stat membru al Uniunii Europene, datele fiind destinate a face obiectul unei

prelucrări în statul respectiv, comunicarea în cauză reprezintă o transmitere de date în străinătate.

În ceea ce priveşte obligativitatea notificării, Legea nr. 677/2001 stabileşte condiţia declarării prelucrărilor de date personale efectuate pe teritoriul României la Autoritatea de Supraveghere, cu excepţia situaţiilor care sunt scutite de la notificare (art. 22 alin. 2 din lege, Deciziile nr. 90/2006, nr. 100/2007 şi nr. 23/2012 ale preşedintelui autorităţii).

În schimb, transferul datelor angajaţilor în ţări membre ale Uniunii Europene este necesar a fi declarat prin intermediul notificării.

Operatorului i s-a comunicat că, în privinţa prelucrării datelor personale ale persoanelor fizice, regula instituită de Legea nr. 677/2001, modificată şi completată, este aceea că prelucrarea acestor date, inclusiv dezvăluirea acestora, se efectuează numai cu consimţământul persoanei în cauză, dat în mod expres şi neechivoc.

Cazurile de excepţie de la obligativitatea obţinerii consimţământului sunt reglementate expres de art. 5 alin. (2) din Legea nr. 677/2001, printre care şi situaţia în care prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate.

Prin urmare, societăţii i s-a recomandat ca, în calitate de angajator, să ia măsuri care să asigure un echilibru între interesul legitim urmărit în îndeplinirea scopului prelucrării şi protecţia drepturilor fundamentale ale persoanei vizate (angajatul). Astfel, anterior prelucrării/transmiterii datelor într-un stat membru al Uniunii Europene, la acţionarul majoritar, este necesară realizarea informării persoanelor vizate, potrivit art. 12 din Legea nr. 677/2001, modificată şi completată.

Această informare trebuie să fie suficient de detaliată şi, dacă datele se intenţionează a fi transferate, să indice în special scopul transferului, datele sau categoriile de date transferate, statul unde este situat destinatarul datelor, dacă acest stat acordă sau nu o protecţie adecvată a datelor în sensul Directivei 95/46/CE şi al Legii nr. 677/2001, modificată şi completată.

- ***Necesitatea notificării în contextul iniţiativei cetăţeneşti***

Autorităţii de Supraveghere i s-a solicitat punctul de vedere cu privire la calitatea de operator şi, implicit, necesitatea depunerii notificării în situaţia exercitării iniţiativei legislative de către cetăţeni.

În acest context, s-a comunicat petentului faptul că, pentru ca o prelucrare de date cu caracter personal să intre în sfera de aplicare a legii susmenţionate, este necesar ca datele să fie organizate într-un *sistem de evidenţă, accesibil potrivit unor criterii determinate*,

indiferent dacă acest sistem este organizat în mod centralizat ori descentralizat sau este repartizat după criterii funcţionale ori geografice.

Astfel, având în vedere prevederile Legii nr. 189/1999 privind exercitarea iniţiativei legislative de către cetăţeni, republicată, este îndeplinită calitatea de operator de date cu caracter personal, înregistrarea unei notificări în Registrul de evidenţă a prelucrărilor de date cu caracter personal fiind necesară numai în măsura în care sunt îndeplinite condiţiile de mai sus.

***<u>Secţiunea a 4-a – Activitatea de reprezentare în faţa instanţelor de judecată</u>***

Practica instanţelor de judecată în litigiile referitoare la protecţia datelor s-a menţinut şi în anul 2012 într-o formă unitară.

Deşi unele sancţiuni contravenţionale aplicate de Autoritatea de Supraveghere au fost contestate în instanţă, litigiile deduse judecăţii au fost soluţionate în sensul menţinerii măsurilor aplicate.

Constatăm, aşadar, la nivelul instanţelor de toate gradele, existenţa unei abordări şi interpretări similare a normelor specifice domeniului protecţiei datelor personale, fapt ce confirmă aplicarea eficientă a legislaţiei şi, implicit, respectarea principiilor de prelucrare statuate la nivel naţional şi comunitar.

În cele ce urmează, prezentăm câteva situaţii relevante în care au fost contestate sancţiunile aplicate de Autoritatea de Supraveghere:

- ***Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video***

În urma investigaţiei efectuate de Autoritatea de Supraveghere pentru soluţionarea unei plângeri la o asociaţie de proprietari, s-a constatat că aceasta utiliza un sistem de supraveghere video în scopul „protecţiei bunurilor şi persoanelor”.

Subliniem că, prin Avizul 4/2007 privind conceptul de date cu caracter personal, Grupul de Lucru Art. 29 opinează: “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. Din acest punct

de vedere, sunt considerate date cu caracter personal în special datele constituite din sunete şi imagini, în măsura în care acestea conţin informaţii cu privire la o persoană."

Aşadar, imaginile şi sunetele care se raportează la persoane fizice identificate sau identificabile sunt considerate date cu caracter personal:

a) chiar dacă imaginile sunt utilizate în cadrul unui circuit închis; chiar dacă nu sunt asociate cu datele de identitate ale persoanei;
b) chiar dacă nu se raportează la persoane a căror figură a fost filmată, deşi conţin alte informaţii (spre ex. numărul de înmatriculare al vehiculului sau numărul PIN – *numărul de identificare personală* – obţinut la supravegherea instalaţiilor automate de retragere a banilor – ATM);
c) independent de suportul utilizat pentru prelucrare (de ex. sisteme video fixe sau mobile, precum video-receptoare portabile; imagini color sau alb-negru), de tehnica utilizată (dispozitive prin cablu, dispozitive cu fibră optică), de tipul de aparate (fixe, rotative, mobile), de modalităţile de obţinere (continuă sau discontinuă, de exemplu în cazul imaginilor obţinute la depăşirea limitelor de viteză; situaţia este diferită în cazul înregistrării de imagini efectuate ocazional şi izolat), precum şi de dezvăluire (conexiunea cu un „centru", transmiterea de imagini către terminale la distanţă etc.).

Identificarea unei persoane vizate poate fi, în limitele impuse de Directiva 95/46/CE, rezultatul unei combinări de date cu informaţiile deţinute de terţi sau cu utilizarea unor tehnici particulare sau dispozitive speciale.

Operatorul controlat, asociaţie de proprietari, utiliza mai multe camere de supraveghere ce erau orientate spre palier, acestea permiţând focusarea imaginii şi identificarea persoanelor filmate, imaginile filmate fiind stocate pe un server, localizat la parterul blocului, pe o perioadă de 30 de zile, ulterior imaginile fiind şterse automat prin înregistrarea altor imagini.

Scopul prelucrării imaginilor prin utilizarea sistemului de supraveghere video, declarat de operatorul de date cu prilejul controlului, este protecţia bunurilor şi persoanelor. Operatorul a mai declarat că la imaginile filmate au acces societatea cu care are încheiat contractul de service şi mentenanţă şi organele de poliţie şi că, urmare a unor evenimente produse, deja existase o solicitare din partea unei secţii de poliţie de transmitere a unei înregistrări.

Din verificările efectuate, s-a reţinut că, deşi informa persoanele vizate în legătură cu faptul că incinta este supravegheată video, operatorul nu notificase prelucrările de date efectuate în scopul protecţiei bunurilor şi persoanelor prin monitorizarea accesului.

În consecinţă, a fost constatată săvârşirea de către operator a contravenţiei prevăzute de art. 31 din Legea nr. 677/2001, omisiunea de a notifica şi notificarea cu rea credinţă, în forma omisiunii de a notifica, iar operatorul a fost amendat.

Operatorul a formulat plângere împotriva procesului-verbal de constatare/sancţionare încheiat de Autoritatea de Supraveghere, însă instanţa de judecată l-a menţinut ca legal, iar hotărârea a rămas irevocabilă.

- ***Prelucrarea datelor de identificare prin reţinerea copiei cărţii de identitate***

În exercitarea atribuţiilor de control, Autoritatea de Supraveghere a efectuat o investigaţie, ca urmare a unei plângeri referitoare la limitarea accesului la serviciile de comunicaţii electronice, prin condiţionarea, de către furnizorul respectiv, a depunerii fotocopiei cărţii de identitate, motivându-se necesitatea acesteia la întocmirea facturii fiscale.

În acest context, precizăm că prelucrarea datelor cu caracter personal având funcţie de identificare (seria şi numărul actului de identitate, codul numeric personal) poate fi efectuată numai cu stricta respectare a prevederilor art. 4, art. 5 şi art. 8 din Legea nr. 677/2001, modificată şi completată.

Astfel, precizăm faptul că, potrivit dispoziţiilor art. 4 alin. (1) din Legea nr. 677/2001, modificată şi completată, datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie prelucrate cu bună-credinţă şi în conformitate cu dispoziţiile legale în vigoare, colectate în scopuri determinate, explicite şi legitime, să fie adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate.

În ceea ce priveşte susţinerea operatului de date cu caracter personal privind necesitatea prelucrării datelor cu caracter personal susmenţionate în scopul emiterii facturilor fiscale, menţionăm că, potrivit art. 127 alin. (1) şi art. 155 alin. (5) lit. d) şi f) din Legea nr. 571/2003 privind Codul fiscal, cu modificările şi completările ulterioare, factura conţine, în mod obligatoriu, codul de identificare fiscală/codul numeric personal, numai în situaţia în care beneficiarii bunurilor achiziţionate sunt persoane impozabile.

În acest sens a fost exprimat şi punctul de vedere al Ministerului Finanţelor Publice căruia Autoritatea de Supraveghere s-a adresat în cadrul demersurilor sale.

În consecinţă, Autoritatea de Supraveghere consideră că prelucrarea codului numeric personal este excesivă prin raportare la scopul urmărit şi la mijloacele utilizate, respectiv emiterea facturii fiscale şi a chitanţei pentru încasarea sumei reprezentând contravaloarea pachetului de servicii de comunicaţii electronice.

Mai mult, potrivit art. 8 din Legea nr. 677/2001, prelucrarea codului numeric personal şi a seriei şi numărului actului de identitate poate fi efectuată numai dacă persoana vizată şi-a dat în mod expres consimţământul sau prelucrarea este prevăzută în mod expres de o dispoziţie legală.

Totodată, existenţa consimţământului expres şi neechivoc este prevăzută în art. 5 alin. (1) din Legea nr. 677/2001, modificată şi completată, potrivit căruia orice prelucrare de date cu caracter personal poate fi efectuată numai dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru acea prelucrare.

Or, astfel cum rezultă din conţinutul procesului-verbal, utilizatorii sunt obligaţi să-şi dea acordul la achiziţionarea pachetului de servicii de comunicaţii electronice pentru prelucrarea datelor lor, prin fotocopierea actului de identitate, în caz contrar „actul de vânzare cumpărare nu este realizat".

Această modalitate de obţinere a consimţământului încalcă prevederile art. 5 din Legea nr. 677/2001, consimţământul astfel exprimat fiind viciat.

În consecinţă, operatorul nu a respectat cerinţele Legii nr. 677/2001, modificată şi completată, referitoare la prelucrarea datelor cu caracter special, întrucât a prelucrat codul numeric personal al petiţionarului atât în lipsa unor dispoziţii legale, cât şi a consimţământului expres şi echivoc al acestuia.

Faţă de cele de mai sus, a fost constatată săvârşirea de către operator a contravenţiei prevăzute de art. 32 din Legea nr. 677/2001, respectiv prelucrarea nelegală a datelor cu caracter personal, iar operatorul a fost amendat.

Operatorul a formulat plângere împotriva procesului-verbal de constatare/sancţionare, însă instanţa a respins acţiunea ca neîntemeiată, consfinţind astfel că Autoritatea de Supraveghere a aplicat în mod corect şi legal măsurile respective ca urmare a constatării încălcării dispoziţiilor Legii nr. 677/2001.

## ***Secţiunea a 5-a – Activitatea de comunicare şi relaţii publice***

În considerarea importanţei publicării de către Comisia Europeană a proiectului pachetului legislativ de reformă în domeniul protecţiei datelor cu caracter personal, activitatea de comunicare a Autorităţii de Supraveghere s-a concentrat asupra dezbaterii publice a acestor documente, precum şi a cooperării inter-instituţionale pe plan naţional, pentru pregătirea poziţiei României.

Astfel, unul din evenimentele de impact în care a fost implicată activ Autoritatea de Supraveghere a fost reprezentat de Reuniunea organizată de Reprezentanţa Comisiei Europene în România, în primăvara anului 2012, prilej cu care au fost dezbătute implicaţiile proiectului de Regulament preconizat la nivelul Uniunii Europene,

O altă expresie a creşterii gradului de conştientizare a publicului cu privire la drepturile sale, dar şi a preocupării operatorilor asupra modului de folosire a datelor personale, a fost reprezentată de primirea de către instituţia noastră a unui număr semnificativ de cereri prin care s-au solicitat informaţii cu privire la aplicarea Legii nr. 677/2001.

În acelaşi timp, prin informaţiile furnizate telefonic şi în cadrul audienţelor acordate la sediul Autorităţii de Supraveghere, s-a realizat informarea rapidă şi eficientă a cetăţenilor şi a operatorilor, în sensul că au fost oferite, într-o manieră directă, informaţii utile cu privire la drepturile persoanelor vizate şi obligaţiile specifice operatorilor, lămuriri cu privire la condiţiile prelucrării datelor şi la dezvăluirea acestora către terţi.

Prin intermediul site-ului Autorităţii de Supraveghere s-a urmărit asigurarea unei informări adecvate a persoanelor fizice, cât şi a operatorilor care ni se pot adresa, utilizând inclusiv adresa de e-mail pusă la dispoziţie în acest sens: anspdcp@dataprotection.ro .

Atenţia acordată de mass-media domeniului protecţiei datelor personale s-a reflectat în articolele de presă publicate, pe teme specifice diverse, în reportaje televizate, ceea ce denotă interesul manifestat pentru aspectele ce implică utilizarea corespunzătoare a datelor cu caracter personal. Mass-media constituie un permanent factor important în atingerea obiectivului de sensibilizare a publicului larg cu privire la principiile de protecţie a datelor cu caracter personal.

# CAPITOLUL AL IV-LEA
# ACTIVITATEA DE CONTROL

## ***Secţiunea 1 Prezentare generală***

Activitatea de monitorizare şi control desfăşurată de Autoritatea de Supraveghere are ca scop asigurarea aplicării şi respectării prevederilor legislaţiei existente în domeniul protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal, precum şi protejarea drepturilor şi intereselor persoanelor vizate.

Activitatea de control desfăşurată în anul 2012 a fost influenţată de deficitul de resurse umane şi financiare căruia i s-au adăugat situaţii conjuncturale generate de blocarea posturilor, astfel încât programarea investigaţiilor a fost efectuată, în principal, pe raza municipiului Bucureşti şi judeţele apropiate, cu prioritate pentru soluţionarea plângerilor şi sesizărilor. Un număr mai mic de investigaţii s-a desfăşurat în zonele îndepărtate ale ţării, pentru soluţionarea respectivelor cazuri urmându-se în special procedura de investigaţii în scris.

În cursul anului 2012, au fost efectuate 94 investigaţii pe teren şi 41 în scris, pentru soluţionarea plângerilor şi sesizărilor înregistrate la autoritatea de supraveghere.

Astfel, a fost efectuat un număr total de 131 acţiuni de control pe teren, dintre care 37 controale din oficiu şi 94 investigaţii, ca urmare a celor 667 de plângeri şi sesizări transmise Autorităţii de Supraveghere.

În urma desfăşurării controalelor, au fost aplicate sancţiuni contravenţionale constând în 85 de avertismente şi 24 amenzi, toate acestea fiind dispuse în urma demersurilor de soluţionare a plângerilor şi sesizărilor adresate autorităţii.

În acelaşi context, s-a dispus încetarea prelucrării datelor personale sau a anumitor categorii de date (4 decizii**),** suspendarea prelucrării datelor cu caracter personal (1 decizie), ştergerea datelor cu caracter personal prelucrate (4 decizii); a mai fost emisă o recomandare prin care s-a dispus urmărirea respectării dispoziţiilor legale în vigoare cu privire la prelucrarea datelor cu caracter personal de către Ministerul Justiţiei în cadrul aplicaţiei ECRIS.

În activitatea de verificare a respectării dispoziţiilor legale desfăşurată pe parcursul anului 2012, Autoritatea de Supraveghere a avut drept obiective principale:

- investigarea modalităţii de prelucrare a datelor cu caracter personal în domeniul bancar;

- monitorizarea prelucrării datelor cu caracter personal în domeniul comunicaţiilor electronice;
- verificarea modalităţii de prelucrare a codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală;
- verificarea condiţiilor care trebuie respectate în cazul prelucrării datelor privind starea de sănătate.

Totodată, s-a continuat investigarea modalităţii de prelucrarea a datelor cu caracter personal ale angajaţilor, în special a datelor biometrice ale acestora.

În plus, datorită extinderii accentuate a utilizării sistemelor de supraveghere video în spaţii publice şi private, destinate prevenirii săvârşirii de fapte de natură să aducă atingere persoanelor fizice, bunurilor şi proprietăţilor publice ori private, Autoritatea de Supraveghere a dedicat anul 2012 monitorizării condiţiilor de utilizare a acestor sisteme.

## ***Secţiunea a 2-a: Investigaţii pe domenii de activitate***

- ***Prelucrarea datelor cu caracter personal în domeniul bancar***

Petiţiile adresate Autorităţii de Supraveghere care au vizat domeniul bancar au avut ca obiect, în general, transmiterea de către bănci (sau alte unităţi financiar-bancare) la Biroul de credit a datelor personale fără consimţământul persoanelor vizate sau fără respectarea drepturilor acestora, fiind încălcate prevederile Legii nr. 677/2001 şi ale Deciziei nr. 105/2007 cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit. Mai mulţi petenţi s-au plâns de faptul că nu au fost informaţi în termenul legal cu privire la transmiterea datelor. Alţi petenţi reclamă faptul că nu au primit răspuns în termen de 15 zile la petiţiile adresate instituţiilor financiar-bancare prin care şi-au exercitat drepturile prevăzute de Legea nr. 677/2001.

În situaţiile în care, în urma investigaţiilor realizate s-a constatat că operatorii, instituţii financiar-bancare, nu au respectat prevederile Legii nr. 677/2001 şi ale Deciziei nr. 105/2007, în ceea ce priveşte, în principal, termenul de transmitere a datelor către Biroul de credit, termenul de înştiinţare prealabilă a persoanelor vizate, transmiterea unui răspuns în termen de 15 zile la cererile petenţilor de exercitare a drepturilor prevăzute de Legea nr. 677/2001, respectivii operatori au fost sancţionaţi, iar datele au fost şterse.

În unele cazuri, în cadrul investigaţiei, instituţiile financiar-bancare au adus argumente şi au prezentat documente echipei de control din care a rezultat faptul că raportarea datelor

personale la Biroul de Credit a avut loc cu respectarea dispoziţiilor Legii nr. 677/2001 şi ale Deciziei nr. 105/2007.

*FIŞĂ DE CAZ*

Un petent a reclamat faptul că o societate bancară a raportat la Biroul de Credit date negative, ca urmare a unor restanţe înregistrate în mod eronat de către bancă în legătură cu creditul acordat acestuia.

Petentul a făcut dovada că a plătit ratele restante, susţinând că nu a fost înştiinţat înainte de a fi raportat la Biroul de Credit în conformitate cu prevederile art. 8 pct. 2 din Legea nr. 677/2001 şi nu a primit informaţiile prevăzute la art. 9 (1) din Decizia nr. 105/2007 a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

De asemenea, acesta a precizat că a fost în întârziere de plată, pentru creditul acordat în baza unei convenţii de credit, numai pentru 59 de zile, şi nu pentru 3 luni.

Conform înscrisurilor prezentate de către bancă echipei de control, cu ocazia investigaţiei efectuate, petentului i s-a transmis o adresă - înştiinţare prealabilă, prin care i se aducea la cunoştinţă faptul că, dacă nu achită suma restantă în termen de 30 de zile calendaristice de la data când suma trebuia achitată, datele sale negative vor fi transmise la SC Biroul de Credit SA.

Înştiinţarea prealabilă, astfel cum rezultă din borderoul de transmitere, a fost transmisă petentului prin scrisoare recomandată cu confirmare de primire, la adresa înscrisă în convenţia de credit. Potrivit declaraţiilor operatorului, ultima actualizare a datelor personale ale petentului menţionează pentru corespondenţă adresa de domiciliu la care i s-a transmis înştiinţarea prealabilă precizată mai sus.

Petentul a anexat petiţiei sale un act adiţional la convenţia de credit, document ce face dovada unei noi adrese de corespondenţă. De asemenea, conform prevederilor din actul adiţional, se modifică Condiţiile speciale ale convenţiei de credit, în sensul că: „Orice notificare sau solicitare se va face în scris şi va fi considerată corect efectuată:

- dacă va fi transmisă Băncii prin scrisoare recomandată sau confirmare de primire, la adresa sucursalei/a petiţiei menţionată în preambulul prezentului Act Adiţional;
- dacă va fi transmisă împrumutaţilor, prin scrisoare recomandată cu confirmare de primire, la adresa de corespondenţă detaliată în preambulul prezentului Act Adiţional."

Prin urmare, adresa de corespondenţă a clientului este adresa menţionată în preambulul actului adiţional (care face parte din convenţia de credit), aspect neluat în considerare de către societatea bancară.

Reprezentanţii băncii au susţinut că notificările şi somaţiile comunicate petentului au fost transmise şi cu confirmare de primire la adresa de corespondenţă menţionată în convenţie, nu la noua adresă menţionată în actul adiţional care a modificat convenţia iniţială.

În timpul controlului, reprezentanţii băncii nu au putut face dovada primirii corespondenţei de către petent la noua adresă.

De asemenea, în timpul efectuării investigaţiei, reprezentanţii băncii au şters datele negative ale petentului de la Biroul de Credit.

Societatea bancară a fost sancţionată contravenţional (avertisment) pentru prelucrarea nelegală a datelor cu caracter personal, întrucât a raportat la Biroul de Credit datele cu caracter personal ale petentului fără să îl înştiinţeze în prealabil, conform obligaţiei prevăzute de Decizia nr. 105/2007 a Autorităţii de Supraveghere cu privire la prelucrările de date cu caracter personal efectuate în sisteme de evidenţă de tipul birourilor de credit. Totodată, au fost încălcate prevederile Legii nr. 677/2001 conform cărora datele cu caracter personal trebuie să fie exacte şi dacă este cazul, actualizate, precum şi cele referitoare la informarea persoanei vizate.

*FIŞĂ DE CAZ*

O altă situaţie semnalată instituţiei noastre cu privire la prelucrarea datelor cu caracter personal în domeniul bancar a fost dezvăluirea de către o societate bancară a codului numeric personal (CNP-ul), atât în cazul efectuării unui transfer bancar către un client al băncii (CNP-ul persoanei care efectuează transferul este menţionat în detaliile tranzacţiei, deci vizualizat de beneficiar), cât şi în momentul în care un client efectuează un transfer on-line către un alt client al aceleiaşi societăţi bancare (CNP–ul beneficiarului este afişat la detaliile despre tranzacţie).

Pentru elucidarea aspectelor semnalate de petent, instituţia noastră a efectuat o investigaţie la societatea bancară şi s-a adresat Băncii Naţionale a României şi Asociaţiei Române a Băncilor.

În urma demersurilor întreprinse la operator (societatea bancară) a reieşit că această instituţie dezvăluie codul numeric personal al plătitorului, respectiv al beneficiarului unei plăţi, prin extrasul de cont, astfel:

- în cazul în care plătitorul are cont la această bancă, iar beneficiarul are cont la altă bancă, în extrasul de cont emis de banca investigată clientului său (plătitor), figurează atât codul numeric personal al plătitorului, cât şi cel al beneficiarului.
- în cazul tranzacţiilor dintre clienţii acestei bănci sunt afişate în extrasul de cont atât codul numeric personal al beneficiarului, cât şi cel al plătitorului.

- în situaţia în care plătitorul are cont la altă bancă, iar beneficiarul are cont la banca investigată, în extrasul de cont eliberat de această bancă clientului său (beneficiar) apare atât codul numeric personal al plătitorului cât şi al beneficiarului.

Pentru susţinerea modalităţilor de efectuare a plăţilor susmenţionate, operatorul a invocat o serie de reglementări, printre care Ordonanţa de Urgenţă nr. 99/2006, Legea nr. 656/2002, Hotărârea nr. 594/2008, Regulamentul nr. 9/2008, Regulamentul nr. 2/2005 etc., precum şi documentul intitulat „Termeni şi Condiţii Generale de Afaceri (TCGA)".

În corespondenţa purtată cu Banca Naţională a României, s-a precizat că prevederile actelor normative emise de această instituţie bancară, menţionate mai sus, nu instituie obligativitatea completării codului numeric personal al plătitorului pentru iniţierea unor operaţiuni de plată către persoane, altele decât Trezoreria Statului.

Astfel, Banca Naţională a României a precizat că, numai în cazul instrumentului de plată utilizat în vederea iniţierii unei plăţi către/de către Trezoreria Statului (ordinul de plată pentru Trezorerie - OPT) sunt menţionate ca elemente obligatorii codul de identificare fiscală al plătitorului, respectiv beneficiarului (art. 3 din Regulamentul Băncii Naţionale a României nr. 2/2005). Potrivit reglementărilor în vigoare, respectiv art. 3 din Regulamentul Băncii Naţionale a României nr. 2/2005 şi art. 5 lit. e) din Norma metodologică din 04.03.2005 privind utilizarea şi completarea ordinului de plată pentru Trezoreria Statului (OPT), elaborată de Ministerul Finanţelor Publice, „în rubrica „Cod de identificare fiscală" se înscrie codul de identificare fiscală al plătitorului care poate fi, după caz, codul de înregistrare fiscală sau alt cod unic de înregistrare, codul numeric personal sau numărul de identificare fiscală".

De asemenea, nici în celelalte acte normative invocate de societatea bancară investigată nu au fost identificate reglementări care să impună dezvăluirea CNP-ului plătitorului, respectiv al beneficiarului unei plăţi, prin extrasul de cont.

În acest context, operatorul a fost sancţionat cu amendă pentru prelucrarea nelegală a datelor cu caracter personal, în condiţiile în care a dezvăluit CNP-ul persoanelor vizate (plătitori sau beneficiari ai unor plăţi), prin extrasele de cont emise de bancă, fără consimţământul expres al persoanelor vizate în acest sens şi fără ca această dezvăluire să fie prevăzută în mod expres de o dispoziţie legală.

De asemenea, Autoritatea de Supraveghere a emis o decizie prin care s-a dispus ştergerea codului numeric personal al persoanelor vizate, respectiv al plătitorilor sau beneficiarilor unor plăţi, din extrasele de cont pe care le emite banca investigată. Societatea bancară a adus la îndeplinire decizia autorităţii.

- ***Prelucrarea datelor cu caracter personal în domeniul comunicaţiilor electronice***

*A. Primirea de comunicări comerciale nesolicitate*

În cursul anului 2012, a crescut considerabil numărul plângerilor având ca obiect primirea de comunicări comerciale nesolicitate, transmise prin telefon (apeluri telefonice ori SMS) sau prin poşta electronică. În cazul plângerilor considerate admisibile au fost efectuate investigaţii pentru soluţionarea aspectelor semnalate. Cazurile care nu au fost reţinute ca fiind admisibile s-au referit la acele situaţii în care petiţionarii nu au parcurs procedura prealabilă adresării unei plângeri, în condiţiile art. 25 din Legea nr. 677/2001, nu a fost posibilă identificarea expeditorului comunicărilor comerciale respective, petiţionarii aveau calitatea de persoane juridice sau nu au pus la dispoziţia Autorităţii de Supraveghere dovezi relevante ori mesajele reclamate nu îndeplineau condiţiile legale spre a fi considerate „comunicări comerciale nesolicitate" în sensul Legii nr. 365/2002 (spre exemplu, mesaje cu caracter electoral).

*FIŞĂ DE CAZ*

Într-unul dintre cazurile investigate, petentul a reclamat primirea în mod repetat a unui newsletter de la un operator, în ciuda faptului că a încercat să se dezaboneze de la acest serviciu. În urma investigaţiei, a rezultat că operaţiunea de dezabonare nu a funcţionat, fiind utilizată o adresă de e-mail folosită temporar în cadrul unei promoţii, care ulterior a fost blocată. Faţă de constatări, operatorului reclamat i-au fost aplicate sancţiuni contravenţionale în baza Legii nr. 677/2001 şi Legii nr. 506/2004, întrucât a continuat să trimită comunicări comerciale petentului, deşi acesta îşi manifestase opoziţia.

*B. Prelucrarea datelor de trafic în cadrul serviciului My Clicknet al unui operator de telefonie şi Internet*

*FIŞĂ DE CAZ*

În baza mai multor sesizări adresate de către un petent, Autoritatea de Supraveghere a efectuat o serie de investigaţii la un operator de telefonie şi Internet.

Obiectul investigaţiilor a constat în verificarea modului de prelucrare a datelor de trafic ale abonaţilor/utilizatorilor de servicii de Internet ai operatorului, în mod particular, cu privire la activarea, dezactivarea şi funcţionarea serviciului MyClicknet.

În urma efectuării mai multor investigaţii s-a constatat faptul că serviciul My Clicknet, pus în funcţiune de către operator din septembrie 2011, reprezintă un serviciu cu valoare adăugată, ce are ca scop personalizarea navigării pe Internet a abonaţilor/utilizatorilor săi, în vederea furnizării de publicitate comportamentală şi presupune direcţionarea unei copii a traficului, în vederea analizării şi prelucrării datelor de trafic ale acestora, atât anterior, cât şi ulterior acceptării acestui serviciu, prin instalarea unor fişiere tip „cookie" pe calculatoarele abonaţilor/utilizatorilor săi. Acest serviciu a fost pus în aplicare prin utilizarea soluţiei Phorm şi instalarea echipamentelor Phorm pe reţeaua operatorului.

Operaţiunile susmenţionate trebuiau efectuate cu respectarea prevederilor art. 4 şi 5 din Legea nr. 506/2004.

În acest sens, Autoritatea de Supraveghere a solicitat operatorului prezentarea unor dovezi de obţinere a consimţământului (scris) prealabil şi informat al abonaţilor/utilizatorilor pentru prelucrarea datelor lor de trafic, în sensul prevederilor din Legea nr. 506/2004, pentru acest scop specific al furnizării paginii de invitaţie, pagină care permite ulterior instalarea cookie-urilor aferente serviciului MyClicknet. Faţă de această solicitare, reprezentanţii operatorului nu au putut prezenta astfel de dovezi, documentul invocat de aceştia (Condiţii generale pentru furnizarea serviciilor operatorului) neconţinând astfel de clauze care să fie asimilate unui consimţământ expres şi informat pentru acest scop specific.

În aceeaşi măsură, nu au fost prezentate dovezi privind obţinerea consimţământului prealabil informat al abonaţilor/utilizatorilor pentru instalarea cookie-ului de opt-out, anterior şi ulterior furnizării paginii de invitaţie. Astfel, anterior furnizării paginii de invitaţie, sistemul permite verificarea prin comparare a tentativelor de accesare a Internetului de către abonat/utilizator, cu adresele URL din lista predefinită şi implementată în sistem.

În urma investigaţiilor efectuate, s-a dispus sancţionarea contravenţională a acestui furnizor, prin aplicarea unei amenzi pentru următoarele fapte:

1. nerespectarea prevederilor art. 4 alin. (2) din Legea nr. 506/2004, întrucât operatorul a efectuat operaţiuni de direcţionare şi supraveghere a comunicărilor şi a datelor de trafic aferente, ale abonaţilor/utilizatorilor săi, în scopul furnizării serviciului cu valoare adăugată MyClicknet, înainte de furnizarea paginii de invitaţie, sub aspectul efectuării copiei traficului prin mirroring, al verificării prin comparare a tentativelor de accesare a Internetului de către abonat cu adresele URL din lista predefinită şi implementată în sistem şi al verificării existenţei unui cookie oix specific acestui serviciu, fără îndeplinirea niciuneia dintre condiţiile de la art. 4 alin. (2) lit. a)-c) din Legea nr. 506/2004;

2. nerespectarea condiţiilor prevăzute la art. 4 alin. (5) din Legea nr. 506/2004 şi art. 5 din Legea nr. 506/2004 referitoare la prelucrarea datelor de trafic, întrucât operatorul a prelucrat

datele de trafic ale abonaţilor/utilizatorilor săi la serviciile de Internet, în scopul furnizării serviciului cu valoare adăugată MyClicknet, care implică utilizarea reţelei de comunicaţii electronice în scopul stocării de informaţii în echipamentele terminale ale acestora şi al obţinerii accesului la informaţia stocată în acest mod (prin instalarea de cookie-uri), fără a obţine în prealabil consimţământul expres şi informat complet al abonaţilor la serviciile de Internet ale operatorului, anterior furnizării paginii de invitaţie ce permite exprimarea acordului sau dezacordului pentru activarea serviciului MyClicknet, cât şi ulterior, în ceea ce priveşte instalarea cookie-ului opt-out pentru cei care nu şi-au dat consimţământul.

*C. Dezvăluirea datelor personale pe Internet*

Autoritatea de Supraveghere a înregistrat un număr considerabil de plângeri şi sesizări având ca obiect dezvăluirea datelor personale pe Internet. În cazul celor considerate admisibile, au fost efectuate investigaţii pentru soluţionarea aspectelor semnalate. Cazurile care nu au fost reţinute ca fiind admisibile s-au referit la acele situaţii în care petiţionarii nu au parcurs procedura prealabilă adresării unei plângeri, în condiţiile art. 25 din Legea nr. 677/2001 sau au sesizat prelucrări de date personale realizate pe pagini de Internet unde nu a fost posibilă identificarea operatorului de date personale ori care nu intrau sub incidenţa legii române.

Prezentăm mai jos constatările rezultate din procedura de soluţionare a plângerilor şi sesizărilor relevante din acest domeniu:

*FIŞĂ DE CAZ*

Mai mulţi petiţionari au reclamat divulgarea pe paginile de Internet ale unor instanţe de judecată (disponibile prin portal.just.ro) a mai multor date personale decât cele strict necesare pentru asigurarea publicităţii cauzelor aflate pe rolul acestora. În urma investigaţiilor efectuate de Autoritatea de Supraveghere, s-a constatat nerespectarea Legii nr. 677/2001 şi ca atare, au fost emise recomandări către Ministerul Justiţiei şi Consiliul Superior al Magistraturii, cu privire la modul de funcţionare a aplicaţiei ECRIS utilizată de instanţele judecătoreşti:

a) stabilirea exactă a datelor cu caracter personal care sunt strict necesare pentru realizarea scopului urmărit prin aplicaţia ECRIS, respectiv portalul instanţelor de judecată, în condiţiile în care datele trebuie să fie adecvate, pertinente şi neexcesive (postarea numai a numelui şi prenumelui justiţiabililor în cadrul soluţiei publicate);

b) elaborarea unor instrucţiuni unitare la nivel central referitoare la prelucrarea datelor personale, care să fie aplicate de către toate persoanele aflate sub autoritatea operatorului, în calitate de utilizatori ai aplicaţiei ECRIS;

c) instruirea persoanelor (angajaţilor) care lucrează sub autoritatea operatorului cu privire la dispoziţiile Legii nr. 677/2001, modificată şi completată, în special cu privire la prelucrarea datelor cu caracter personal în cadrul aplicaţiei ECRIS, portalul instanţelor de judecată;

d) revizuirea tuturor înregistrărilor efectuate până în prezent în aplicaţia ECRIS, în concordanţă cu instrucţiunile de mai sus, precum şi ştergerea datelor personale care nu îndeplinesc condiţiile de legitimitate a prelucrării datelor cu caracter personal;

e) stabilirea unei durate limitate de stocare a datelor cu caracter personal conţinute în aplicaţia ECRIS, portalul instanţelor de judecată, raportat la principiul proporţionalităţii scopului prelucrării efectuate şi în concordanţă cu dispoziţiile legale ale Codului de procedură civilă, Codului de procedură penală şi ale Legii Arhivelor Naţionale;

f) protejarea adecvată a datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat.

Plângerile primite au fost soluţionate favorabil, datele personale excesiv publicate de instanţele judecătoreşti fiind şterse.

*FIŞĂ DE CAZ*

Autoritatea de Supraveghere a fost sesizată de instituţia similară din Italia, cu privire la cazul adus la cunoştinţa sa de un petent ale cărui date personale se aflau în continuare divulgate pe Internet, aferente unui rechizitoriu emis în anul 2005 de către un Parchet, din care au fost ulterior preluate informaţii ce permit identificarea petentului, într-o serie de articole publicate de ziarele aparţinând unor anumiţi operatori. Petentul îşi exercitase dreptul de intervenţie, în vederea obţinerii ştergerii datelor personale, în raport cu Parchetul şi una dintre publicaţii, fără să îi fie soluţionate pozitiv cererile până la data la care Autoritatea de Supraveghere a iniţiat demersurile legale.

În urma investigaţiilor efectuate, s-au aplicat sancţiuni contravenţionale în sarcina acestor operatori, conform Legii nr. 677/2001. De asemenea, în cazul Parchetului şi al uneia dintre publicaţii, întrucât nu au adoptat măsuri de ştergere a datelor petentului din proprie iniţiativă (aşa cum a procedat cealaltă publicaţie), s-a dispus ştergerea tuturor datelor care permiteau identificarea petentului din toate documentele disponibile pe paginile de Internet aparţinând acestor operatori. Parchetul a dat curs deciziei emise de Autoritate, în cazul

publicaţiei urmând a se analiza iniţierea unei acţiuni judecătoreşti pentru a obţine punerea în executare a deciziei emise.

În plus, s-a emis o recomandare către Ministerul Public în vederea adoptării măsurilor necesare pentru asigurarea de către toate parchetele a respectării actelor normative în domeniul protecţiei datelor personale, interne şi internaţionale, inclusiv a recomandărilor Consiliului Europei şi a jurisprudenţei în materie, în legătură cu publicarea comunicatelor de presă sau a altor materiale informative pe Internet, astfel încât să fie garantată confidenţialitatea datelor cu caracter personal ale persoanelor fizice şi realizarea unui just echilibru între dreptul la informaţie şi dreptul la viaţă intimă, familială şi privată, implicit, dreptul la protecţia datelor personale.

Recomandarea a făcut referire la toate comunicatele de presă sau alte materiale informative existente pe paginile de Internet deţinute şi administrate de către parchetele din cadrul Ministerului Public, indiferent de data publicării acestora; măsurile prevăzute în recomandare trebuie aplicate prin evaluarea unui just echilibru între dreptul la informaţie şi dreptul la viaţă intimă, familială şi privată, implicit, dreptul la protecţia datelor personale.

*FIŞĂ DE CAZ*

În baza unei sesizări, s-a constatat că pe pagina de Internet a unei Case Judeţene de Pensii se afla postat un document în cuprinsul căruia erau menţionate mai multe date cu caracter personal, aparţinând unui număr de 87 de persoane care beneficiau de bilete de tratament, respectiv codul numeric personal şi numele complet al acestora. În urma demersurilor Autorităţii de Supraveghere, a rezultat că publicarea acestei liste se datorează unei erori tehnice, lista fiind la scurt timp retrasă, corectată şi afişată din nou pe site în forma finală. Ulterior, adresa URL unde a fost publicat documentul respectiv nu a mai putut fi accesată.

- ***Prelucrarea codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală***

La începutul anului 2012 a intrat în vigoare Decizia nr. 132/2011 a preşedintelui Autorităţii de Supraveghere privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală. Potrivit art. 6 al deciziei, colectarea şi prelucrarea codului numeric personal şi a datelor cu caracter personal cu funcţie de identificare de aplicabilitate generală, inclusiv dezvăluirea acestora, prin efectuarea şi reţinerea de copii de pe cartea de identitate sau de pe documente care le

conţin, sunt interzise, cu excepţia situaţiilor în care persoana vizată şi-a dat în mod expres consimţământul, când prelucrarea este prevăzută în mod expres de o dispoziţie legală, sau, în alte cazuri, cu avizul Autorităţii de Supraveghere şi numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.

Urmare a acestei decizii, Autoritatea de Supraveghere a procedat la verificarea din oficiu a respectării obligaţiei de notificare de către diverse entităţi publice şi private care reţin copii de pe cărţile de identitate, inclusiv prin scanarea acestor documente.

*FIŞĂ DE CAZ*

Un caz relevant în acest domeniu se referă la menţinerea copiei de pe actul de identitate al unui petent de către un furnizor de telefonie şi Internet, împotriva voinţei sale. În urma investigaţiei efectuate de Autoritatea de Supraveghere, a rezultat că această societate solicită beneficiarilor de servicii cablu TV o copie a actului de identitate, la data înmânării echipamentului utilizat pentru furnizarea serviciilor.

Petentul a contestat necesitatea depunerii unui astfel de document şi a solicitat să îi fie restituit. Reprezentanţii operatorului nu au prezentat dovezi privind existenţa unui temei legal sau a unei autorizaţii din partea Autorităţii de Supraveghere pentru reţinerea şi stocarea copiilor actelor de identitate aparţinând clienţilor săi. Ca atare, codul numeric personal şi seria şi numărul actului de identitate ale petentului au fost prelucrate, prin reţinerea copiei actului de identitate, fără consimţământul acestuia şi fără respectarea celorlalte condiţii prevăzute de art. 8 din Legea nr. 677/2001, reluate în art. 2 din Decizia nr. 132/2011. În acelaşi timp, s-a constatat faptul că operatorul a omis să menţioneze în notificarea depusă la Autoritatea de Supraveghere prelucrarea datelor personale privind codul numeric personal şi seria şi numărul actului de identitate ale clienţilor săi.

Faţă de aceste constatări, s-a reţinut săvârşirea unor fapte contravenţionale în temeiul Legii nr. 677/2001. De asemenea, prin decizia preşedintelui autorităţii, s-a dispus încetarea prelucrării prin colectare şi stocare, a codului numeric personal şi a seriei şi numărului actului de identitate, prin reţinerea copiei actului de identitate al petentului, cu obligaţia de a-i restitui copiile actului de identitate. În prezent, se află pe rolul instanţelor judecătoreşti contestarea actelor emise de Autoritatea de Supraveghere.

*FIŞĂ DE CAZ*

Într-un alt caz, a fost reclamată reţinerea copiei actului de identitate al petentului de către o societate bancară, cu ocazia efectuării unei operaţiuni ocazionale la ghişeul unei agenţii aparţinând acestei bănci. Din investigaţia efectuată de Autoritatea de Supraveghere, a

rezultat că această instituţie bancară verifică şi reţine copiile actelor de identitate ale clienţilor în mod invariabil, chiar şi pentru motivul refuzului de furnizare a copiei actului de identitate, cum a fost prezentat cazul petentului, invocându-se în acest sens dispoziţiile Regulamentului BNR nr. 9/2008 şi ale Legii nr. 656/2002 (dispoziţiile legale din domeniul prevenirii şi sancţionării spălării banilor privind măsurile obligatorii de cunoaştere a clientelei), deşi situaţia petentului nu se încadra în prevederile art. 9 din Legea nr. 656/2002.

În aceeaşi măsură, este excesivă aplicarea unei astfel de măsuri sub pretextul unei necesităţi viitoare de a dovedi identitatea deponenţilor în faţa instituţiilor abilitate. Într-o atare interpretare, orice client poate fi tratat, prezumtiv, drept o persoană ce prezintă suspiciuni în privinţa tranzacţiilor efectuate la ghişeul băncii, chiar şi în situaţii care nu sunt expres reglementate de art. 9 alin. (1) din Legea nr. 656/2002. Aplicarea unor măsuri prudenţiale de către instituţiile bancare în astfel de cazuri ar fi posibilă prin verificarea datelor personale din actele de identitate ale persoanelor care efectuează tranzacţii ce nu intră sub incidenţa Legii nr. 656/2002 şi ale Regulamentului BNR nr. 9/2008, prin confirmarea veridicităţii datelor de identificare de către lucrătorii bancari în sistemul de evidenţă intern al băncii, dar fără păstrarea copiei actului de identitate.

Faţă de cele constatate, s-a dispus aplicarea unei sancţiuni contravenţionale, solicitându-se, totodată, băncii să restituie petentului copia actului de identitate şi să adapteze procedurile interne la prevederile art. 8 din Legea nr. 677/2001 şi ale Deciziei Autorităţii de Supraveghere nr. 132/2011, în privinţa situaţiilor în care poate fi permisă reţinerea copiilor de pe actele de identitate.

*FIŞĂ DE CAZ*

Autoritatea de Supraveghere a primit mai multe sesizări cu privire la faptul că unele asociaţii care au centre de închiriat biciclete îşi fotografiază clienţii şi le solicită copii sau le scanează actele de identitate, fără acordul prealabil al acestora.

În urma acestor sesizări, s-au efectuat investigaţii, în cadrul cărora s-a constatat faptul că, pentru a închiria o bicicletă, clientul îşi poate crea un cont utilizând nume, prenume, adresă, cod numeric personal, e-mail, nr. mobil, parolă, ID sau poate merge direct la un centru de închiriere unde încheie un contract cu asociaţia. Persoanele care nu şi-au încărcat fotografia pe propriul cont sunt fotografiate la centrul de închiriere şi lasă o copie a actului de identitate sau li se scanează acest act.

Cele două asociaţii au fost sancţionate contravenţional cu amendă pentru săvârşirea contravenţiei prevăzute de art. 32 din Legea nr. 677/2001 şi cu avertisment pentru săvârşirea

contravenţiei de ”Omisiunea de a notifica şi notificarea cu rea-credinţă”, potrivit art. 31 din Legea nr. 677/2001.

În acelaşi timp, li s-a recomandat operatorilor să reanalizeze necesitatea colectării on-line a datelor cu caracter personal speciale (cod numeric personal), precum şi necesitatea colectării imaginii (prin ridicare de copii şi scanare a actelor de identitate) raportat la scopul colectării.

- ***Prelucrarea datelor cu caracter personal privind starea de sănătate***

*A. Prelucrarea datelor cu caracter special, inclusiv a datelor privind starea de sănătate, în cadrul Registrului Naţional al Donatorilor Voluntari de Celule Stem Hematopoietice*

*FIŞĂ DE CAZ*

Autoritatea de Supraveghere a fost notificată în cursul anului 2012 în legătură cu prelucrările efectuate în cadrul Registrului Naţional al Donatorilor Voluntari de Celule Stem Hematopoietice. Datele colectate în acest caz sunt: date privind starea de sănătate, nume, prenume, CNP, adresa de domiciliu, grupa sanguină şi Rh-ul, date care reflectă profilul de histocompatibilitate.

Registrul Naţional al Donatorilor Voluntari de Celule Stem Hematopoietice a fost înfiinţat prin HG nr. 760/2009. Scopul înfiinţării acestui registru este crearea şi gestionarea pe teritoriul României a unei baze de date informatice privind persoanele fizice care şi-au dat acceptul pentru a dona celule stem, în care să fie prevăzute datele personale, medicale şi de histocompatibilitate. EuropDonor-Registrul internaţional al donatorilor a fost înfiinţat printr-o directivă europeană. RNDVCSH va fi interconectat la registrul internaţional.

Ca urmare a controlului efectuat, având în vedere natura datelor sensibile, susceptibile de a prezenta riscuri pentru viaţa privată a persoanelor vizate, s-a constatat că se vor prelucra şi codul numeric personal şi date privind originea etnică, date care nu fuseseră notificate Autorităţii de Supraveghere.

Având în vedere că, la data efectuării controlului, registrul nu era funcţional, autoritatea a apreciat să recomande operatorului completarea notificării iniţiale.

*B. Prelucrarea datelor biometrice*

În anul 2012, Autoritatea de Supraveghere a primit mai multe plângeri şi sesizări prin care s-a solicitat intervenţia instituţiei noastre, deoarece operatorii de date, în calitatea lor de angajatori, au instituit pontarea orelor de program pe baza datelor biometrice rezultate din scanarea amprentelor digitale ale salariaţilor.

*FIŞĂ DE CAZ*

În urma investigaţiilor efectuate la mai mulţi operatori, ca urmare a primirii unor sesizări, a reieşit că atingerea scopului declarat al prelucrării datelor, respectiv evidenţierea timpului de lucru pentru angajaţii unor societăţi de grup, se poate realiza şi prin metode alternative, mai puţin intruzive decât prelucrarea datelor biometrice. Astfel, anterior introducerii acestui sistem, evidenţierea timpului de lucru se realizase prin semnarea condicilor de prezenţă şi, temporar, prin utilizarea unor cartele de acces. Mai mult, după introducerea noului sistem de pontare electronică bazat pe colectarea datelor biometrice, pentru o parte dintre angajaţii societăţilor din grup evidenţierea timpului de lucru s-a realizat în continuare prin semnarea condicilor de prezenţă.

În acest context, operatorii la care s-au efectuat investigaţii au fost sancţionaţi cu amendă pentru săvârşirea contravenţiilor prevăzute de art. 31 şi 32 din Legea nr. 677/2001. De asemenea, prin decizie a preşedintelui Autorităţii de Supraveghere s-a dispus încetarea prelucrării datelor biometrice ale angajaţilor acestor operatori în scopul evidenţei timpului de lucru al acestora şi ştergerea datelor biometrice deja colectate.

Ulterior, a fost reluată investigaţia ca urmare a revenirii petentului cu sesizarea că operatorii susmenţionaţi nu respectă măsurile dispuse de instituţia noastră, investigaţie în cadrul căreia nu s-au confirmat cele sesizate de petent.

- ***<u>Prelucrarea datelor cu caracter personal prin sisteme de supraveghere video</u>***

În societatea contemporană se constată extinderea tot mai accentuată a utilizării sistemelor de supraveghere video în spaţiile publice şi private, în scopul prevenirii săvârşirii de fapte de natură a aduce atingere persoanelor fizice, bunurilor şi proprietăţilor publice ori private.

Astfel, numeroase entităţi publice sau private au început să utilizeze, din ce în ce mai des, sisteme de supraveghere video, în principal pentru a controla deplasarea persoanelor, accesul în anumite spaţii, precum şi accesul la anumite evenimente ori situaţii.

Având în vedere riscurile implicate de utilizarea sistemelor de supraveghere video, colectarea şi conservarea datelor obţinute prin aceste mijloace ar trebui monitorizate astfel încât să existe garanţii minime pentru protecţia drepturilor individuale ale cetăţenilor.

Faţă de cele de mai sus, prelucrarea datelor prin mijloace de supraveghere video s-a aflat permanent în atenţia Autorităţii de Supraveghere.

*A. Prelucrarea datelor cu caracter personal prin sisteme de supraveghere video în cadrul unităţilor de învăţământ*

Urmare a intrării în vigoare a Deciziei privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video nr. 52/2012, Autoritatea de Supraveghere a procedat la verificarea respectării obligaţiei de notificare de către diverse entităţi publice şi private, în special unităţi de învăţământ, care utilizează mijloace de supraveghere video.

Astfel, au fost efectuate o serie de investigaţii din oficiu în legătură cu prelucrările de date prin sisteme de supraveghere video, ca urmare a monitorizării prin astfel de sisteme a examenelor de bacalaureat sau ca urmare a primirii unor sesizări ori plângeri din partea persoanelor vizate.

La efectuarea acestor investigaţii au fost avute în vedere, în principal, verificarea perioadei de stocare a imaginilor stabilită prin decizia emisă de preşedintele Autorităţii de Supraveghere, a condiţiilor de acces la imaginile stocate şi de dezvăluire a datelor prelucrate, a respectării cerinţelor minime de securitate şi a exercitării drepturilor persoanelor vizate.

La finalul investigaţiilor efectuate în unităţile de învăţământ, s-a concluzionat că nu sunt înregistrate imagini prin intermediul sistemelor video instalate în sălile de curs, cu excepţia celor captate în timpul desfăşurării examenelor de bacalaureat.

*B. Prelucrarea datelor cu caracter personal prin sisteme de supraveghere video, efectuată de către asociaţiile de proprietari sau de către angajatori***.**

*FIŞĂ DE CAZ*

Un petent a sesizat Autoritatea de Supraveghere cu privire la instalarea şi funcţionarea unui sistem de supraveghere video în blocul unde domiciliază, precum şi în legătură cu faptul că, la cererile prin care şi-a exercitat drepturile prevăzute de Legea nr. 677/2001 (drepturile de opoziţie, intervenţie şi acces) asociaţia de proprietari nu a emis nici un răspuns.

În urma investigaţiei efectuate a reieşit că sistemul de supraveghere video a fost instalat la asociaţia de proprietari în baza unui contract de prestări servicii în scopul prevenirii

comiterii faptelor penale, pentru siguranţa proprietarilor. Faţă de serviciile prestate, în cadrul investigaţiei s-a constatat că furnizorul acestui sistem îndeplineşte calitatea de persoană împuternicită în sensul art. 3 lit. f) din Legea nr. 677/2001, pentru prelucrarea efectuată pe seama asociaţiei.

Totodată a reieşit că petentul a adresat cererile prin care îşi exercita drepturile susmenţionate persoanei împuternicite.

În urma investigaţiei efectuate, asociaţia de proprietari a fost sancţionată cu avertisment pentru săvârşirea contravenţiilor prevăzute de art. 31 şi art. 32 din Legea nr. 677/2001.

De asemenea, s-a recomandat modificarea contractului dintre cele două părţi, în sensul art. 20 alin. (5) din Legea nr. 677/2001 şi semnarea unor angajamente de confidenţialitate de către angajaţii împuternicitului care au acces la înregistrările video din sistem, conform art. 19 din Legea nr. 677/2001. De asemenea, s-a recomandat clarificarea obligaţiilor ce revin împuternicitului în legătură cu soluţionarea cererilor prin care persoanele vizate îşi exercită drepturile prevăzute de Legea nr. 677/2001.

*FIŞĂ DE CAZ*

Autoritatea de Supraveghere a fost sesizată cu privire la faptul că accesul în birourile unei Direcţii pentru Evidenţa Persoanelor se face pe bază de amprentare a angajaţilor şi că birourile direcţiei sunt supravegheate video.

În urma investigaţiei efectuate la această instituţie a reieşit că sistemul de supraveghere video a fost instalat în scop de protejare a bunurilor instituţiei, a registrelor de stare civilă şi a altor documente care aparţin Direcţiei pentru Evidenţa Persoanelor şi de a monitoriza accesul persoanelor în birourile instituţiei. Sistemul de monitorizare a accesului angajaţilor pe bază de amprentă s-a instalat în scopul pontării orelor de serviciu.

În cadrul investigaţiei, s-a reţinut că atingerea scopurilor declarate mai sus se poate realiza şi prin metode alternative, mai puţin intruzive decât supravegherea video în birouri şi prelucrarea datelor biometrice. Astfel, anterior introducerii sistemului de supraveghere video în birouri şi a sistemului de amprentare, monitorizarea accesului persoanelor în birourile instituţiei, precum şi evidenţierea timpului de lucru pentru propriii angajaţi s-au realizat prin utilizarea unor cartele de acces.

În acest context operatorul a fost sancţionat cu avertisment, respectiv amendă, pentru săvârşirea contravenţiilor prevăzute de art. 31 şi 32 din Legea nr. 677/2001. De asemenea, prin Decizia preşedintelui Autorităţii de Supraveghere s-a dispus încetarea prelucrării

imaginii prin sistemul de supraveghere video instalat în birourile angajaţilor şi ştergerea imaginilor deja colectate până la data prezentei decizii.

Atât procesul-verbal, cât şi decizia preşedintelui Autorităţii de Supraveghere au fost atacate în instanţă.

*C. Prelucrarea datelor cu caracter personal prin sisteme de supraveghere video in cadrul activităţilor de prevenire, cercetare, reprimare a infracţiunilor, menţinerea ordinii publice*

Autoritatea de Supraveghere a efectuat controale la autorităţile poliţieneşti de sector din municipiul Bucureşti, pentru a verifica legalitatea prelucrărilor de date cu caracter personal prin utilizarea mijloacelor de supraveghere video în aceste incinte.

Ca urmare a controalelor efectuate, s-a constatat că doar la anumite secţii de poliţie sunt instalate camere de supraveghere video; în unele cazuri, imaginile preluate nu sunt stocate, fiind doar vizualizate în timp real de către ofiţerul de serviciu; în alte situaţii, camerele video sunt orientate către căile de acces, imaginile preluate sunt stocate pe server şi vizualizate numai de persoanele avizate în acest sens. S-a constatat, de asemenea, că nu se execută alte operaţiuni asupra imaginilor stocate, acestea nu sunt dezvăluite altor destinatari şi nu există legături cu alte prelucrări sau sisteme de evidenţă.

În urma verificărilor efectuate, s-a constatat că toate secţiile de poliţie, care au instalate camere de supraveghere video, au afişate la intrarea în sediu pictograme de avertizare şi anunţuri de informare a persoanelor vizate cu privire la monitorizarea accesului şi securitatea bunurilor şi persoanelor prin utilizarea sistemelor de supraveghere video, în conformitate cu prevederile art. 12 din Legea nr. 677/2001, modificată şi completată.

## CAPITOLUL AL V-LEA
## ACTIVITATEA DE RELAŢII INTERNAŢIONALE

Restricţiile bugetare au afectat şi în cursul anului 2012 activitatea de relaţii internaţionale, Autoritatea de Supraveghere aflându-se, de cele mai multe ori, în imposibilitatea de a asigura reprezentarea în cadrul reuniunilor la care a fost invitată să participe.

Cu toate acestea, Autoritatea de Supraveghere şi-a îndeplinit obligaţia legală de a participa, în calitate de observator, la reuniunile Autorităţii comune de control Schengen, iar în calitate de membru cu drepturi depline, la reuniunile organismelor comunitare de control Europol, Eurodac, Vămi, Cooperare poliţienească şi judiciară – foruri ce reunesc, în principal, reprezentanţi ai autorităţilor naţionale responsabile de protecţia datelor personale din fiecare stat al Uniunii Europene.

Subiectele dezbătute în cadrul acestor reuniuni au vizat în special aspecte privind consolidarea capacităţii de exercitare a controlului independent de către autorităţile naţionale de protecţia datelor personale, exercitarea dreptului de acces de către persoanele vizate, stabilirea competenţelor de supraveghere ale autorităţilor comune de control, modalităţile de implementare a Acordului TFTP în cadrul Programului de urmărire a finanţărilor în scopuri teroriste, precum şi probleme specifice întâmpinate în utilizarea sistemelor informatice de către autorităţile poliţieneşti şi judiciare.

Autoritatea de Supraveghere a participat anul acesta la misiunea de evaluare Schengen a Poloniei şi Ungariei, în vederea re-evaluării modului în care aceşti „membri vechi" îndeplinesc condiţiile impuse prin *acquis*-ul Schengen.

Dezbaterile pe marginea propunerilor de modificare a cadrului legal referitor la protecţia datelor existent la nivel european au constituit şi în cursul acestui an un alt element important al activităţii Autorităţii de Supraveghere la nivel internaţional.

Protecţia efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea şi detalierea drepturilor persoanelor vizate, ci şi a obligaţiilor celor care prelucrează/procesează date cu caracter personal. În mod firesc, acest fapt conduce la o sporire a sarcinilor administrative care revin operatorilor de date cu caracter personal.

Unitatea aplicării legii este piesa de bază a funcţionării UE, întrucât cetăţenii UE aşteaptă să fie trataţi egal. Ca atare este atributul legislaţiei UE să asigure aplicarea acesteia în toate ţările membre, fără a uita însă de aspectul competitivităţii în domeniul privat în aceste ţări.

Autoritatea de Supraveghere, ca şi celelalte autorităţi similare din statele membre U.E., şi-a manifestat acordul cu privire la abordarea şi, totodată, încercarea de a soluţiona prin intermediul propunerilor legislative noile provocări impuse de colectările masive de date şi utilizarea acestora în contextul unei lumi globalizate. În acest sens, au fost indicate în mod special ca fiind binevenite:

- regulile privind o transparenţă sporită şi un mai mare control asupra prelucrărilor de date;
- reglementarea principiului privind minimalizarea datelor;
- îmbunătăţirea posibilităţilor de acordare de daune persoanelor vizate ce au suferit un prejudiciu;
- clarificarea regulilor privind drepturile de acces şi de opoziţie;
- includerea drepturilor referitoare la problemele ridicate de mediul online (noul drept de portabilitate a datelor şi dreptul „de a fi uitat”);
- introducerea unor reguli simplificate şi consecvente pentru operatorii de date;
- introducerea principiului responsabilităţii;
- introducerea unor mijloace şi mecanisme precum protecţia datelor „*by design*” şi „*by default*”, studii de impact asupra vieţii private, numirea unui ofiţer pe protecţia datelor (data protection officer – DPO) şi obligaţiile privind notificarea breşelor sistemului de securitate, toate acestea servind drept stimulente pentru a demonstra responsabilitatea operatorului;
- introducerea posibilităţii atât pentru operator, cât şi pentru persoana vizată de a se adresa unei singure autorităţi de supraveghere (one stop shop) prin crearea conceptului de *lead authority* (pentru operator) care cooperează cu celelalte autorităţi de supraveghere implicate, cu toate că în ceea ce priveşte relaţia autorităţilor cu persoana vizate este încă loc pentru a aduce îmbunătăţiri;
- solicitarea unei cooperări active între autorităţile de supraveghere şi consolidarea independenţei şi atribuţiilor acestora, inclusiv prin introducerea amenzilor administrative.

## CAPITOLUL AL VI-LEA
## ACTIVITATEA DE SUPRAVEGHERE

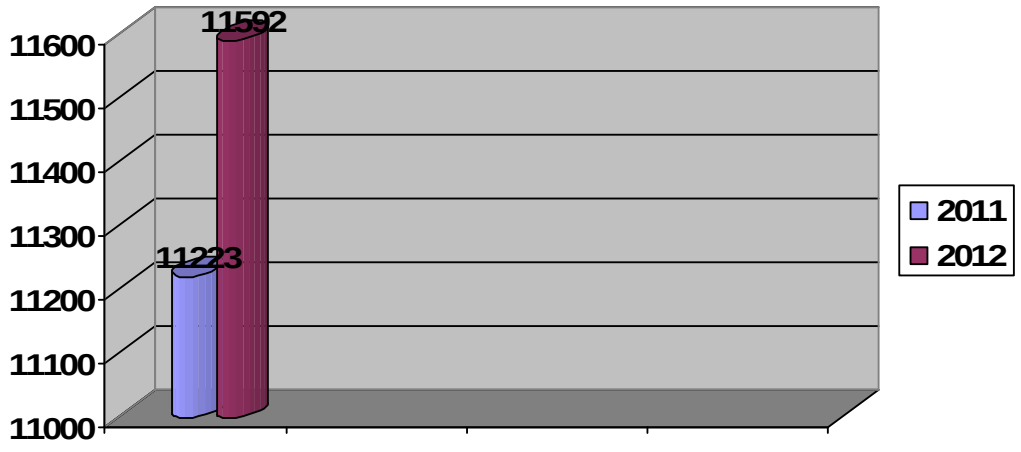
Autoritatea de Supraveghere îşi exercită atribuţiile de supraveghere şi prin activitatea de înregistrare şi analizare a notificărilor depuse de către operatorii de date cu caracter personal. În acest sens, în anul 2012, Autoritatea de Supraveghere a analizat un număr de **11592** solicitări din partea operatorilor, fie că acestea au fost notificări, fie alte cereri privind aspecte ce ţin de prelucrările de date.

Dintre acestea, **10014** au fost notificări privind prelucrările efectuate atât pe teritoriul României, cât şi transferuri de date pe teritoriul Uniunii Europene, precum şi în state terţe.

Astfel, un număr de **9501** notificări au fost fără transfer de date în afara teritoriului ţării noastre, iar **408** notificări au fost depuse având declarate transferuri de date în UE, ZEE, ţări cu nivel de protecţie adecvat al datelor, în baza principiilor Safe Harbor, precum şi în temeiul art. 30 din Legea nr. 677/2001, modificată şi completată.

De asemenea, au fost efectuate **105** transferuri în baza art. 29 alin. (4 ) din Legea nr. 677/2001, modificată şi completată, respectiv pe baza contractelor cu clauze standard. În acest sens, a fost emis un număr de **42** autorizaţii de transfer.

Totodată, au fost analizate 1578 de alte solicitări ale operatorilor, privind aspecte referitoare la dispoziţiile Legii nr. 677/2001, modificată şi completată, rapoarte anuale ale autorităţilor publice etc.




**Grafic comparativ cu anul 2011 al solicitărilor venite din partea operatorilor**

În vederea soluţionării unor notificări, atunci când a existat premisa nesocotirii unor drepturi ale persoanelor vizate şi încălcări ale Legii nr. 677/2001, au fost propuse investigaţii.

## ***Secţiunea 1 – Activitatea de înregistrare a prelucrărilor de date***

Referitor la declaraţiile de notificare pe propria răspundere, în anul 2012, s-a înregistrat o creştere considerabilă a numărului operatorilor, în special a celor din domeniul învăţământului, care au notificat prelucrări de date personale pentru scopurile „educaţie şi cultură" şi „video-supraveghere". Operatorii au fost îndrumaţi, pentru informarea persoanelor vizate asupra supravegherii video, să utilizeze afişe cu pictograme adecvate, care să conţină şi menţiuni privind scopurile supravegherii video şi operatorul care răspunde de supraveghere. Evoluţia tehnologică în plină expansiune din acest domeniu, care oferă noi posibilităţi de prelucrare a imaginilor, a impus şi o analizare a garanţiilor de asigurare a protecţiei efective a drepturilor şi libertăţilor persoanei vizate (limitarea duratei de stocare a imaginilor, informarea prealabilă a persoanelor, proporţionalitatea sistemului folosit prin raportare la scopul urmărit).

Prelucrările efectuate în baza reglementării mai sus-menţionate au fost notificate în principal de unităţile de învăţământ de toate gradele (scoli generale, licee, universităţi), cât şi de inspectoratele şcolare.

Totodată, dispoziţiile Deciziei nr. 132/2011 a preşedintelui autorităţii privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal, având o funcţie de identificare de aplicabilitate generală, au impus o analiză temeinică a declaraţiilor operatorilor ce au prelucrat aceste categorii de date, urmărind respectarea condiţiilor dezvăluirii acestora către terţi şi a tuturor regulilor specifice de prelucrare.

Manifestând o atenţie deosebită faţă de prevenirea riscurilor de utilizare excesivă şi de dezvăluire a datelor cu caracter special sau de acces neautorizat la acestea, Autoritatea de Supraveghere a recomandat operatorilor de date personale (din toate domeniile de activitate) să colecteze numai acele date cu caracter special strict necesare realizării unui scop determinat, explicit şi legitim, să obţină consimţământului expres al persoanei vizate şi să o informeze cu privire la toate drepturile acesteia.

Este de remarcat faptul că operatorii din domeniul marketingului direct sau al comerţului on-line au răspuns la recomandările şi observaţiile formulate de autoritate în ceea ce priveşte prelucrarea excesivă a codului numeric personal şi a numărului şi seriei cărţii/buletinului de identitate pe formulare sau cupoane, acolo unde nu există consimţământul explicit al persoanei vizate sau, în mod expres, o dispoziţie legală.

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

În România, transferul de date către un stat terţ se notifică şi se autorizează în cazul în care este efectuat în baza unui contract care conţine garanţii suficiente cu privire la protecţia drepturilor fundamentale ale persoanelor, conform art. 29 alin. (4) din Legea nr. 677/2001.

În cazul transferului de date către entităţi din Statele Unite ale Americii care au aderat la Principiile Safe Harbor, Autoritatea de Supraveghere a solicitat actualizarea certificatului deţinut de entitatea din Statele Unite ale Americii pentru situaţiile în care certificatul emis de Ministerul Comerţului din Statele Unite ale Americii era în afara termenului de valabilitate.

Referitor la notificarea transferurilor de date în străinătate, am constatat că, în general, operatorii cunosc prevederile Legii nr. 677/2001 cu privire la faptul că nu trebuie notificate transferurile de date efectuate în baza unor legi speciale sau ale unor acorduri internaţionale ratificate de România (în principal persoane juridice din sectorul public).

De asemenea, aceştia au ţinut cont la elaborarea contractelor între părţile între care are loc transferul de date, de prevederile Deciziilor privind clauzele contractuale tip pentru transferul de date cu caracter personal către operatorii sau persoanele împuternicite de către operator, stabilite în ţări terţe, în temeiul Directivei 95/46/CE a Parlamentului European.

În acest sens, în anul 2012, Autoritatea de Supraveghere a emis un număr de **42** autorizaţii de transfer în baza unor contracte cu clauze standard în următoarele domenii de activitate notificate:

- managementul resurselor umane, realizarea unei baze unitare de date, la nivel de grup, şi asigurarea siguranţei bazei de date (unele societăţi aleg, pentru o siguranţă mai mare a datelor stocate, să păstreze datele angajaţilor pe servere din străinătate): India, Malaezia, Filipine, SUA, Emiratele Arabe Unite, Singapore;

- testare antidrog: SUA;

- gestiune economico-financiară şi administrativă: India;

- reclamă, marketing şi publicitate: SUA;

- operaţiuni, activităţi bancare: Taiwan, India;

- cesiune de creanţe şi colectarea acestora de către importatorul de date: Emiratele Arabe Unite;

- găzduirea, întreţinerea şi administrarea soluţiei pentru activitatea emiterii card-urilor de credit: India;

- activitatea de intermediere în asigurări: SUA;

- asistenţă tehnică: Filipine;

- contactarea furnizorilor sau a clienţilor pentru informaţii de afaceri: India.

Având în vedere propunerea Comisiei Europene referitoare la un nou regulament privind protecţia persoanelor fizice cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, care va înlocui Directiva 95/46/CE, Autoritatea de Supraveghere este preocupată de respectarea regulilor corporatiste obligatorii (Binding Corporate Rules) pentru operatorii care efectuează transferul datelor, în contextul obţinerii autorizaţiei transferului către state terţe.

## CAPITOLUL AL VII-LEA
## MANAGEMENTUL ECONOMIC AL AUTORITĂŢII

Pentru anul 2012 Autoritatea de Supraveghere a avut alocate fondurile prin Legea bugetului de stat nr. 293/2011, cu modificările şi completările ulterioare, structura finală fiind următoarea:

Mii lei

| Denumire indicator | Cod | Buget actualizat la 31.12.2012 | Sume cheltuite până la 31.12.2012 | Execuţie (%) |
|---|---|---|---|---|
| Total cheltuieli | 51.01 | 3.320.000 | 3.296.371 | 99,28 |
| Cheltuieli de personal | 10 | 2.133.000 | 2.130.397 | 99,87 |
| Bunuri şi servicii | 20 | 894.000 | 885.586 | 99,05 |
| Cheltuieli de capital | 71 | 293.000 | 292.839 | 99,95 |

Restricţiile existente în execuţia bugetară au impus o permanentă actualizare a priorităţilor pentru realizarea celor mai importante proiecte cu fondurile existente.

Astfel, bugetul alocat diminuat faţă de anul precedent a avut ca efect renunţarea la efectuarea unor achiziţii de bunuri şi a investigaţiilor din oficiu pe teren în teritoriu.

În ceea ce priveşte utilizarea fondurilor alocate, putem preciza următoarele:

Suma aferentă cheltuielilor de personal ale Autorităţii de Supraveghere a constituit un procent de 64% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 2.130 mii lei, este mai mică cu 39 mii lei faţă de 2011 înregistrându-se în continuare un deficit de personal. Majoritatea cheltuielilor de personal au fost aferente plăţilor făcute pentru munca salariată a angajaţilor din departamentele de specialitate.

Cheltuielile cu deplasările au reprezentat 4,3 % din totalul cheltuielilor pe anul 2012 faţă de 5.8 % efectuate în anul 2011, deci cu 1,5 %mai mic.

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

La nivelul Uniunii Europene, Autoritatea de Supraveghere are obligaţia de a participa la lucrările Grupului de lucru Art. 29 şi la grupurile de lucru pe domeniul protecţiei datelor constituite la acest nivel şi ale autorităţilor comune de control (Schengen, Europol, Eurodac)

şi la lucrările Consiliului Europei în domeniu. Sumele alocate pentru deplasări cuprind şi aceste cheltuieli.

Nivelul relativ scăzut al celorlalte cheltuieli cu bunurile şi serviciile achiziţionate, respectiv de 885.586 lei, este rezultatul mai multor factori, dintre care menţionăm: criteriul preţului cel mai scăzut aplicat în procedurile de achiziţii, alăturat unor cerinţe tehnice atent stabilite, precum şi restricţiile bugetare.

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