

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

***R A P O R T   A N U A L***

***2011***

*Raportul de activitate este prezentat Senatului României, în temeiul art. 5 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, publicată în Monitorul Oficial al României nr. 391 din 9 mai 2005, cu modificările și completările ulterioare.*

***București***

## CUPRINS

<b>CAPITOLUL I: PREZENTARE GENERALĂ</b> .....	p. 4
<b>CAPITOLUL AL II-LEA: ACTIVITATEA DE SUPRAVEGHERE</b> .....	p. 6
<b>CAPITOLUL AL III-LEA: ACTIVITATEA DE CONTROL</b>	
<b>Secțiunea 1:</b> Prezentare generală.....	p. 8
<b>Secțiunea a 2-a:</b> Investigații tematice.....	p. 9
<b>Secțiunea a 3-a:</b> Activitatea de soluționare a plângerilor și sesizărilor.....	p. 14
<b>CAPITOLUL AL IV-LEA: ACTIVITATEA DE REGLEMENTARE ȘI CONSULTARE</b>	
<b>Secțiunea 1:</b> Acte cu caracter normativ emise de Autoritatea de Supraveghere.....	p. 28
<b>Secțiunea a 2-a:</b> Avizarea actelor normative.....	p. 29
<b>Secțiunea a 3-a:</b> Opinii emise în diverse chestiuni privind protecția datelor.....	p. 43
<b>Secțiunea a 4-a:</b> Activitatea de reprezentare în fața instanțelor judecătorești.....	p. 50
<b>CAPITOLUL AL V-LEA: ACTIVITATEA DE RELAȚII EXTERNE</b> .....	p. 55
<b>CAPITOLUL AL VI-LEA: COMUNICARE ȘI RELAȚII PUBLICE</b>	
<b>Secțiunea 1:</b> Activitatea de comunicare și relații publice.....	p. 57
<b>Secțiunea a 2-a:</b> Relația cu mass-media.....	p. 60
<b>CAPITOLUL AL VII-LEA: MANAGEMENTUL ECONOMIC AL AUTORITĂȚII</b> ...	p.61

## CUVÂNT ÎNAINTE

**Domnule președinte al Senatului,**

**Stimați senatori,**

Am deosebita onoare de a vă supune atenției Raportul de activitate pe anul 2011 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, ce conține aspecte relevante din exercitarea competențelor sale în domeniul protecției datelor cu caracter personal.

În limitele bugetului alocat, acțiunile Autorității de Supraveghere s-au concentrat, în principal, pe activitatea de soluționare a plângerilor și sesizărilor primite de la persoanele fizice, în scopul apărării dreptului la viață privată. Am efectuat 214 acțiuni de control pe teren, în special pe raza municipiului București, pentru a ne înscrie în limitele bugetare.

Măsurile și sancțiunile aplicate în urma acțiunilor de control au fost menținute de instanțele de judecată, care au confirmat temeinicia acestora și au respins contestațiile formulate de operatori împotriva proceselor verbale de sancționare contravențională emise de Autoritatea de Supraveghere.

Subliniez faptul că activitatea a fost realizată cu un număr redus de personal de execuție comparativ cel existent în anii anteriori și raportat la volumul crescut al solicitărilor primite, în condițiile în care sunt vacante atât posturi de execuție de specialitate specifică, cât și cele de conducere ale structurilor funcționale pe protecția datelor.

Pe lângă problema resurselor umane, o altă situație obiectivă care a afectat semnificativ desfășurarea activității specifice a Autorității, în semestrul II al anului 2011, a fost legată de mutarea temporară într-un spațiu pus la dispoziție de RA APPS, pe durată determinată de un an, până la alocarea unui sediu adecvat.

Pentru considerente exprimate în cuprinsul raportului, supun atenției dumneavoastră necesitatea consolidării Autorității din punct de vedere organizatoric și funcțional.

**Georgeta Basarabescu,**

**Președinte**

## **CAPITOLUL I**

## **PREZENTARE GENERALĂ**

Raportul de activitate al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal pe anul 2011 este structurat pe șapte capitole, după cum urmează:

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

Capitolul II privind activitatea de supraveghere a prelucrărilor de date cu caracter personal prezintă analiza formularelor transmise de operatorii de date, persoane fizice și juridice, care au avut obligația depunerii acestora. Au fost înregistrate un număr total de 11223 de notificări privind prelucrările de date realizate atât pe teritoriul României, cât și în statele membre, ori transferuri în state terțe.

Capitolul III referitor la activitatea de control constă într-o analiză a activității de control, în privința investigațiilor din oficiu și a celor efectuate pe baza plângerilor ori sesizărilor înregistrate. Au fost efectuate un număr total de 214 acțiuni de control pe teren, dintre care un număr de 72 investigații din oficiu și controale prealabile, la care se adaugă un număr de 141 investigații ca urmare a plângerilor și sesizărilor transmise Autorității de Supraveghere. În urma investigațiilor, au fost aplicate sancțiuni contravenționale constând în avertismente și amenzi în cuantum total de 61.300 lei.

Investigațiile efectuate din oficiu au vizat, în principal, verificarea respectării de către operatori a dispozițiilor Legii nr. 677/2001.

Cele mai multe dintre aceste plângeri au avut ca obiect raportarea datelor personale ale debitorilor diferitelor bănci la Biroul de Credit, prelucrarea datelor personale ale contribuabililor caselor de asigurări de sănătate, prelucrarea datelor biometrice ale angajaților, prelucrarea codului numeric personal, dezvăluirea datelor cu caracter personal pe Internet.

În cazurile considerate ca fiind întemeiate, au fost aplicate sancțiuni contravenționale și, după caz, s-a dispus, prin decizia președintelui Autorității de Supraveghere, încetarea prelucrării sau ștergerea datelor.

Activitatea în domeniul avizării și consultării este inclusă în Capitolului IV, care evidențiază, în principal, avizarea proiectelor actelor normative referitoare la aspecte privind protecția datelor, precum și clarificarea problemelor semnalate de diverși operatori. Aceasta s-a concretizat în emiterea a unui număr de 58 de avize și 1213 de opinii.

Prin petițiile adresate autorității, persoanele fizice și operatorii de date au solicitat informații referitoare la incidența legislației privind protecția datelor asupra activității

desfășurate de operatori, necesitatea depunerii notificării, prelucrarea datelor cu caracter special, legalitatea dezvăluirii unor date, transferul acestora în străinătate.

În secțiunea referitoare la reprezentarea în fața instanțelor de judecată, sunt prezentate dosarele relevante aflate pe rolul instanțelor judecătorești în care Autoritatea de Supraveghere a fost parte și sunt evidențiate problemele care au determinat nașterea acestor litigii, respectiv contestarea proceselor-verbale de către operatorii cărora li s-au aplicat sancțiuni.

Este de subliniat faptul că, în general, instanțele de judecată au interpretat legislația privind protecția datelor personale într-o manieră similară celei în care Autoritatea de Supraveghere a înțeles să aplice dispozițiile legale și să sancționeze faptele comise de operatori.

Capitolului V prezintă activitatea de relații externe a Autorității de Supraveghere. Sub acest aspect, reprezentanții instituției au participat la un număr restrâns de grupuri de lucru specifice în domeniul protecției datelor cu caracter personal.

Capitolul VI privind activitatea de comunicare și relații publice cuprinde informații privind activitatea instituției desfășurată în relaționarea cu alte autorități și instituții publice, cu operatorii, persoanele vizate, prin răspunsurile la cererile adresate cu privire la aplicarea Legii nr. 677/2001, a activității de audiențe și dispecerat, inclusiv în relația cu mass-media.

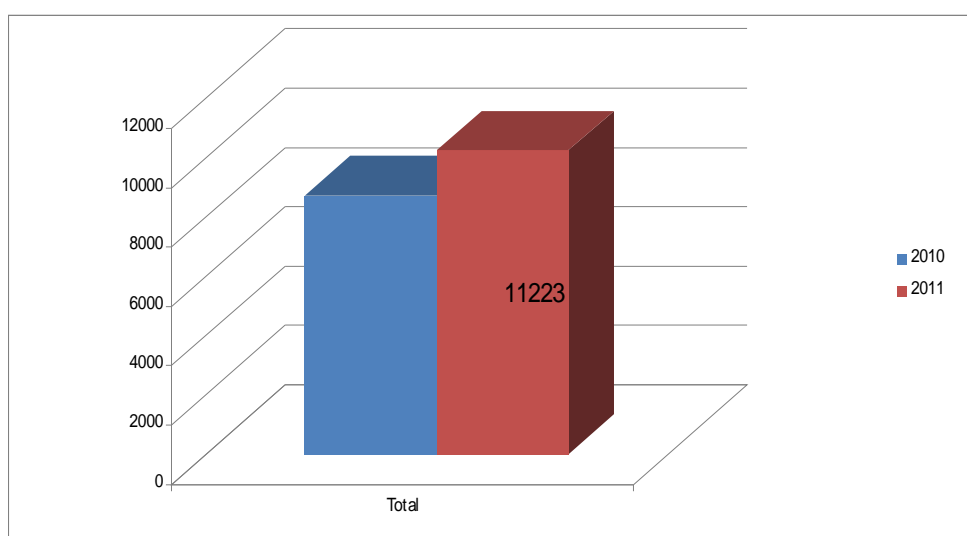
Capitolul VII referitor la resursele materiale și financiare conține informații referitoare la creditele bugetare puse la dispoziție și sumele cheltuite pe fiecare articol al clasificăției bugetare.

## **CAPITOLUL AL II-LEA**

## ACTIVITATEA DE SUPRAVEGHERE

În exercitarea atribuțiilor de supraveghere a operatorilor, Autoritatea de Supraveghere a simplificat procedura birocratică de înregistrare a notificărilor primite în format electronic, în condițiile existenței unui număr redus de salariați activi.

În anul 2011, Autoritatea de Supraveghere a analizat un număr de total de **11.223** notificări privind prelucrări de date. Comparativ cu anul 2010, numărul de solicitări a crescut cu aproximativ 2500 notificări.



În ceea ce privește modalitatea de completare a formularului de notificare de către operatori, este de menționat faptul că întreaga responsabilitate revine operatorului, punându-se accent pe obligațiile operatorului de a notifica autorității de supraveghere orice prelucrare ori ansamblu de prelucrări având același scop sau scopuri corelate. Prelucrarea datelor cu caracter personal trebuie notificată autorității de supraveghere de către operatorul de date cu caracter personal, anterior începerii acesteia.

Ca și în anii precedenți, s-au constatat anumite deficiențe în ceea ce privește modalitatea de completare a formularelor de notificare, în sensul menționării incorecte a scopului prelucrării, a categoriilor de date și a destinatarilor.

Totodată, din examinarea formularelor de notificare a rezultat că, în mai multe cazuri, a fost menținută confuzia asupra termenilor de operator – împuternicit, definiți de Legea nr. 677/2001.

Ca un aspect pozitiv, este de remarcat faptul că operatorii au răspuns, în general, la recomandările și observațiile formulate de autoritate, manifestând interes în corectarea erorilor din formularele de notificare.

De asemenea, am remarcat un feed-back adecvat față de solicitarea anexării unor documente suplimentare la formularele de notificare și o înțelegere a obligației realizării informării persoanelor vizate asupra drepturilor lor în temeiul art. 12 – 18 din Legea nr. 677/2001, modificată și completată, a principiului consimțământului persoanei vizate ca o garanție a îndeplinirii condițiilor de legitimitate a prelucrărilor de date cu caracter personal.

Pentru că aplicarea corectă a unui act normativ presupune o cunoaștere corespunzătoare a prevederilor sale, prin intermediul informațiilor furnizate pe site-ului autorității atât operatorii de date cu caracter personal, cât și persoanele fizice ale căror date personale sunt prelucrate, sunt informate cu privire la obligațiile și, respectiv, drepturile reglementate de Legea nr. 677/2001.

Modalitatea de notificare on-line este benefică atât pentru operator, oriunde ar fi situat pe teritoriul țării, cât și pentru Autoritatea de Supraveghere. De asemenea, există posibilitatea consultării pe site-ul autorității a registrului on-line privind prelucrările notificate de operatori.

Totodată, s-a remarcat schimbarea atitudinii operatorilor față de respectarea legislației specifice domeniului protecției datelor personale, manifestarea interesului crescut pentru notificarea prelucrărilor de date cu caracter personal, buna înțelegere a conținutului noțiunilor din formularul de notificare, conștientizarea necesității realizării informării persoanelor vizate asupra drepturilor acestora în temeiul art. 12 – 18 din Legea nr. 677/2001, a respectării principiului „consimțământului persoanei vizate”, ca o garanție a îndeplinirii condițiilor de legitimitate a prelucrărilor de date cu caracter personal.

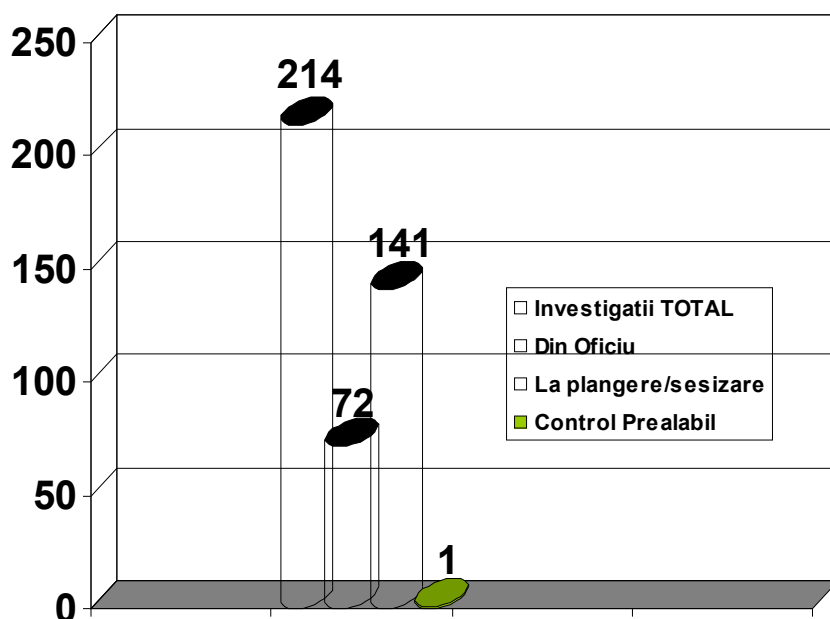
## **CAPITOLUL AL III-LEA**

### **ACTIVITATEA DE CONTROL**

## Secțiunea 1: Prezentare generală

Activitatea de control desfășurată în anul 2011 a fost influențată de restricțiile bugetare, astfel încât programarea investigațiilor a fost efectuată, în principal, pe raza municipiului București, cu prioritate pentru soluționarea plângerilor și sesizărilor.

Astfel, în cursul anului 2011, a fost efectuat un număr total de **214** acțiuni de control pe teren, dintre care un număr de **72** investigații din oficiu, **1** control prealabil și un număr de **141** investigații ca urmare a plângerilor și sesizărilor transmise Autorității de Supraveghere.



Majoritatea investigațiilor din oficiu au urmărit realizarea planului anual alcătuit pe baza unor teme desprinse din practica autorității, în domeniile în care se constatare în perioada anterioară o aplicare neadecvată a Legii nr. 677/2001.

Investigațiile au fost programate cu două teme principale :



- activități desfășurate de persoane care exercită profesii liberale (avocați, notari, executori judecătorești și alții)
- operatori/împuterniciți din domeniul marketingului direct.

În urma investigațiilor, au fost aplicate sancțiuni contravenționale constând în **41** de avertismente și **50** amenzi.

Cuantumul total al amenzilor aplicate a fost de **61.300 lei** (RON).

În conformitate cu prevederile art. 21 alin. (3) lit. d) din Legea nr. 677/2001 și ale art. 3 alin. (5) din Legea nr. 102/2005, în cazul în care s-a constatat încălcarea dispozițiilor Legii nr. 677/2001, în funcție de împrejurări s-au dispus, pe lângă sancțiunile contravenționale, și unele măsuri specifice obligatorii, prin decizii ale președintelui Autorității de Supraveghere.

În acest context, au fost emise **6 decizii** prin care s-a dispus măsura încetării prelucrării datelor personale sau numai a anumitor categorii de date, **1 decizie** prin care s-a dispus măsura suspendării prelucrării datelor cu caracter personal prelucrate și **1** recomandare prin care s-a dispus urmărirea respectării dispozițiilor legale în vigoare cu privire la comunicarea prin publicitate pe Internet a actelor administrative fiscale emise de autoritatea publică investigată.

## **Secțiunea a 2-a Investigații tematice**

Reduse ca număr, ca urmare a motivelor menționate în secțiunea de mai sus, investigațiile din oficiu au urmărit realizarea obiectivului stabilit prin planul anual tematic.

În conformitate cu obiectivul acestuia, au fost vizate domeniile în care se constatase anterior o aplicare neadecvată a Legii nr. 677/2001, respectiv în domeniul activităților desfășurate de persoane ce exercită profesii liberale și ale marketingului direct.

### **2.1. Investigații tematice efectuate la persoane ce exercită profesii liberale**

Investigațiile desfășurate la entitățile care prelucrează date cu caracter personal în scop notarial au avut ca scop verificarea modalității în care sunt respectate prevederile Legii nr. 677/2001 în cadrul activității notariale, inclusiv sub aspectul respectării drepturilor persoanelor vizate.

Entitățile supuse controlului au fost: birouri notariale și asociații notariale care prelucrează datele personale numai în calitate de operatori.

Autoritatea de Supraveghere a verificat dacă în acest domeniu sunt prelucrate și datele personale ale minorilor. Astfel, s-a constatat un număr restrâns de astfel de prelucrări,

efectuate numai pentru legalizarea cărților de identitate, diplomelor de absolvire și certificatelor de naștere ale acestora.

În urma efectuării investigațiilor s-a recomandat operatorilor informarea corectă și completă a persoanelor vizate prin intermediul documentelor de colectare a datelor sau prin afișare la sediu.

### ***FIȘĂ DE CAZ***

În cadrul unei investigații efectuate de Autoritatea de Supraveghere la un birou notarial care a notificat prelucrările pe care le efectuează în scopul activității notariale, s-a constatat că nu a reconfirmat prelucrările de date cu caracter personal efectuate pentru scopul declarat.

Notariatul public prin activitatea desfășurată prelucrează următoarele date personale: nume, adresă de domiciliu, CNP, serie și nr. act de identitate, data nașterii, etc. Aceste date se regăsesc în documentele emise de operator (contracte de vânzare-cumpărare, procuri, etc.) clienților.

Datele prelucrate sunt transmise către autoritățile publice și organizațiile profesionale, iar perioada de stocare a datelor cu caracter personal este prevăzută în Nomenclatorul arhivistic pentru o perioadă cuprinsă între 3 ani până la 5 ani sau permanent.

S-a mai constatat că operatorul nu realizează o informare completă a persoanelor vizate care să respecte prevederile art. 12 din Legea nr. 677/2001, așa cum reiese din documentele emise de operator (contract de vânzare-cumpărare).

Operatorul nu a luat toate măsurile de protejare a datelor cu caracter personal așa după cum prevede de Ordinul nr. 52/2002 și nu a elaborat o politică de securitate scrisă, însă a stabilit modalități de autentificare și identificare a utilizatorilor la baza de date cu caracter personal, acces la sistem în funcție de atribuțiile de serviciu;

În desfășurarea activității operatorul utilizează un sistem de evidență mixt, iar accesul la documentele emise este unul restricționat.

Operatorul nu și-a stabilit clauze de confidențialitate pentru angajații săi.

Față de constatările efectuate, echipa de control a recomandat operatorului să transmită formularul de notificare completat potrivit scopurilor în care prelucrează date cu caracter personal în conformitate atât cu dispozițiile Legii nr. 677/2001 cât și ale Deciziei nr. 95/2008 a președintelui Autorității de Supraveghere.

S-a mai recomandat ca operatorul să realizeze o informare completă a persoanelor vizate, în sensul furnizării tuturor informațiilor prevăzute de condițiile art. 12 din Legea nr.

677/2001 și, de asemenea, ca operatorul să elaboreze o procedură pentru asigurarea securității prelucrărilor de date personale în conformitate cu Ordinul nr. 52/2002.

## **2.2. Investigații tematice efectuate la entități care desfășoară activități în domeniul marketingului direct**

Investigațiile desfășurate la entitățile care prelucrează date cu caracter personal în scop de marketing direct au avut ca scop verificarea modalității în care sunt respectate prevederile Legii nr. 677/2001.

În acest domeniu de activitate entitățile colectează datele cu caracter personal, fizic și/sau on-line pe baza comenzii. Datele colectate în scop de marketing direct sunt, în principal, numele, prenumele, adresa, email, parolă, telefon.

### ***FIȘĂ DE CAZ***

Autoritatea de supraveghere a efectuat o investigație la o societate comercială care are ca obiect principal de activitate „servicii hosting și internet”.

Operatorul a notificat Autorității de Supraveghere prelucrarea datelor cu caracter personal colectate în 2010, pentru care a primit număr de înregistrare în registrul de evidență a prelucrării a datelor cu caracter personal.

Din verificarea site-ului societății a rezultat că există un formular de colectare de date ce se completează în vederea efectuării unei comenzi on-line. Acest formular conține următoarele date cu caracter personal: numele, prenumele, adresa, email, parolă, telefon, cod numeric personal, iar scopul prelucrării este „servicii de comunicații electronice”, conform declarațiilor reprezentanților societății.

Formularul conține mențiunea : „Doriți să obțineți informații despre produse, servicii, etc. ?” , cu posibilitatea de a opta.

Perioada de stocare a datelor cu caracter personal este de 2015 – 2019. Din declarațiile reprezentanților operatorului a rezultat faptul că în momentul în care clientul nu mai dorește continuarea colaborării, datele sale sunt șterse automat din baza de date. Datele cu caracter personal sunt colectate de operator direct de la persoana vizată.

Siguranța datelor este asigurată prin certificat, la baza de date stocată având acces persoanele desemnate.

Baza de date cu caracter personal este găzduită de o altă societate care asigură și mentenanța servere-lor. Prin Contractul de service IT dintre operator și societate este stabilită o clauză de confidențialitate a datelor personale, cu mențiunea că accesul la baza de date este posibilă numai cu acordul în prealabil al operatorului.

În urma controlului efectuat, s-a recomandat operatorului eliminarea câmpului CNP din formularul de comandă și completarea notei de informare conform dispozițiilor Legii 677/2001.

### **2.3. Prelucrarea nelegală a datelor cu caracter personal**

În cursul anului 2011, mai mulți petenți au formulat plângeri prin care au reclamat faptul că operatorii au încălcat dreptul de acces, prevăzut în art. 13 din Legea nr. 677/2001, respectiv fie nu au transmis persoanelor vizate informațiile solicitate, fie nu s-a răspuns cererilor formulate de persoanele vizate în termenul legal de 15 zile.

#### ***FIȘĂ DE CAZ***

Printr-o plângere adresată Autorității de Supraveghere, s-a reclamat faptul că o instituție publică a dezvăluit datele personale ale mai multor persoane, inclusiv ale petentului, printr-un răspuns comun formulat către mai mulți petiționari.

Din verificările efectuate, s-a reținut că un răspuns comun la mai multe cereri formulate de petiționari având același conținut, a fost trimis către 13 persoane, având menționate în clar numele, prenumele, adresa poștală și de e-mail ale fiecăruia dintre petiționari. În cazul petentului, conform înscrisului și a declarațiilor sale, sunt specificate: nume, prenume, adresa reședinței și adresa de e-mail.

De asemenea, a rezultat că 13 persoane au depus individual cerere în temeiul Legii nr. 544/2001, prin care au solicitat furnizarea unor informații de interes public.

Petiționarii au solicitat ca răspunsurile să fie transmise fie pe adresa poștală, fie prin intermediul poștei electronice.

Potentul a solicitat ca răspunsul să fie transmis la adresa de corespondență indicată în petiție sau la adresa de e-mail specificată.

Răspunsul formulat de instituția publică la cele 13 petiții a fost transmis, atât prin poștă scrisă cât și prin poștă electronică, prin menționarea în clar a datelor personale ale tuturor petiționarilor astfel încât fiecare persoană a aflat datele cu caracter personal ale celorlalți 12 petiționari.

Reprezentanții instituției publice au declarat că motivul pentru care s-a transmis răspunsul de această manieră, permițând dezvăluirea fără consimțământ a unor date personale, a fost datorită conținutului identic al petițiilor, întrucât s-a considerat că provin din aceeași sursă.

Față de cele relatate mai sus, operatorul a fost sancționat contravențional, pentru săvârșirea contravenției prevăzută de art. 32 din Legea nr. 677/2001, respectiv prelucrarea nelegală a datelor cu caracter personal, prin încălcarea art. 5 din aceeași lege, întrucât operatorul a dezvăluit datele personale (nume, prenume, adresă poștală, adresă de e-mail) ale unor petiționari, fără consimțământul expres al acestora și/sau în lipsa unui temei legal expres care să permită o astfel de diseminare.

### ***FIȘĂ DE CAZ***

Printr-o plângere adresată Autorității de Supraveghere, un petent a reclamat faptul că o companie de telefonie mobilă a încălcat dreptul de acces la date prevăzut de art. 13 din Legea nr. 677/2001, petentul fiind nemulțumit de răspunsul transmis de reprezentanții companiei.

Din corespondența purtată dintre operator și petent s-a reținut că acesta din urmă, prin cererea sa, s-a identificat prin nume, cod numeric personal, număr de telefon, adresă de e-mail și a precizat că a fost client al companiei, din anul 2009, după care și-a portat numărul de telefon într-o altă rețea.

Operatorul a răspuns petentului în sensul că acceptul cu privire la prelucrarea datelor cu caracter personal a fost dat de petent la momentul semnării contractului, iar după rezilierea numărului de telefon mobil, adică după anularea contractului semnat, prelucrarea datelor cu caracter personal a încetat, în momentul anulării contractului.

De asemenea, petentul a fost informat în legătură cu faptul că numărul de telefon reprezintă o sursă internă ce poate fi accesată doar în scopuri ce vizează bazele interne ale companiei și nu poate fi folosit în alte situații.

Potentul a mai susținut că a fost sunat de un reprezentant al operatorului, care a susținut că a luat numărul de telefon din baza de date a companiei.

Din declarațiile reprezentantului operatorului a reieșit că numărul de telefon rămâne proprietatea companiei care a alocat numărul de telefon, iar serviciul este prestat de compania unde petentul și-a portat numărul de telefon mobil.

Reprezentantul companiei a mai declarat că datele personale (nume, număr de telefon mobil) sunt stocate în sistemul electronic o perioadă de 3 ani de la data încetării contractului după care se anonimizează datele personale.

Față de cele relatate mai sus, operatorul a fost sancționat contravențional, pentru săvârșirea contravenției prevăzută de art. 32 din Legea nr. 677/2001, cu încălcarea dreptului de acces la date, prevăzut de art. 13 din aceeași lege, întrucât operatorul nu a comunicat petentului toate informațiile prevăzute de art. 13 alin. (1) din Legea nr. 677/2001 și nu le-a transmis acestuia în termen de 15 zile de la data cererii transmise operatorului.

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

Autoritatea de Supraveghere a primit în cursul anului 2011 un număr de **679** petiții dintre care **404** plângeri și **124** sesizări prin care au fost sesizate aspecte legate de posibile încălcări ale drepturilor reglementate de Legea nr. 677/2001 și ale Legii nr. 506/2004. De asemenea, s-au primit **90** solicitări de informații referitoare la domeniul protecției datelor personale și un număr de **61** petiții care nu intră în obiectul de activitate al Autorității.

Cele mai multe dintre aceste plângeri au avut ca obiect raportarea datelor personale ale debitorilor diferitelor bănci la Biroul de Credit, prelucrarea datelor personale ale contribuabililor caselor de asigurări de sănătate, prelucrarea datelor biometrice ale angajaților, prelucrarea CNP-ului, dezvăluirea datelor cu caracter personal pe Internet.

Ca și în anii anteriori, o parte din plângerile depuse de persoanele vizate au fost respinse ca inadmisibile sau neîntemeiate pentru următoarele motive:

- nerespectarea procedurii prealabile prevăzute de lege;
- reclamarea unor fapte în legătură cu care Autoritatea de Supraveghere nu avea competența materială sau teritorială să intervină, cum ar fi: refuzul furnizării unor date informatice aparținând unor terțe persoane, primirea de comunicări comerciale specifice marketingului direct de la operatori care nu erau situați în România, prin mijloace care se află pe teritoriul altor state, fapte care sunt în competența altor instituții sau autorități publice;
- neprezentarea de dovezi în susținerea plângerii.

În cazurile considerate ca fiind întemeiate, au fost aplicate sancțiuni contravenționale și, după caz, s-a dispus prin decizia președintelui Autorității de Supraveghere încetarea prelucrării datelor, ștergerea datelor personale prelucrate cu nesocotirea drepturilor persoanelor vizate sau suspendarea prelucrării datelor personale.

- **Prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență de tipul birourilor de credit**

Petițiile transmise autorității de supraveghere în legătură cu prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență de tipul birourilor de credit au vizat, în general, următoarele aspecte:

- transmiterea datelor personale cu nerespectarea prevederilor Deciziei nr. 105/2007 a președintelui Autorității de Supraveghere privind prelucrările de date cu caracter personal efectuate în sisteme de evidență de tipul birourilor de credit;
- nerespectarea drepturilor persoanelor vizate prevăzute de Legea nr. 677/2001 de către instituțiile de credit;
- raportare abuzivă de date negative la SC Biroul de Credit SA ca urmare a unor restanțe înregistrate în mod eronat de către bancă;
- solicitări de informații privind consecințele transmiterii datelor negative la Biroul de Credit;
- solicitări adresate în mod eronat autorității de supraveghere de a comunica informații referitoare la datele înscrise la SC Biroului de Credit SA.

Multe dintre petițiile care vizau transmiterea ilegală de date la SC Biroul de Credit SA, au fost trimise instituției noastre fără respectarea procedurii prealabile, respectiv fără a fi înaintată o plângere cu același conținut către operator (instituții de credit) sau fără a se aștepta împlinirea termenului de 15 zile, termen care curge de la data sesizării operatorului.

Prin petițiile ale căror aspecte semnalate au făcut obiectul demersurilor instituției noastre, petenții au reclamat faptul că operatorii (instituții de credit):

- au raportat date negative către sisteme de tipul birourilor de credit fără înștiințarea prealabilă prevăzută de art. 8 din Decizia nr. 105/2007;
- nu au furnizat persoanelor vizate (debitori) toate informațiile prevăzute de art. 9 din Decizia nr. 105/2007;
- nu au răspuns în termenul legal de 15 zile, în cazul exercitării dreptului de opoziție;
- au transmis eronat date negative la SC Biroul de Credit SA.

### ***FIȘĂ DE CAZ***

Prin plângerea adresată autorității, petenta a solicitat verificarea modului în care au fost respectate dispozițiile legale în legătură cu transmiterea datelor sale cu caracter personal la SC Biroul de Credit SA.

În fapt, petiționara a susținut că instituția bancară a raportat-o S.C. Biroului de Credit S.A. fără înștiințarea prealabilă, conform art. 8 alin. (2) din Decizia nr. 105/2007.

De asemenea, petenta a reclamat și faptul că banca nu i-a răspuns în termenul legal de 15 zile la cererea prin care a solicitat ștergerea datelor negative transmise la S.C. Biroul de Credit S.A.

În urma investigației efectuate a reieșit că societatea bancară a raportat la SC Biroul de Credit S.A. datele cu caracter personal ale petiționarei, ca urmare a înregistrării unor întârzieri la plata ratelor aferente creditelor acordate de bancă.

Având în vedere faptul că notificarea (înștiințare prealabilă) referitoare la transmiterea datelor la Biroul de Credit S.A. nu a respectat termenul de 15 zile, prevăzut de art. 8 alin. (2) din Decizia nr. 105/2007, societatea bancară fost sancționată contravențional.

Totodată, banca a mai fost sancționată și pentru faptul că nu a comunicat un răspuns în termenul legal de 15 zile, prevăzut de art. 15 alin. (4) din Legea nr. 677/2001, la cererea prin care petiționara a solicitat ștergerea datelor negative transmise la S.C. Biroul de Credit S.A.

#### ***FIȘĂ DE CAZ***

Într-un alt caz, prin plângerea adresată instituției noastre petentul a reclamat faptul că instituția bancară a transmis datele sale personale la Biroul de Credit fără înștiințare prealabilă conform art. 8 alin. (2) din Decizia nr. 105/2007 și nu a răspuns în termenul legal de 15 zile la exercitarea dreptului de opoziție.

În urma investigației efectuate a reieșit că petentul a înregistrat datorii la plata creditului și a fost raportat la Biroul de Credit S.A. anterior emiterii Deciziei nr. 105/2007, care prevede la art. 8 alin. (2) obligația participanților la sistemele de evidență de tipul birourilor de credit de a transmite datele negative ale solicitanților de credit numai după înștiințarea prealabilă a acestora.

Totodată, întrucât s-a constatat că instituția bancară nu a răspuns cererii petiționarului în termenul legal de soluționare, respectiv 15 zile de la data primirii cererii, conform art. 15 alin. (4) din Legea nr. 677/2001, societatea bancară a fost sancționată contravențional.

#### ***FIȘĂ DE CAZ***

Prin plângerea adresată, petiționarul ne-a sesizat faptul că societatea bancară a transmis datele sale cu caracter personal către S.C. Biroul de Credit S.A. cu încălcarea dispozițiilor art. 8 alin. (2) din Decizia nr. 105/2007, în sensul că s-a procedat la raportarea unor date negative la S.C. Biroul de Credit S.A., fără notificare prealabilă.



În urma investigației efectuate la societatea bancară a rezultat că, în calitate de client al băncii, petiționarul a beneficiat de două credite care au fost restructurate, iar ulterior refinanțate, acesta figurând în evidența societății bancare cu un singur credit.

În acest context, societatea bancară a radiat inițial de la S.C. Biroul de Credit S.A. înregistrările întâzierilor care au fost efectuate până la data operării restructurării în cazul ambelor credite.

Ulterior, ca urmare a demersurilor instituției noastre, referitoare la notificarea (înștiințarea prealabilă) a petiționarului, înainte de raportarea datelor negative la S.C. Biroul de Credit S.A., conform prevederilor art. 8 alin. (2) și art. 9 alin (1) din Decizia nr. 105/2007, societatea bancară a procedat la corectarea informațiilor transmise la Biroul de Credit și după restructurarea creditelor.

Astfel, din analizarea Raportului de credit emis de Biroul de Credit, a reieșit că datele negative transmise de societatea bancară la Biroul de Credit cu privire la restanța petentului au fost șterse, situația semnalată fiind astfel remediată.

### ***FIȘĂ DE CAZ***

Printr-o plângere, un petent a reclamat faptul că o societate bancară a raportat la S.C. Biroul de Credit S.A. date negative ca urmare a unor restanțe înregistrate în mod eronat de către bancă în legătură cu creditul său.

În urma investigației efectuate la societatea bancară a rezultat că în mod eronat au fost raportate datele negative la S.C. Biroul de Credit S.A. referitoare la contractul de credit al petiționarului.

Întrucât, potrivit art. 4 din Decizia nr. 105/2007, participanții au obligația de a transmite date exacte și corecte către sistemele de evidență de tipul birourilor de credit, societatea bancară a efectuat demersurile necesare pentru corectarea informațiilor transmise la S.C. Biroul de Credit S.A.

Astfel, din analizarea Raportului de credit emis de S.C. Biroul de Credit S.A. a reieșit că datele negative transmise de societatea bancară la S.C. Biroul de Credit S.A. cu privire la restanța petentului au fost șterse, situația semnalată fiind remediată.

- **Dezvăluirea datelor cu caracter personal pe Internet**

Prin mai multe petiții adresate Autorității de Supraveghere, a fost semnalată dezvăluirea unor date cu caracter personal, în special al codului numeric personal, pe internet.

➤ **Prelucrarea datelor personale ale contribuabililor caselor de asigurări de sănătate**

***FIȘĂ DE CAZ***

În cursul anilor 2010-2011, Autoritatea de Supraveghere a fost sesizată cu privire la publicarea pe paginile de Internet ale caselor de asigurări de sănătate din județele Brașov, Constanța și Bistrița-Năsăud a datelor personale ale contribuabililor în cadrul anunțurilor colective emise în baza Codului de procedură fiscală (decizii de impunere, somații) pentru sute de persoane fizice presupus datornice la fondul de asigurări de sănătate. Din investigațiile efectuate de Autoritatea de Supraveghere a rezultat că aceste case teritoriale nu au efectuat diligențele necesare pentru comunicarea actelor administrative fiscale în celelalte modalități reglementate de art. 44 alin. (2) lit. a), b) sau c) din Codul de procedură fiscală, cu respectarea caracterului exact și actualizat al informațiilor utilizate în vederea emiterii și ulterior, dacă este cazul, a publicității deciziilor de impunere față de aceste persoane.

Publicitatea actelor administrative fiscale prin Internet este reglementată de Ordinul ministrului finanțelor publice nr. 94/2006 privind aprobarea modelului și conținutului formularelor și a instrucțiunilor de completare a acestora în vederea îndeplinirii procedurii de comunicare a actelor administrative fiscale prin publicitate, ca o ultimă și subsidiară modalitate de comunicare a acestor acte.

Conform instrucțiunilor de completare din anexa nr. 2 la acest ordin, pct. 1, comunicarea prin publicitate se efectuează în situația în care actul administrativ fiscal nu a putut fi comunicat prin una dintre modalitățile de comunicare prevăzute la art. 44 alin. (2) lit. a), b) și c) din Codul de procedură fiscală, respectiv: prezentarea contribuabilului la sediul organului fiscal, remiterea sub semnătură a actului administrativ fiscal de către organul fiscal, prin poștă la domiciliul fiscal al contribuabilului cu scrisoare recomandată cu confirmare de primire și alte mijloace (fax, e-mail), dacă se asigură transmiterea textului actului administrativ fiscal și confirmarea primirii acestuia.

Modelul anunțului colectiv prevăzut în anexa nr. 1<sup>B</sup> la Ordinul ministrului finanțelor publice nr. 94/2006 cuprinde: nume, prenume, denumire contribuabil, domiciliu fiscal, denumire, număr și dată act administrativ fiscal.

Comunicarea cererilor și a tuturor actelor de procedură se va face din oficiu prin agenții procedurale, iar dacă nu este posibilă comunicarea, se va face prin poștă cu scrisoare recomandată cu dovadă de primire sau prin alte mijloace ce asigură transmiterea textului

actului și confirmarea primirii acestuia. De asemenea, Codul de procedură civilă prevede expres cazurile în care comunicarea se realizează prin afișare, iar atunci când reclamantul învederează că, deși a făcut tot ce i-a stat în putință nu a izbutit să afle domiciliul pârâtului, președintele instanței va dispune citarea acestuia prin publicitate (la ușa instanței, în Monitorul Oficial al României sau într-un ziar mai răspândit). Conform art. 95 alin. (4) din Codul de procedură civilă, dacă se dovedește citarea cu rea-credință, toate actele de procedură vor fi anulate, reclamantul putând fi sancționat cu amendă și obligat la despăgubiri, potrivit legii.

În plus, Curtea Constituțională a precizat că publicitatea prevăzută de art. 44 alin. (3) din Codul de procedură fiscală este una dintre modalitățile de comunicare a actelor administrative fiscale, reținând că în cauză comunicarea actului administrativ-fiscal de impunere nu s-a putut realiza datorită lipsei de la domiciliu a destinatarului, situație în care s-a procedat la comunicarea prin publicitate. Considerăm că această situație poate fi asimilată unui „motiv obiectiv” la care face referire Curtea Constituțională în Decizia sa nr. 667/2009, pentru a se putea recurge la comunicarea prin publicitate, ca „ultimă și subsidiară modalitate de comunicare a actelor administrative fiscale”.

Potrivit Legii nr. 677/2001, prelucrarea trebuie să se realizeze cu bună-credință și în conformitate cu dispozițiile legale în vigoare, iar datele personale prelucrate trebuie să fie adecvate, pertinente, neexcesive prin raportare la scopul prelucrării, exacte și actualizate, colectate în scopuri determinate, explicite și legitime și stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară atingerii scopurilor prelucrării.

Pentru încălcarea acestor dispoziții legale, Autoritatea de Supraveghere a dispus sancționarea contravențională a caselor de asigurări de sănătate reclamate pentru săvârșirea contravenției prevăzute de art. 32 din Legea nr. 677/2001 și, prin decizia președintelui, următoarele măsuri:

- a) ștergerea de pe pagina de Internet a datelor personale ale persoanelor fizice către care s-au emis decizii de impunere, prezente în toate listele cu contribuabili persoane fizice publicate pe site-urile de Internet aparținând caselor de asigurări, față de care nu s-au efectuat diligențele necesare pentru comunicarea actelor administrative fiscale în celelalte modalități reglementate de art. 44 alin. (2) lit. a), b) sau c) din Codul de procedură fiscală;

- b) respectarea caracterului legal, exact și actualizat al informațiilor utilizate la emiterea și ulterior, dacă este cazul, la publicitatea pe Internet a deciziilor de impunere față de aceste persoane.

Ulterior adoptării măsurilor de către Autoritatea de Supraveghere, Curtea Constituțională și-a reiterat soluțiile din jurisprudența anterioară. Astfel, prin Decizia nr. 536/2011, Curtea Constituțională a constatat că dispozițiile art. 44 alin. (3) din Ordonanța Guvernului nr. [92/2003](#) privind [Codul de procedură fiscală](#) sunt neconstituționale în măsura în care se interpretează în sensul că organul fiscal emitent poate să procedeze la comunicarea actului administrativ fiscal prin publicitate, cu înlăturarea nejustificată a ordinii de realizare a modalităților de comunicare prevăzute la art. 44 alin. (2) lit. a)-d) din aceeași ordonanță, subliniind totodată că atât instanțele judecătorești, cât și organele administrative trebuie să se conformeze deciziei Curții și să o aplice ca atare.

Deși toate casele de asigurări de sănătate sancționate au atacat în fața instanțelor judecătorești atât procesele-verbale, cât și deciziile Autorității de Supraveghere, au dat curs la scurt termen de la comunicarea deciziilor, măsurilor impuse de autoritate, astfel că în prezent nu mai sunt publicate pe paginile de Internet datele personale ale contribuabililor.

➤ **Prelucrarea datelor personale ale contribuabililor aflați în procedura de executare silită pentru neplata taxelor și impozitelor**

***FIȘĂ DE CAZ***

Printr-o petiție adresată instituției noastre, am fost sesizați în legătură cu o posibilă încălcare a dispozițiilor Legii nr. 677/2001, întrucât pe un link aparținând unei instituții publice (primărie) apărea un document pdf care cuprindea date (nume, prenume, codul numeric personal, adresa, rol, nr. titlu și data) ale anumitor persoane aflate în procedura de executare silită.

În urma investigației efectuate, a reieșit că pe site-ul instituției publice, în cadrul secțiunii “Impozite și taxe locale”, sunt disponibile listele anexate la anunțurile colective pentru comunicarea prin publicitate, emise de un serviciu public finanțe locale, în perioada 2008-2011. Listele publicate prin internet în perioada 2008-2010 conțineau, printre alte date, și CNP și suma restantă, date excluse din listele publicate prin internet în cursul anului 2010.

Nu au fost identificate liste anexate la anunțuri colective pentru comunicarea prin publicitate din 2007. Referitor la link-ul transmis de petent, din verificările efectuate s-a constatat că lista care conține date cu caracter personal ale unor persoane fizice către care au

fost emise somații de plată în 2007, putea fi accesată pe internet și la data efectuării investigației.

Conform declarațiilor reprezentanților operatorului, anunțurile colective pentru comunicarea prin publicitate și listele anexate acestora se întocmesc potrivit legislației fiscale în vigoare (Codul de procedură fiscală) și se comunică prin publicitate potrivit art. 44 alin. (3) din Codul de procedură fiscală, prin afișarea la sediu și pe pagina de internet a primăriei și produc efecte în termen de 15 zile de la data afișării anunțului.

De asemenea, s-a menționat că, ulterior, listele menționate mai sus sunt păstrate pe site-ul primăriei o perioadă de 5 ani, pentru îndeplinirea obligației de comunicare prin publicitate a actelor administrative fiscale, conform termenului de prescripție a creanțelor fiscale stabilit prin art. 131 din Codul de procedură fiscală.

Față de cele constatate, instituția publică a fost sancționată contravențional, deoarece a dezvăluit pe pagina de internet codul numeric personal și suma restantă a contribuabililor persoane fizice aflați în procedura de executare silită în perioada 2008 – 2010, date considerate a fi excesive.

Totodată, a fost sancționată contravențional și pentru că a dezvăluit date cu caracter personal fără a stabili o perioadă de timp corespunzătoare pentru realizarea scopului publicării prevăzut de Codul de procedură fiscală (comunicarea actului administrativ fiscal) și fără să fie făcută dovada actualizării acestor liste pe măsura stingerii creanțelor bugetare.

#### ➤ **Alte cazuri de dezvăluire a datelor personale pe Internet**

##### ***FIȘĂ DE CAZ***

Prin petițiile adresate autorității, o petiționară a reclamat postarea abuzivă a datelor sale personale pe o pagină de Internet, care nu aparține Poliției Române. De asemenea, petenta nu figura pe site-ul Poliției Române ca persoană urmărită.

Din verificările efectuate a rezultat că, în urma accesării adresei URL indicate, este posibilă vizualizarea datelor personale, inclusiv a fotografiei mai multor persoane fizice, printre care și ale petentei: nume, prenume, cod numeric personal, serie și număr act de identitate, data și locul nașterii, cetățenia, domiciliul (stradă, număr, localitate, județ), motivul căutării („mandat de arestare preventivă”), fapta săvârșită („delapidare și fals în înscrisuri sub semnătură privată”), data când a fost în urmărire generală (13.11.2003), imagine.

În urma investigației efectuate la deținătorul numelui de domeniu, nu a fost posibilă identificarea exactă a persoanei care a divulgat datele personale ale petiționarei la adresele de

Internet invocate. Cu toate acestea, în baza demersurilor întreprinse, deținătorul numelui de domeniu a dispus suspendarea acestor pagini de Internet care, în prezent, nu mai pot fi accesate.

### ***FIȘĂ DE CAZ***

Prin mai multe petiții, Autoritatea de Supraveghere a fost sesizată cu privire la publicarea fotocopiesi actului de identitate aparținând unui judecător într-un articol publicat pe site-ul unei publicații.

Anterior efectuării investigației, din verificările efectuate pe respectivul site s-a constatat că fotocopia cărții de identitate nu mai este cuprinsă în articolul sus menționat.

În urma investigației s-a constatat că fotocopia cărții de identitate a fost postată pe site cel mult o zi, fiind ștearsă din arhiva electronică a site-ului.

Din declarațiile reprezentantului operatorului a reieșit că fotocopia a fost publicată în scop jurnalistic, fără a se intenționa a se aduce atingere datelor personale ale petentei, scopul declarat fiind acela de a face legătura între domiciliul magistratului și acela al unei persoane prejudiciate, acest ultim scop constituind subiectul articolului publicat.

Operatorul a fost sancționat contravențional, deoarece a dezvăluit datele cu caracter personal ale unei persoane, inclusiv codul numeric personal, seria și numărul cărții de identitate, fără consimțământul acesteia, publicând în cadrul unui articol date care nu erau necesare pentru atingerea scopului jurnalistic al prelucrării.

### ***FIȘĂ DE CAZ***

Autoritatea pentru Protecția Datelor și Libertatea Informației din Germania a sesizat Autoritatea de supraveghere cu privire la plângerea unei persoane fizice împotriva a două companii înregistrate în România care au publicat pe site-urile lor, datele personale ale respectivei persoane fizice. Astfel, conform informațiilor transmise de Autoritatea pentru Protecția Datelor din Germania, a fost dezvăluită adresa privată a petiționarei, asociată cu serviciile medicale pe care le prestează, în condițiile în care nu a făcut publică adresa personală în niciun registru public, fapt pentru care dorește ștergerea datelor.

Autoritatea pentru Protecția Datelor din Germania nu a transmis către Autoritatea de supraveghere plângerea petentei și nu a făcut dovada că aceasta s-a adresat în scris celor două companii, conform prevederilor art. 14 și 15 din Legea nr. 677/2001.

În contextul în care cele două societăți nu figurau în Registrul de evidență a prelucrărilor de date cu caracter personal, s-au efectuat investigații, în urma cărora s-a

constatat că, la acel moment, nu mai erau disponibile pe Internet datele personale ale petentei, la niciuna din cele două adrese de internet folosite de acestea. Astfel, unul dintre operatori a decis să înceteze publicarea informațiilor despre cabinetele medicilor din Germania, iar celălalt a șters efectiv datele petentei din portalul public înregistrat în Germania. De altfel, a rezultat că orice persoană interesată poate solicita și obține ștergerea sau rectificarea informațiilor publicate la respective adresă de Internet, completând formularul electronic disponibil on-line prin accesarea numelui în cauză.

Ambele societăți au fost sancționate pentru săvârșirea unor fapte contravenționale prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

- **Prelucrarea datelor biometrice ale angajaților**

Autoritatea de Supraveghere a fost sesizată în 2011 în două cazuri cu privire la prelucrarea datelor biometrice ale angajaților, în scopul evidențierii timpului de lucru al acestora (pontaj).

Pentru verificarea celor semnalate, au fost efectuate mai multe investigații, în urma cărora au rezultat următoarele constatări:

- introducerea sistemelor electronice de pontare aveau la bază colectarea prin scanare a amprentei digitale, astfel că fiecare angajat era obligat ca la orice intrare/ieșire din incinta unității angajatoare să utilizeze aparatele de citire biometrică în vederea înregistrării timpului efectiv de lucru;
- decizia introducerii unui astfel de sistem, luată de conducerea instituțiilor publice în cauză (un spital de urgență și o primărie) a avut la bază intenția de a impune angajaților respectarea programului de lucru, întrucât, anterior, evidențierea timpului de lucru se realiza prin semnarea condicilor de prezență, situație în care unii angajați înregistrau întârzieri și absențe sau semnau în locul altor colegi;
- aducerea la cunoștința angajaților a deciziei de introducere a noului sistem de pontaj s-a realizat cu puțin timp înainte de punerea sa în funcțiune;
- doar într-unul dintre cele două cazuri investigate a fost solicitat și consimțământul scris al salariaților în acest sens; cu toate acestea, la data informării prealabile a angajaților, s-a adus la cunoștința acestora

consecințele refuzului de a accepta utilizarea sistemului de pontaj pe baza datelor biometrice, respectiv, neachitarea orelor care nu figurează în pontajul electronic, situație ce ar putea conduce până la desfacerea contractului de muncă;

- deși introducerea sistemului de pontaj electronic a avut ca scop renunțarea la sistemul anterior de evidențiere a prezenței angajaților în baza semnării condicilor de prezență, la ambele entități investigate s-a permis totuși pentru anumite persoane sau compartimente utilizarea în continuare a condicilor;
- obligația de notificare a prelucrării datelor personale (date biometrice) în scopul evidențierii timpului de lucru nu a fost îndeplinită în conformitate cu dispozițiile Legii nr. 677/2001 și ale Deciziei președintelui Autorității de supraveghere nr. 11/2009, respectiv, cu 30 de zile înainte de începerea prelucrării.

Pe baza acestor constatări, Autorității de supraveghere a dispus următoarele măsuri:

- sancționarea contravențională a entităților controlate, pentru săvârșirea contravențiilor prevăzute de art. 31 (nerespectarea obligațiilor de notificare), art. 32 (prelucrarea excesivă a datelor biometrice prin raportare la scopul prelucrării și netransmiterea răspunsului la plângerile adresate, în termenul legal) și art. 33 (neexecutarea copiilor de siguranță) din Legea nr. 677/2001;
- emiterea unei decizii de suspendare, iar ulterior de încetare a prelucrării datelor biometrice ale angajaților în scopul evidențierii timpului de lucru.

La emiterea deciziilor Autorității de Supraveghere, au fost avute în vedere următoarele considerente:

Atingerea scopului declarat al prelucrării datelor, respectiv, evidențierea timpului de lucru pentru angajați, se putea realiza și prin metode alternative, mai puțin intruzive decât prelucrarea datelor biometrice, fie prin intermediul condicilor de prezență, fie prin utilizarea altor funcții ale sistemului electronic implementat. De altfel, s-a constatat că prezența unora dintre angajați se evidențiază în continuare prin semnarea condicilor de prezență. O astfel de situație de utilizare a unor mijloace diferite pentru atingerea aceluiași scop poate conduce la apariția unor discriminări în aplicarea regulilor interne între angajații aceleiași entități. În plus, în cadrul relațiilor de muncă angajator-angajat, acordul scris exprimat de angajații uneia dintre cele două entități controlate nu ar putea fi asimilat unui consimțământ liber exprimat și în cunoștință de cauză pentru a legitima prelucrarea datelor biometrice în scopul evidențierii



timpului de lucru, cu atât mai mult date fiind consecințele refuzului de a accepta (neachitarea orelor care nu figurează în pontajul electronic, situație ce poate conduce până la desfacerea contractului de muncă). Ca atare, potrivit art. 4 alin. (1) lit. c) din Legea nr. 677/2001, modificată și completată, prelucrarea datelor biometrice ale angajaților este excesivă prin raportare la scopul în care acestea sunt colectate și ulterior prelucrate.

În urma investigațiilor, cele două entități au pus în executare dispozițiile deciziilor emise de Autoritatea de Supraveghere, privind încetarea prelucrării datelor biometrice ale angajaților în scopul evidențierii timpului de lucru.

- **Prelucrarea codului numeric personal**

Din analiza plângerilor și sesizărilor înregistrate la Autoritatea de Supraveghere, precum și urmare a investigațiilor efectuate pornind de la acestea, s-a constatat existența mai multor situații în care operatorii prelucrează date cu caracter personal având funcție de identificare, în special codul numeric personal, în lipsa consimțământului persoanelor vizate sau a unei dispoziții legale exprese.

Autoritatea de Supraveghere a fost sesizată prin mai multe cereri cu privire la faptul că un număr semnificativ de entități publice (primării, servicii de finanțe publice locale) care au implementat sisteme de plăți electronice în vederea informării on-line a datoriilor contribuabililor - persoane fizice și a achitării acestora prin mijloace de plată electronică, utilizează ca instrumente de identificare și autentificare CNP-ul plătitorului.

În aceste situații, în urma investigațiilor realizate, s-a apreciat că folosirea datelor personale, în special a codului numeric personal, contravine prevederilor art. 8 din Legea nr. 677/2001, întrucât consimțământul utilizatorului nu se bazează pe o informare prealabilă cu privire la scopul real al prelucrării datelor cu caracter personal și nici nu există o prevedere legală care să autorizeze expres această procedură.

Totodată, s-a constatat că autoritățile administrației publice centrale și locale care utilizează sisteme electronice de plată on-line cu autentificare pe bază de CNP nu asigură o securitate adecvată a prelucrărilor de date cu caracter personal, în conformitate cu Ordinul nr. 52/ 2002.

În urma acțiunilor de control întreprinse în aceste cazuri, pe lângă sancționarea operatorilor, s-a impus acestora să nu mai utilizeze ca modalități de identificare și

autentificare codul numeric personal, ci alte instrumente care să asigure accesul exclusiv al utilizatorilor la informațiile confidențiale care îi privesc.

#### FIȘĂ DE CAZ

O altă situație supusă atenției Autorității de Supraveghere este aceea a prelucrării datelor cu caracter personal din cartea de identitate pentru achiziționarea și reîncărcarea cartelelor prepaid de telefonie mobilă. În acest caz, în condițiile în care nu există dispoziții legale în acest sens, refuzul prezentării cărții de identitate determină limitarea accesului consumatorului persoană fizică la serviciul de telefonie mobilă.

În urma investigațiilor efectuate, s-a pus în vedere operatorilor să modifice modalitatea de achiziționare a cartelelor prepaid, în sensul că la cumpărarea acestora, solicitarea copiei cărții de identitate să aibă loc numai dacă se obține consimțământului scris al persoanei vizate. Cât privește, reîncărcarea cartelelor prepaid, autoritatea de supraveghere a dispus ca acest serviciu să nu mai fie condiționat de prezentarea cărții de identitate.

#### FIȘĂ DE CAZ

Autoritatea de Supraveghere a fost sesizată de mai mulți studenți cu privire la faptul că pe site-urile universităților la care sunt înscriși există un profil unde fiecare student are creat un cont personal. Prin accesarea paginii de profil, pe bază de cod numeric personal, se pot vizualiza datele cu caracter personal ale unui student și ale părinților acestuia (nume și prenume, nume după căsătorie, data nașterii, locul nașterii, sex, religie, serie, nr BI/CI, CNP, stare civilă și situație militară, precum și alte informații legate de școlarizare).

Din verificările efectuate, s-a constatat faptul că acest tip de profil aparține unei aplicații (University Management System -UMS) destinate instituțiilor de învățământ superior iar din punct de vedere tehnic, autentificarea se face prin introducerea CNP-ului și a datei de naștere.

Scopul prelucrării datelor cu caracter personal în cadrul acestei aplicații este ținerea unei evidențe centralizate a tuturor studenților, precum și a situației lor școlare și financiare, date care sunt solicitate de Ministerul Educației, Cercetării, Tineretului și Sportului în vederea realizării registrului matricol unic la nivel național.

Recomandarea Autorității de Supraveghere în aceste cazuri a fost aceea de a se găsi un alt cod unic de identificare, altul decât codul numeric personal, pentru accesarea profilului studentului.

## FIȘĂ DE CAZ

Codul numeric personal este prelucrat și în cadrul comerțului on-line, pentru întocmirea facturilor fiscale.

În urma investigațiilor realizate atât din oficiu cât și ca urmare a primirii unor plângeri, desfășurate la diverși operatori care prelucrează date cu caracter personal în domeniul comerțului on-line, s-a constatat că o parte dintre aceștia colectează și prelucrează codul numeric personal al clienților persoane fizice, telefonic și/sau on-line, invocând ca justificare dispozițiile Codului fiscal și cerințele Agenției Naționale de Administrare Fiscală, care ar impune ca obligatorie colectarea CNP-ului pentru întocmirea facturilor fiscale, începând cu 1 ianuarie 2007. Alți operatori nu colectează CNP-ul în scopul întocmirii facturilor fiscale, susținând că nu există dispoziții normative sau administrative în acest sens.

Față de aceste aspecte contradictorii, Autoritatea de Supraveghere a solicitat punctul de vedere al Ministerului Finanțelor Publice și al Agenției Naționale de Administrare Fiscală care a precizat că nu există dispoziții legale exprese privind colectarea codului numeric personal în scopul întocmirii facturilor fiscale.

În cazurile investigate în practică, în care operatorii prelucrează codul numeric personal, precum și alte date cu caracter personal având o funcție de identificare de aplicabilitate generală, fără a exista consimțământul persoanei vizate sau o dispoziție legală expresă, s-a urmărit, în principal, respectarea principiului caracterului adecvat, pertinent și neexcesiv al datelor cu caracter personal prin raportare la scopul în care sunt colectate și ulterior prelucrate, precum și existența unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

Având în vedere diversitatea cazurilor în care sunt prelucrate date cu caracter personal având o funcție de identificare de aplicabilitate generală, în special codul numeric personal, fără a exista o justificare temeinică a acestor prelucrări de date, s-a considerat necesar a se propune emiterea unei decizii privind condițiile prelucrării acestor categorii de date.

## CAPITOLUL AL IV-LEA

### ACTIVITATEA DE AVIZARE ȘI CONSULTARE

#### **Secțiunea 1 - Acte cu caracter normativ emise de Autoritatea de supraveghere**

În anul 2011, Autoritatea de supraveghere a adoptat **Decizia nr. 132/2011 privind condițiile prelucrării codului numeric personal și a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală.**

Această decizie a fost emisă în considerarea caracterul special al codului numeric personal, pentru a cărui protecție operatorul este obligat să ia măsuri tehnice și organizatorice destinate să îi asigure confidențialitatea și securitatea, în scopul de a preveni toate riscurile de dezvăluire sau acces neautorizat.

La adoptarea acestei reglementări s-au luat în considerare condițiile stabilite de dispozițiile art. 8 din Legea nr. 677/2001, conform cărora prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală se efectuează numai dacă persoana vizată și-a dat în mod expres consimțământul sau dacă prelucrarea este prevăzută în mod expres de o dispoziție legală. În același timp, doar Autoritatea de supraveghere este în măsură să stabilească și alte cazuri în care se poate efectua prelucrarea acestor date numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

În considerarea importanței codului numeric personal, s-a interzis fotocopierea oricăror documente care conțin această dată cu caracter personal, inclusiv a actelor de identitate, dacă nu există un temei legal expres sau acordul expres al persoanei implicate.

Adoptarea acestei reglementări s-a fundamentat pe dispozițiile Directivei 95/46/CE, potrivit cărora se permite statelor membre, independent de normele generale, să prevadă condiții de prelucrare speciale pentru sectoare specifice, fiind împuternicite să asigure punerea în aplicare a protecției persoanei și prin acte cu putere de lege în anumite sectoare, completând sau clarificând cu norme speciale principiile cu privire la protecția drepturilor și libertăților persoanelor, în special a dreptului la viață privată, în ceea ce privește prelucrarea datelor cu caracter personal.

## **Secțiunea a 2-a – Avizarea actelor normative**

În temeiul art. 21 alin. (3) lit. h) din Legea nr. 677/2001, Autoritatea de Supraveghere a emis o serie de avize asupra actelor normative elaborate de diverse instituții și autorități publice care se refereau la aspecte privind prelucrarea datelor cu caracter personal.

În anul 2011, Autoritatea de Supraveghere a emis o serie de avize asupra unui număr de **58** de proiecte de acte normative.

Dintre cele mai importante, prezentăm următoarele:

### ***❖ Proiectul Ordonanței de urgență a Guvernului pentru modificarea și completarea Ordonanței Guvernului nr. 37/2007 privind efectuarea recensământului populației și al locuințelor din România în anul 2011***

Cu privire la acest proiect, Autoritatea de Supraveghere a efectuat observații cu privire la obligația obținerii consimțământului expres al persoanelor intervievate sau al reprezentanților legali ai acestora, precum și cu privire la obligația informării persoanelor vizate în conformitate cu art. 12 din Legea nr. 677/2001.

În acest context, Autoritatea de Supraveghere a recomandat să se aibă în vedere inserarea în cuprinsul formularului de înregistrare a unei note de informare în care să se indice identitatea operatorului, scopul colectării datelor, destinatarii acestora, existența dreptului de acces, intervenție și opoziție a persoanelor vizate, condițiile exercitării acestora, precum și asumarea respectării obligației de confidențialitate și securitate a datelor.

Alături de aceste aspecte, s-a considerat necesară și menționarea faptului că informațiile privind etnia, religia și limba maternă se furnizează la consimțământul persoanei vizate. În același timp, Autoritatea de Supraveghere a subliniat că se poate recurge la marcarea datelor respective și inserarea unor note de subsol cu explicațiile aferente.

Deși recomandările privind consimțământul au fost preluate de inițiator, cele referitoare la obligația de informare adecvată și necesitatea furnizării tuturor datelor nu s-au concretizat prin inserarea în formularele-tip de colectare a datelor personale pentru recensământ a notelor de informare respective.

**❖ *Proiectul Hotărârii Guvernului pentru modificarea și completarea Hotărârii Guvernului nr. 1502/2009 privind organizarea și desfășurarea recensământului populației și al locuințelor din România în anul 2011***

Referitor la propunerile privind furnizarea de informații despre persoanele care lipsesc temporar, de către alte persoane, Autoritatea de Supraveghere a subliniat faptul că Legea nr. 677/2001 stabilește principiile potrivit cărora datele trebuie să fie adecvate și pertinente, iar operatorul are obligația de a înregistra date exacte și, dacă este cazul, actualizate; în acest scop s-a informat cu privire la obligația de a se lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate și pentru care vor fi ulterior prelucrate, să fie șterse sau rectificate.

În consecință, pentru respectarea acestor obligații trebuie identificate modalități de corectare sau rectificare a informațiilor înregistrate și care au fost furnizate de alte persoane decât persoana vizată.

De asemenea, s-a apreciat ca necesară adăugarea de mențiuni privind obligația de asigurare a securității și confidențialității informațiilor colectate și înregistrate prin intermediul instrumentelor de recensământ.

Totodată, s-a considerat necesară specificarea unor dispoziții în proiect privind instruirea personalului de recensământ și asupra regulilor de prelucrare a datelor cu caracter personal, în special în ceea ce privește măsurile de securitate și confidențialitate a acestora, pe care operatorul trebuie să le ia și să le respecte, în conformitate cu art. 19 și 20 din Legea nr. 677/2001, modificată și completată.

Recomandările Autorității de Supraveghere nu au fost preluate, Institutul Național de Statistică susținând că s-ar încălca dispozițiile Legii nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, cu modificările și completările ulterioare, în sensul că s-ar realiza paralelisme de reglementare, întrucât toate cerințele sunt prevăzute în Ordonanța de urgență a Guvernului pentru modificarea și completarea Ordonanței Guvernului nr. 37/2007 privind efectuarea recensământului populației și al locuințelor din România în anul 2011.

**❖ *Proiectul de Lege privind exercitarea prin corespondență a dreptului de vot de către alegătorii români cu domiciliul sau reședința în străinătate***

Referitor la proiectul actului normativ susmenționat, Autoritatea de Supraveghere a apreciat că modalitatea de exercitare a votului prin corespondență nu este de natură să asigure

respectarea cerințelor legislației din domeniul protecției datelor cu caracter personal, în special cele cu privire securitatea datelor.

În acest context, s-a subliniat faptul că operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Totodată, s-a considerat că acest sistem va întâmpina dificultăți în a asigura că doar persoanele autorizate vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor legale, iar în eventualitatea în care datele vor deveni disponibile unor terți, va fi dificilă menținerea standardului de confidențialitate și securitate adecvat pentru protejarea lor și, în consecință, drepturile fundamentale ale alegătorilor în cauză vor fi afectate.

Din considerentele prezentate mai sus, Autoritatea de Supraveghere și-a menținut constant opinia potrivit căreia sistemul de vot prin corespondență nu conferă garanțiile necesare protejării drepturilor alegătorilor în calitate de persoane vizate ale căror date sunt prelucrate de către autoritățile și instituțiile publice implicate în activitatea de asigurare a exercitării prin corespondență a dreptului de vot.

**❖ *Proiectul Legii privind reținerea datelor generate sau prelucrate, de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații***

Față de conținutul acestui document, Autoritatea de Supraveghere a efectuat mai multe observații, astfel:

Referitor la mențiunile privind autoritățile competente să solicite datele reținute de furnizori, s-a apreciat că este necesară identificarea concretă a acestora, pentru evitarea oricăror abuzuri în ceea ce privește drepturile persoanelor vizate, aceasta constituind o garanție suplimentară în acest sens.

Cât privește domeniul siguranței naționale și trimiterile generice la dispozițiile legale speciale în materie (care, de altfel, nu sunt în acord cu Convenția pentru protecția drepturilor și libertăților fundamentale), alături de lipsa unei proceduri specifice de solicitare a datelor reținute, Autoritatea de Supraveghere a apreciat că aceste elemente pot conduce la încălcări grave ale dreptului fundamental la viață privată.

De asemenea, s-a apreciat că sintagma „datelor necesare pentru identificarea abonatului” denotă ambiguitate și nu este în acord cu Decizia Curții Constituționale nr. 1258 din 8 octombrie 2009.

Adăugarea a o serie de infracțiuni în textul proiectului de lege, presupune extinderea câmpului de aplicare a acestei legi la alte infracțiuni decât cele grave, aspect ce încalcă Directiva 2006/24/CE care se referă doar la „crime grave”.

În privința eliminării situației de excepție a forței majore, Autoritatea de Supraveghere a subliniat faptul că proiectul actului normativ trebuie să ia în considerare diferitele ipoteze ce se pot ivi în activitatea de aplicare a acestuia, astfel încât să se prevină apariția ulterioară a unor situații nereglementate.

Referitor la eliminarea procedurii de solicitare a datelor reținute, în opinia Autorității aceasta conduce la crearea unor situații neclare, astfel că menținerea unei proceduri speciale de solicitare și comunicare a datelor reținute se impune, cu atât mai mult cu cât, anumite articole din proiect stabilesc ipotezele în care se aplică Codul de procedură penală și cele din legile speciale în materie.

Totodată, lipsa unui cadru legal de stabilire a conținutului autorizației, precum și de arhivare și distrugere a datelor va conduce la ambiguități în activitatea de acces la datele reținute și apariția de abuzuri în respectarea drepturilor fundamentale ale persoanelor vizate, pentru aceleași argumente prezentate la început.

În plus, Autoritatea de Supraveghere a subliniat că cele două tipuri de operațiuni sunt distincte: pe de o parte, interceptarea și înregistrarea convorbirilor telefonice sau a altor comunicări care presupune înregistrarea a însuși conținutului acestora (aspect interzis în mod expres de proiectul legii), operațiuni autorizate în baza Codului de procedură penală, iar pe de altă parte, reținerea unor date de trafic și localizare, aferente unor comunicări prin mijloace electronice, autorizată în baza proiectului de lege.

Prin urmare și autorizarea accesului la date se impune a fi reglementată distinct și expres și nu prin trimiteri generice la Codul de procedură penală.

În consecință, Autoritatea de Supraveghere a apreciat că se impune instituirea unei proceduri de solicitare și comunicare a datelor reținute, chiar stabilirea de garanții suplimentare față de cele anterior prevăzute în textul Legii nr. 298/2008, în cadrul actualului proiect de lege.

În plus, Autoritatea de supraveghere a propus adăugarea, ca autoritate competentă să monitorizeze aplicarea prevederilor legii, și a Autorității Naționale pentru Comunicații, potrivit competențelor legale specifice ale acesteia.



În consecință, modificările propuse prin proiect au fost apreciate că erau de natură a aduce o gravă atingere dreptului la viață privată și protecției datelor cu caracter personal, intrând în contradicție cu unele prevederi ale Directivei 2006/24/CE, cu decizii ale CEDO, precum și ale Curții Constituționale, astfel că Autoritatea de Supraveghere nu a putut exprima un aviz favorabil față de respectiva redactare a textului proiectului Legii privind reținerea datelor generate sau prelucrate, de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații.

În plus, la nivelul Comisiei Europene a fost demarat un proces de evaluare a Directivei 2006/24/CE, ale cărui rezultate au fost publicate sub forma unui raport adresat Parlamentului European și Consiliului. Una dintre principalele concluzii ale raportului a fost că reținerea datelor reprezintă o limitare semnificativă a dreptului la viață privată, motiv pentru care Comisia Europeană va avea în vedere instituirea unor reglementări mai stricte în ceea ce privește stocarea, accesarea și utilizarea datelor reținute.

#### *❖ Proiectul Hotărârii Guvernului privind întocmirea și completarea registrului de evidență a salariaților (REVISAL)*

Autoritatea de Supraveghere a **avizat negativ** propunerea susmenționată, întrucât s-a considerat că aduce atingere gravă vieții private a persoanelor fizice, venind în contradicție cu principiile statuate de Convenția Consiliului Europei nr. 108/1981 și cu prevederile Directivei 95/46/CE a Parlamentului European și a Consiliului.

În acest sens, Autoritatea de Supraveghere a considerat că este necesară definirea rolului și responsabilităților tuturor entităților implicate în procesul de întocmire și completare a registrului salariaților, în vederea stabilirii în mod clar a calității acestora de operatori sau împuterniciți, potrivit definițiilor date de Legea nr. 677/2001.

S-a subliniat că este necesară luarea în considerare a principiilor de protecție a datelor încă de la crearea sistemelor și aplicațiilor informatice utilizate, în special prin stabilirea persoanelor autorizate, după caz a autorităților și instituțiilor publice, care vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate. **|**

Având în vedere prevederile actului normativ susmenționat și a investigației efectuate de reprezentanții Autorității de Supraveghere la sediul Ministerului Muncii, Familiei și Protecției Sociale, președintele Autorității a emis o **recomandare** prin care solicita Ministerului Muncii, Familiei și Protecției Sociale eliminarea obligației prestatorilor de a

prezenta inspectoratelor teritoriale de munca dovada înregistrării ca operator de date cu caracter personal.

Recomandarea președintelui Autorității de Supraveghere a fost însușită de conducerea Ministerului Muncii, Familiei și Protecției Sociale care, la data de 23 decembrie 2011, a publicat în Monitorul Oficial nr. 920, Ordinul nr. 2822/2011 prin care asigură intrarea în legalitate sub aspectul prelucrării datelor cu caracter personal.

În consecință, subliniem faptul că angajatorilor și prestatorilor de servicii nu le revine obligația de a notifica Autoritatea de Supraveghere pentru operațiunile pe care le efectuează asupra datelor cu caracter personal în vederea transmiterii și completării Registrului general de evidență a salariaților.

#### *❖ Cinci proiecte de legi transmise de Ministerul Justiției*

##### *I. Legea pentru punerea în aplicare a Legii nr. 134/2010 privind Codul de procedură civilă*

Cu privire la acest proiect, Autoritatea de Supraveghere a apreciat că sunt necesare precizări exprese privind faptul că pentru stabilirea modului concret de acces la bazele de date se încheie protocoale între autoritățile solicitante și organele administrației de stat, cu respectarea dispozițiilor legale privind protecția datelor cu caracter personal, în special a celor referitoare la confidențialitatea și securitatea prelucrărilor.

În acest context, Autoritatea de Supraveghere a subliniat că accesul direct la bazele de date prezintă un nou risc, atât prin faptul că datele personale vor fi dezvăluite unui număr mare de destinatari, dar și prin aceea că va oferi noi posibilități pentru eventuala utilizare incorectă a acestora. Astfel, aceste sisteme trebuie să asigure faptul că doar persoanele autorizate vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor legale. Totodată, punctele de acces multiple dintr-o rețea deschisă, precum Internetul, cresc riscul interceptării datelor personale iar odată ce acestea devin disponibile unui număr mare de persoane, va deveni dificilă menținerea standardului de confidențialitate adecvat pentru protejarea datelor.

Referitor la modalitățile de încunoștințarea a părților, aceste măsuri trebuie să asigure, potrivit stadiului tehnicii utilizate în procesul de prelucrare și de costuri, un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate.

Astfel, în privința alegerii modalității de transmitere a informațiilor prin poștă electronică, Autoritatea de Supraveghere a subliniat că aceasta presupune expunerea

comunicării la o serie de riscuri, cum ar fi interceptarea, modificarea, pierderea, distrugerea, întârzieri în primirea datelor, etc., motiv pentru care acest tip de comunicare necesită luarea de măsuri care să garanteze securitatea informațiilor comunicate, pentru evitarea anumitor riscuri care ar putea avea un impact considerabil asupra vieții private a cetățenilor.

În acest sens, s-a considerat necesară completarea acestor dispoziții cu mențiuni exprese privind obligația luării și respectării măsurilor tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal, de către toți actorii implicați în implementarea acestui tip de comunicare.

În ceea ce privește modalitatea de obținere a informațiilor de către executorul judecătoresc, acestea nu sunt specificate expres în proiectul de lege, fiind lăsate la aprecierea executorului judecătoresc, în funcție de necesitatea realizării executării silite. În acest context, precizăm că dispozițiile art. 4 din Legea nr. 677/2001, modificată și completată stabilesc, ca principiu, faptul că datele trebuie să fie adecvate, pertinente și neexcesive în raport cu scopul prelucrării.

Având în vedere dispozițiile legale de mai sus și întrucât entitățile solicitate a dezvălui datele au obligația, prin lege, de a le furniza, pentru garantarea protecției datelor personale ale justițiabililor, autoritatea a apreciat ca necesară stabilirea și a obligației executorului judecătoresc de a respecta caracterul adecvat, pertinent și neexcesiv al datelor cu caracter personal solicitate și de a le utiliza numai în scopurile pentru care au fost obținute, precum și de a lua măsurile tehnice și organizatorice necesare pentru asigurarea confidențialității și securității datelor.

## ***II. Legea privind organizarea și funcționarea sistemului de probațiune***

Autoritatea de Supraveghere a apreciat că toate regulile privind protecția datelor cu caracter personal se impun a fi respectate, cu atât mai mult cu cât unele dintre datele colectate sunt de natură sensibilă (starea de sănătate, infracțiunile săvârșite, pedepsele care se execută, măsuri educative dispuse etc.).

## ***III. Legea pentru punerea în aplicare a codului de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale***

Dispozițiile privind modificarea și completarea Legii nr. 304/2004 privind organizarea judiciară, republicată, nu conțin referiri la termenile de stocare ale înregistrărilor prin mijloace tehnice video sau audio ale ședințelor de judecată, scopul acestor înregistrări și nici la

modalitatea de asigurare a drepturilor persoanelor vizate – participanții la proces – în special cel de acces la informațiile astfel înregistrate.

În acest context, menționăm că dispozițiile legale referitoare la informarea persoanei vizate (art. 12), exercitarea dreptului de acces la propriile date (art. 13), comunicarea măsurilor luate în cazul solicitărilor venite din partea persoanei vizate de a-și exercita dreptul de intervenție (art. 14 alin. 3), precum și dreptul de opoziție la prelucrarea datelor (art. 15), nu se aplică în cazul activităților de prevenire, cercetare și reprimare a infracțiunilor și de menținere a ordinii publice, precum și al altor activități desfășurate în domeniul dreptului penal, dacă prin aplicarea acestora este prejudiciată eficiența acțiunii sau obiectivul urmărit în îndeplinirea atribuțiilor legale ale autorității publice.

Cu toate acestea, drepturile de mai sus trebuie asigurate, odată ce situațiile care au justificat luarea măsurilor respective au încetat.

Prin urmare, Autoritatea de Supraveghere a considerat că se impune completarea articolului cu dispoziții care să reglementeze cele expuse mai sus.

Referitor la textele care reglementează tehnicile speciale de supraveghere, pentru aceleași rațiuni prezentate mai sus, drepturile persoanelor vizate – persoanele ale căror date sunt prelucrate, indiferent de calitatea acestora – trebuie asigurate. Astfel, la fiecare dintre aceste tehnici de supraveghere, Autoritatea de Supraveghere a apreciat că trebuie stabilite condițiile exercitării drepturilor persoanelor vizate. Or, doar la „Conservarea datelor informatice și a datelor privind traficul informațional” se prevede informarea persoanelor față de care se efectuează urmărirea penală.

Mai mult, potrivit reglementării propuse, măsurile dispuse de procuror nu sunt autorizate de judecătorul de drepturi și libertăți - măsura se dispune de procuror din oficiu sau la cererea organului de cercetare penală - ca în actuala formulare a Legii nr. 135/2010, creându-se un dezechilibru între protecția dreptului fundamental la viață intimă, familială și privată al persoanei vizate și interesul legitim al operatorului care ar putea fi lezat.

De altfel, art. 26 din Constituție obligă autoritățile publice la respectarea și ocrotirea vieții intime, familiale și private. Astfel, garantarea, prin lege, a luării unor măsuri temeinic justificate de intruziune în viața privată nu face decât să transpună condițiile stabilite de art. 53 din Legea fundamentală, mai ales aceea de a nu aduce atingere existenței dreptului sau a libertății.

În plus, obiectul art. 8 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale este de a proteja individul împotriva ingerințelor arbitrare din partea autorităților publice, iar prin aceasta obligă statul să se abțină de la astfel de ingerințe.

În consecință, Autoritatea de Supraveghere a apreciat că aceste dispoziții din proiectul legii se impun a fi modificate și completate în sensul de mai sus.

#### ***IV. Legea privind executarea pedepselor și a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal***

Pentru claritatea normei, Autoritatea de Supraveghere a apreciat că sunt necesare mențiuni privind înțelesul sintagmei de supraveghere electronică la distanță și mijloacele de asigurarea a acestei supravegheri

Pentru o corectă și completă informare, s-a apreciat necesară completarea, în textul proiectului, cu nominalizarea și a Legii nr. 677/2001, având în vedere că în textul proiectului de lege se face referire și la protecția datelor cu caracter personal ale persoanelor condamnate (persoane vizate), față de care penitenciarul are calitatea de operator de date cu caracter personal.

La capitolul intitulat „Documente întocmite de administrația penitenciarului”, întrucât acestea conțin date cu caracter personal, Autoritatea de Supraveghere a considerat că sunt necesare și mențiuni cu privire la faptul că prelucrarea datelor cu caracter personal din dosarul individual al persoanei condamnate și registrele privind persoanele condamnate se realizează cu respectarea Legii nr. 677/2001, modificată și completată.

#### ***V. Legea privind executarea pedepselor, măsurilor educative și a altor măsuri dispuse de organele judiciare în cursul procesului penal, neprivative de libertate:***

Referitor la textele din proiect care reglementează respectarea confidențialității datelor cu caracter personal, Autoritatea de Supraveghere a apreciat că se impune respectarea întregului regim de protecție a datelor cu caracter personal, nu doar cel al confidențialității datelor.

#### ***❖ Proiectul Ordonanței de urgență pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice***

Față de conținutul actului normativ transmis, Autoritatea de Supraveghere a efectuat observații în legătură cu stabilirea obligației notificării de către furnizorii de servicii de comunicații electronice, precum și cu privire la stabilirea modalității notificării prin raportare la prevederile art. 4 din Directiva 2002/58/CE, în forma modificată de Directiva 2009/136/CE,

în sensul că mai multe autorități sunt competente în auditarea măsurilor adoptate de furnizori și emiterea de recomandări.

În consecință, toate aspectele legate de modalitatea de notificare se impun a fi stabilite prin participarea tuturor părților implicate (Autoritatea Națională de Comunicații și Ministerul Comunicațiilor și Societății Informaționale), nefiind pusă în discuție doar responsabilitatea Autorității de Supraveghere.

De asemenea, atribuțiile în ceea ce privește măsurile de securitate în domeniul protecției datelor cu caracter personal sunt partajate între cel puțin două autorități naționale, iar pentru exercitarea atribuțiilor privind asigurarea securității serviciilor de telecomunicații trebuie desemnată ca autoritate responsabilă Autoritatea Națională de Comunicații, raportat la atribuțiile legale ale acesteia.

În consecință, Autoritatea de Supraveghere a apreciat că responsabilitățile stabilite în proiectul ordonanței trebuie îndeplinite și de Autoritatea Națională pentru Administrare și Reglementare în Comunicații, iar Autoritatea de Supraveghere să preia competențe numai în ceea ce privește analizarea atingerilor aduse datelor cu caracter personal sau vieții private a unei persoane fizice.

Prin urmare, modificările propuse prin proiectul ordonanței nu sunt în acord cu prevederile Directivei 2002/58/CE, modificate prin Directiva 2009/136/CE, fiind de natură a institui un regim prin care Autorității de Supraveghere i se impune să îndeplinească atribuții contrare menirii sale de apărare a dreptului la viață privată, ajungându-se în situații opuse, în care s-ar putea chiar diminua garanțiile de protecție a datelor personale și, implicit, a drepturilor persoanelor vizate.

Referitor la modalitatea de obținere a consimțământului prin intermediul internetului sau altor tehnologii similare, Autoritatea de Supraveghere a susținut în mod constant, faptul că trebuie să se asigure atât obținerea expresă și neechivocă a consimțământului persoanei vizate, dar și furnizarea de garanții adecvate pentru respectarea drepturilor persoanelor vizate. În această situație nu există siguranța identității abonatului sau utilizatorului, iar în cazul în care se impune, nu se poate furniza cu certitudine proba obținerii consimțământului.

Mai mult, propunerea urmărește reglementarea obținerii consimțământului în ceea ce privește stocarea sau accesul la informația stocată în echipamentul terminal al abonatului sau utilizatorului, motiv pentru care apreciem că se impune certitudinea identificării acestuia.

În ceea ce privește modalitatea obținerii opt-out a consimțământului, urmare a trecerii termenului de 45 de zile lucrătoare în care abonatul își exprimă consimțământul, Autoritatea de Supraveghere a apreciat că acesta se poate aplica numai în privința telefoniei fixe, telefonul

mobil, prin însăși caracteristica sa, având o conotație mult mai personală, care poate conduce în mare măsură la afectarea vieții private. Prin urmare, sunt necesare mențiuni cu privire la exceptarea telefoniei mobile de la această modalitate de obținere a consimțământului și păstrarea numai a modalității opt-in.

În ceea ce privește regimul sancționator, Autoritatea de Supraveghere a apreciat că acesta se impune a fi modificat în acord cu partajarea atribuțiilor prevăzute la articolele anterioare ale proiectului, între autoritățile naționale competente. Mai mult, competențele Autorității de supraveghere pot fi exercitate numai pentru protejarea drepturilor persoanelor fizice, nu și ale celor juridice.

În aceste condiții, Autoritatea de Supraveghere nu a putut exprima un aviz favorabil proiectului Ordonanței de urgență pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

**❖ *Proiectul Legii privind colectarea datelor personale ale utilizatorilor serviciilor de tip Prepay***

În urma analizării proiectului actului normativ supus avizului, Autoritatea de Supraveghere a concluzionat faptul că, astfel cum sunt formulate anumite prevederi, se aduce o atingere gravă vieții private a persoanelor fizice, venind în contradicție cu principiile statuate de legislația națională și comunitară.

Impunerea obligației de a prezenta un act de identitate utilizatorilor de servicii de comunicații electronice, persoane vizate, potrivit Legii nr. 677/2001, constituie o restrângere a drepturilor acestora, prin condiționarea exercitării de acte/fapte de comerț, nu numai de dovedirea identității persoanelor în cauză, ci și de condiționarea prestării unor servicii de comunicații de prelucrarea datelor cu caracter personal conținute de actul de identitate.

Autoritatea de supraveghere a apreciat că se aduce atingere și libertății consumatorului de a lua decizii la achiziționarea de servicii de comunicații prepay, dat fiind că, prin obligarea prezentării actului de identitate, poate fi influențată opțiunea consumatorului cu privire la achiziționarea sau nu a serviciului respectiv.

Față de cele de mai sus Autoritatea de Supraveghere a ***avizat negativ*** propunerea susmenționată având în vedere faptul că, prin prelucrarea tuturor datelor cu caracter personal conținute de actul de identitate al unei persoane vizate de către furnizorii de servicii de comunicații electronice de tip prepay, sunt grav încălcate principiile proporționalității și stocării datelor prevăzute de Directiva 95/46/CE și de Legea nr. 677/2001.

### ❖ *Propunerea legislativă privind comunicațiile electronice*

Autoritatea de Supraveghere a apreciat că la elaborarea proiectului de act normativ care transpune, printre altele, Directiva 2009/136/CE și Directiva 2009/140/CE, era necesar să se preia și prevederile referitoare la protecția datelor cu caracter personal din aceste acte normative comunitare, cu precădere cele din Directiva 2009/136/CE, așa cum s-a procedat și în cazul elaborării altor acte normative aplicabile în sectorul comunicațiilor electronice.

Activitățile desfășurate în contextul comunicațiilor electronice presupun efectuarea de operațiuni de colectare și prelucrare a unor categorii diferite de date cu caracter personal. Acest fapt are implicații directe asupra drepturilor fundamentale ale persoanelor fizice și poate conduce la atingeri aduse dreptului la viață privată a cetățenilor, în ceea ce privește protecția datelor lor cu caracter personal.

De aceea, Autoritatea de Supraveghere a considerat că este necesară definirea clară a rolului și responsabilităților tuturor entităților din sectorul public și privat implicate în procesul de implementare a actului normativ privind comunicațiile electronice, în vederea stabilirii calității acestora de operatori sau împuterniciți, potrivit definițiilor date de Legea nr. 677/2001.

S-a subliniat că este necesară luarea în considerare a principiilor de protecție a datelor încă de la crearea sistemelor, bazelor de date, registrelor abonaților, inclusiv a aplicațiilor informatice utilizate, în special prin stabilirea persoanelor autorizate, după caz a autorităților și instituțiilor publice sau private, care vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate.

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

În plus, s-a atras atenția cu privire la nerespectarea prevederilor Legii nr. 677/2001 privind consimțământul dat pentru prelucrarea datelor cu caracter personal, în contextul stabilirii prin propunerea legislativă privind comunicațiile electronice a obligațiilor



furnizorilor de servicii de comunicații electronice destinate publicului pe care le au față de abonații la serviciile de telefonie destinate publicului la momentul dezvoltării datelor acestora furnizorilor de servicii de informații privind abonații sau de registre ale abonaților, desemnați conform normelor legale în vigoare de către Autoritatea Națională de Comunicații.

**❖ *Propunerea legislativă privind modificarea și completarea unor acte normative în domeniul securității naționale***

Autoritatea de Supraveghere a avizat proiectul susmenționat, efectuând observații cu privire la necesitatea explicitării situațiilor deosebite care impun înlăturarea unor pericole iminente pentru securitatea națională, pentru evitarea situațiilor ce ar duce la încălcarea abuzivă a drepturilor și libertăților cetățenilor, inclusiv ale celor privind viața intimă și privată.

Referitor la exercitarea drepturilor persoanelor vizate, în special dreptul de acces și cel de intervenție, s-a considerat că articolele din propunerea legislativă referitoare la „Reguli speciale privind protecția datelor cu caracter personal” trebuie să fie în acord cu prevederile Legii nr. 677/2001, respectiv ale Directivei 95/46/CE a Parlamentului European și a Consiliului pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

S-a subliniat, de asemenea, necesitatea luării în considerare a principiilor de protecție a datelor în cadrul efectuării de prelucrări de date în domeniul securității naționale, inclusiv în cazul creării de sisteme, baze de date și chiar a aplicațiilor informatice utilizate, în special prin stabilirea persoanelor autorizate, după caz a autorităților și instituțiilor publice din acest domeniu, care vor avea acces la date, în scopuri legitime și cu respectarea tuturor garanțiilor adecvate pentru respectarea drepturilor persoanelor vizate, precum și necesitatea stabilirii de termene concrete în cazul realizării operațiunilor de stocare, respectiv de arhivare a datelor.

S-a precizat că operatorii de date ce activează în domeniul securității naționale au obligația de a aplica măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvoltării sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmiterea de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală, având în vedere dispozițiile art. 17 alin. (1) din Directiva 95/46/EC a Parlamentului European și prevederile art. 20 din Legea nr. 677/2001.

**❖ Avizarea proiectele dispozițiilor adoptate de Inspectoratul General al  
Poliției Române și mai multe inspectorate județene de poliție**

Potrivit art. 14 din Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, operatorii din acest sector de activitate au obligația întocmirii și supunerii spre avizare Autorității naționale de supraveghere a unor reguli privind: termenele de stocare a datelor pe care le prelucrează, intervalul de timp pentru verificarea periodică a datelor pentru ca acestea să fie exacte, actuale și complete, precum și de ștergere a acestora.

***1. Proiectul Dispoziției Inspectorului General al Poliției Române pentru stabilirea  
regulilor prevăzute de art. 14 din Legea nr. 238/2009 privind reglementarea  
prelucrării datelor cu caracter personal de către structurile/unitățile  
Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și  
combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice***

Urmare a examinării conținutului proiectului dispoziției de mai sus, Autoritatea de Supraveghere a efectuat mai multe observații care au vizat mai ales corelarea unor texte și reanalizarea unor termene de stocare a datelor personale în sensul reducerii acestora.

Observațiile Autorității au fost luate în totalitate în considerare, astfel încât proiectul dispoziției a primit aviz favorabil.

***2. Proiectele dispozițiilor unor Inspectorate Județene de Poliție***

Autoritatea de Supraveghere nu a putut emite un aviz favorabil pentru regulile stabilite de inspectoratele județene de poliție, în temeiul art. 14 din Legea nr. 238/2009, deoarece nu se realiza o aplicare unitară a dispozițiilor Legii nr. 238/2009.

Astfel, Autoritatea de Supraveghere a solicitat informații suplimentare cu privire la necesitatea existenței unor baze de date distincte față de cele gestionate de către Inspectoratul General al Poliției Române.

De asemenea, au fost efectuate observații pentru claritatea textelor referitoare la stocarea datelor, ștergerea automată a acestora, analizarea și identificarea unor situații derogatorii, în care datele pot fi șterse înainte de împlinirea termenelor stabilite, în cazul în care acestea nu mai sunt necesare realizării scopurilor.

În acest context, pentru o aplicare unitară a dispozițiilor Legii nr. 238/2009, în special asupra stabilirii regulilor prevăzute de art. 14 din această lege, Autoritatea de Supraveghere a recomandat și consultarea Inspectoratului General al Poliției Române.

***❖ Proiectul Dispoziției pentru stabilirea procedurilor de protecție a datelor cu caracter personal la nivelul Oficiului Român pentru Imigrări***

Asupra proiectului dispoziției de mai sus, Autoritatea de Supraveghere a efectuat, în principal, observații cu privire la precizarea modalității în care au loc verificările, respectiv prin sondaj sau asupra tuturor datelor.

De asemenea, în proiect s-au făcut referiri la Centrul de Comunicații și Informatică și direcțiile centrale, dar rolul și atribuțiile acestora în prelucrarea datelor cu caracter personal nu au fost precizate în cuprinsul proiectului dispoziției, sens în care s-au solicitat clarificări ale textului respectiv.

Totodată, s-au efectuat observații privind utilizarea termenului „permanent”, în sensul că este necesară stabilirea sau definirea unor perioade de stocare în concordanță cu prevederile legale de mai sus, precum și a condițiilor de stocare în situația în care datele mai sunt păstrate și după îndeplinirea scopului, prin inserarea unor alineate noi.

Pentru aceleași rațiuni de mai sus, prelungirea perioadei de păstrare a datelor nu specifică motivele și termenul maxim pentru care se poate propune aceasta sau dacă nota (raportul) trebuie să fie motivată.

În același timp, s-au solicitat precizări cu privire la temeiurile pe baza cărora au fost stabilite unele termene de 30 de ani.

În consecință, față de forma prezentată a textului proiectului Dispoziției pentru stabilirea procedurilor de protecție a datelor cu caracter personal la nivelul Oficiului Român pentru Imigrări, Autoritatea de Supraveghere nu a putut emite un aviz favorabil, proiectul rămânând în lucru la inițiator.

***Secțiunea a 3 - a Opinii emise în diverse chestiuni privind protecția datelor***

În anul 2011, atât persoanele vizate, cât și operatorii au solicitat un număr de **1213** de opinii cu privire la condițiile legale de prelucrare a datelor cu caracter personal.

În continuare, prezentăm unele dintre cele mai semnificative situații supuse analizei Autorității de supraveghere.

- ***Colectarea și prelucrarea numerelor de telefon din registrele abonaților***

Legea nr. 677/2001 stabilește că nu este necesar consimțământul persoanei vizate când prelucrarea privește date obținute din documente accesibile publicului, conform legii.

Totodată, în cazul în care datele nu sunt obținute direct de la persoana vizată, operatorul este obligat ca, în momentul colectării datelor sau, dacă se intenționează dezvăluirea acestora către terți, cel mai târziu până în momentul primei dezvăluiri, să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care persoana vizată posedă deja informațiile respective:

a) identitatea operatorului și a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informații suplimentare, precum: categoriile de date vizate, destinatarii sau categoriile de destinatari ai datelor, existența drepturilor prevăzute de prezenta lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție, precum și condițiile în care pot fi exercitate;

d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

În consecință, având în vedere dispozițiile legale susmenționate, la contactarea telefonică a persoanei vizate, operatorul are obligația de a furniza informațiile prevăzute mai sus, inclusiv asupra sursei obținerii numărului de telefon, pentru a da posibilitatea acesteia să-și dea consimțământul în cunoștință de cauză.

- ***Obținerea accesului în Registrul Național de Evidență a Persoanelor (RNEP), în scopul verificării datelor de identitate ale solicitanților de certificate digitale calificate***

În solicitarea înaintată Autorității de Supraveghere a fost invocat ca temei legal al prelucrării Instrucțiunile nr. 27/2010 privind măsurile de natură organizatorică și tehnică pentru asigurarea securității prelucrărilor de date cu caracter personal efectuate de către structurile/unitățile Ministerului Administrației și Internelor

În acest context, art. 1 din Instrucțiunile nr. 27/2010 stabilește faptul că acestea se aplică activităților de prelucrare a datelor cu caracter personal efectuate de structurile și unitățile Ministerului Administrației și Internelor, în calitatea acestora de operatori sau împuterniciți ai operatorilor.

În consecință, dispozițiile Instrucțiunilor nr. 27/2010 nu devin aplicabile în cazul solicitării adresate de operator, întrucât nu vizează activitatea specifică de prevenire, cercetare

și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, desfășurată de structurile și unitățile Ministerului Administrației și Internelor. În acest sens, nu poate fi pus în discuție un acces on-line al operatorului la Registrul Național de Evidență a Persoanelor.

Cât privește activitatea de verificare a identității solicitanților exclusiv pe baza actelor de identitate, dispozițiile art. 19 alin. (1) din Legea nr. 455/2001 privind semnătura electronică, invocate de operator ca fiind obligație legală pe care se bazează scopul verificării are următoarea prevede că la eliberarea certificatelor calificate furnizorii de servicii de certificare au obligația de a verifica identitatea solicitanților exclusiv pe baza actelor de identitate. În acest sens, din text rezultă că obligația de verificare are loc la momentul eliberării certificatului de către furnizorul de servicii și nu după depunerea solicitării de către titular, în cadrul activității de emiterie a certificatului.

Cu toate acestea, în situația în care există, după caz, obligații legale impuse de Legea nr. 455/2001 privind semnătura electronică sau un interes legitim din partea operatorului, pentru verificarea identității solicitanților, aceasta se poate realiza în temeiul art. 5 alin. (2) lit. c) sau e) coroborat cu art. 8 alin. (1) lit. a) sau b) din Legea nr. 677/2001, modificată și completată. În acest sens, solicitările vor fi adresate Direcției pentru Evidența Persoanelor și Administrarea Bazelor de Date, pentru situațiile specifice.

Totodată, prelucrările de date efectuate în cadrul acestei activități pot avea ca obiect numai datele cu caracter personal care sunt adecvate, pertinente și neexcesive prin raportare la scopul stabilit, ceea ce înseamnă că în contextul dezvoltării datelor în vederea verificării solicitanților de certificate digitale trebuie să fie strict cele necesare îndeplinirii scopului (minimum de date necesare), cu atât mai mult cu cât dispozițiile Legii nr. 455/2001 nu prevăd în mod expres datele și categoriile de date necesare activității de verificare.

În sensul celor de mai sus, Legea nr. 455/2001 privind semnătura electronică, stabilește faptul că în vederea emiterii certificatelor calificate furnizorii de servicii de certificare trebuie să îndeplinească o serie de condiții, printre care și să verifice, cu mijloace corespunzătoare și conforme dispozițiilor legale, identitatea și, dacă este cazul, atributele specifice ale persoanei căreia îi este eliberat certificatul calificat.

Prin urmare, prelucrarea datelor în vederea verificării identității titularilor de certificate trebuie să respecte prevederile Legii nr. 677/2001, modificată și completată, expuse mai sus, fără ca aceasta să implice conectarea on-line a societății în cauză la Registrul Național de Evidență a Persoanelor.

- ***Condițiile legale care trebuie respectate la prelucrarea datelor prin sistemele de supraveghere video și monitorizare a accesului în clădirea unui bloc de locuințe***

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilități de înregistrare și stocare a imaginilor și datelor se supune atât prevederilor Legii nr. 677/2001, cât și ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor, modificată și completată.

Regula instituită de legea susmenționată este aceea că prelucrarea datelor personale ale unei persoane fizice, de către o altă persoană fizică sau juridică, în calitate sa de operator, se efectuează numai cu consimțământul persoanei în cauză, dat în mod expres și neechivoc, cu excepția cazului în care prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terțului căruia îi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate.

Prin urmare, se poate recurge la o monitorizare prin supraveghere video (sau prin monitorizarea accesului persoanelor fizice în clădire de către o societate de pază), în temeiul dispozițiilor legale de mai sus, dar numai dacă această măsură este proporțională cu riscurile cu care se confruntă operatorul și determină luarea unei asemenea măsuri intruzive. În același timp, trebuie să se țină cont și de interesele, drepturile și libertățile persoanelor vizate – locatarii, vizitatorii, clienții (ale căror imagini se înregistrează).

Astfel, acestea trebuie informate anterior cu privire la luarea unei astfel de măsuri, potrivit art. 12 din Legea nr. 677/2001, prin instalarea unei pictograme adecvate, care să conțină o imagine reprezentativă, poziționată la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

La instalarea echipamentelor de supraveghere video trebuie să se acorde o atenție deosebită modului în care acestea sunt orientate, astfel încât în raza lor de acoperire să nu fie vizualizate proprietățile vecinilor, pentru a se evita orice ingerință în viața privată a acestora.

Camerele de supraveghere ascunse nu pot fi utilizate decât în condițiile și cu autorizările prevăzute de Codul de procedură penală.

În ceea ce privește monitorizarea accesului persoanelor fizice în clădire de către o societate de pază, dacă datele personale se înregistrează într-un sistem de evidență pe suport de hârtie (registru), temeiul legal al art. 5 alin. (2) din Legea nr. 677/2001, precizat anterior, devine aplicabil în aceleași condiții expuse mai sus.

Totodată, este de subliniat că, potrivit art. 20 din Legea nr. 677/2001, operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu

caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Activitatea de monitorizare a accesului în clădire, fie prin mijloacele de supraveghere video, fie prin intermediul firmei de pază în condițiile precizate mai sus, presupune prelucrări de date cu caracter personal, astfel că aceasta se supune obligației de notificare stabilită în sarcina operatorului, prin prevederile Legii nr. 677/2001.

- ***Prelucrarea datelor în contextul furnizării unui serviciu destinat persoanelor fizice care va permite efectuarea unor transferuri de bani și plata unor facturi prin intermediul telefonului mobil***

În situația în care operatorul stabilit în România desfășoară o activitate de prelucrare a datelor care implică și comunicarea acestora către un destinatar situat într-un alt stat din afara UE, datele fiind destinate a face obiectul unei prelucrări în statul respectiv, comunicarea datelor în cauză reprezintă un transfer în străinătate (în cazul în speță, SUA).

În acest sens, în conformitate cu prevederile Legii nr. 677/2001, Autoritatea de Supraveghere poate autoriza transferul de date cu caracter personal către un stat a cărui legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română atunci când operatorul oferă garanții suficiente cu privire la protecția drepturilor fundamentale ale persoanelor. Aceste garanții trebuie să fie stabilite prin contracte încheiate între operatori și persoanele fizice sau juridice din dispoziția cărora se efectuează transferul.

Transferul efectuat în baza unui contract încheiat între exportatorul și importatorul de date, este supus procedurii autorizării.

În acest scop, în funcție de calitatea importatorului de date (operator/împuțernicit) vor fi avute în vedere:

- clauzele contractuale standard care reglementează transferul datelor de la un operator din România către un operator stabilit într-un stat a cărui legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română (Decizia 2001/497/CE privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE, așa cum aceasta a fost modificată prin Decizia 2004/915/CE);

- clauzele contractuale standard care reglementează transferul datelor de la un operator din România către un împuțernicit stabilit într-un stat a cărui legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română (Decizia 2010/87/UE privind clauzele

contractuale standard pentru transferul de date cu caracter personal către persoanele împuternicite de operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului).

De asemenea, transferurile dintr-un stat membru UE (România) către o societate din SUA, se poate efectua fără formalități specifice cum este încheierea unui contract de tipul celui menționat mai sus, în măsura în care societatea respectivă a aderat la principiile Safe Harbor (Decizia 2000/520/CE).

În consecință, față de situația pusă în discuție, în funcție de îndeplinirea condițiilor privind aderarea societății din SUA la Safe Harbour, transferul se va efectua în baza acestor principii (pentru care nu este necesară emiterea unei autorizații din partea Autorității) sau în baza unui contract cu clauze standard (care se autorizează).

În cea de-a doua situație, în funcție de calitatea societății din SUA; respectiv operator sau împuternicit, se va apela la unul dintre modelele de contracte prevăzute de deciziile Comisiei Europene precizate anterior. Clauzele standard se preiau ca atare, operatorul neputând să intervină asupra lor, pentru a se asigura toate garanțiile prevăzute de clauzele-tip, mai ales că se prelucrează codul numeric personal. În acest sens, este necesară încheierea unui contract distinct de contractul de aplicare a contractului-cadru dintre operatorul situat în România și cel situat în SUA.

- ***Transmiterea prin MMS a fotografiilor persoanelor care circulă fără bilet de călătorie pe mijloacele de transport în comun, în scopul întocmirii proceselor-verbale de contravenție***

Potrivit definiției stabilite de Legea nr. 677/2001, fotografiile persoanelor fizice intră în sfera datelor cu caracter personal.

Utilizarea fotografiilor persoanelor fizice în modalitatea expusă de operator, respectiv prin transmiterea acestora către agenții din teren prin MMS, nu respectă principiile expuse mai sus, înscrise în Legea nr. 677/2001, în special cel al legalității și proporționalității scopului, sens în care Autoritatea de Supraveghere apreciază că prelucrarea datelor în acest mod nu se poate efectua.

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

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



Activitatea efectuată în cadrul sistemelor respective presupune prelucrări de date cu caracter personal și se supune condițiilor stabilite de Legea nr. 677/2001, modificată și completată, iar entitatea responsabilă (care achiziționează și utilizează sistemul) de această activitate are calitatea de operator și, implicit, obligațiile stabilite de lege în sarcina sa, inclusiv cea de notificare.

Referitor la prelucrarea datelor biometrice ale angajaților, Autoritatea de Supraveghere apreciază că operațiunile de prelucrare a acestor date prezintă riscuri speciale pentru drepturile și libertățile persoanelor, astfel încât colectarea și prelucrarea acestora este excesivă prin raportare la scopul urmărit și la mijloacele utilizate.

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

- ***Calitatea de operator a unei sucursale a unei societăți străine situate în România***

În funcție de locul unde este situată societatea străină, există două posibilități, după cum aceasta se află în afara Comunității sau într-un stat membru.

În prima situație, devin aplicabile prevederile art. 2 alin. (2) lit. c) și alin. (3) din Legea nr. 677/2001, modificată și completată.

În cea de-a doua situație, față de prevederile legale menționate mai sus, având în vedere calitatea României de stat membru cu drepturi depline al Uniunii Europene, dispozițiile constituționale ale art. 148 din Legea fundamentală, precum și principiul priorității dreptului comunitar statuat de Curtea de Justiție a UE, operatorul situat pe teritoriul Comunității nu are obligația desemnării unui reprezentant. În acest sens, pentru desfășurarea activităților de prelucrare a datelor pe teritoriul României, acești operatori pot apela la împuterniciți.

Astfel, răspunderea pentru obligația de notificare subzistă în sarcina operatorului situat pe teritoriul statului membru respectiv și se supune legii privind protecția datelor din acel stat, împuternicitul fiind obligat să respecte dispozițiile legii române care stabilesc obligații în sarcina sa.

În anumite situații, acești împuterniciți ai societăților din alte state membre (sau din statele din afara Comunității) pot avea și calitatea de operatori, în sensul că pot stabili ei înșiși scopul și mijloacele prelucrării și deține datele colectate și înregistrate în sistemele proprii de

evidență. În această situație, au obligația declarării prelucrărilor de date pe care le efectuează, prin intermediul notificării și, implicit, a respectării Legii nr. 677/2001, modificată și completată.

În consecință, stabilirea calității de operator a unei sucursale a unei societăți străine presupune o analiză a aspectelor mai sus prezentate, raportate la activitatea de prelucrare a datelor efectuată de aceasta.

#### ***Secțiunea a 4-a: Activitatea de reprezentare în fața instanțelor de judecată***

##### ***❖ Prelucrarea datelor biometrice ale angajaților în scopul pontării timpului de lucru***

În urma investigațiilor efectuate de Autoritatea de Supraveghere, atât la operatori din sectorul public, cât și la operatori din sectorul privat, s-a constatat că aceștia prelucrau datele biometrice ale angajaților în scopul pontării timpului de lucru al acestora.

Conform declarațiilor reprezentanților instituției publice la care s-a efectuat investigația, sistemul de pontaj electronic a fost introdus pentru disciplinarea salariaților și pentru o evidență mai ușoară a orelor lucrate.

Datele biometrice obținute din structura amprentelor digitale sunt considerate ca fiind date cu caracter personal, întrucât se circumscriu definiției date de lege ca fiind „orice informație” referitoare la o persoană fizică și au legătură cu persoane identificabile (angajații), astfel că prelucrarea intră sub incidența dispozițiilor Legii nr. 677/2001, modificată și completată.

Pentru introducerea sistemului de pontaj electronic prin amprentare, salariaților li s-a comunicat o dispoziție a conducătorului instituției, fără a solicita un acord expres cu privire la prelucrarea datelor biometrice prin amprentarea digitală, astfel cum stabilește art. 5 alin. (1) din Legea nr. 677/2001.

Potrivit Documentului de lucru privind datele biometrice - Working document on biometrics (WP 80 din 1 august 2003) al Grupului de lucru Art. 29, pentru aplicarea principiului scopului și proporționalității (principalul criteriu în luarea unei decizii cu privire la prelucrarea datelor biometrice), autoritățile de supraveghere trebuie să aibă în vedere riscurile pentru drepturile și libertățile fundamentale ale persoanelor, în special, dacă atingerea scopului respectiv se poate realiza de o manieră mai puțin intruzivă.

În consecință, datele biometrice sunt considerate a fi excesive față de scopul prelucrării, respectiv, pontarea timpului de lucru al angajaților, putând fi utilizate și alte mijloace pentru atingerea acestui scop, mai puțin intruzive în viața privată a angajaților.

Anterior implementării dispozitivelor biometrice este necesară din partea operatorului o analiză temeinică asupra necesității și proporționalității unei astfel de măsuri, precum și identificarea unor soluții alternative care să aibă un impact mai redus asupra vieții private a salariaților.

În acest sens, constatările Curții Europene a Drepturilor Omului rezultate din jurisprudența sa referitoare la încălcarea art. 8 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale, și anume la faptul că protecția oferită de acest articol ar fi diminuată în mod inacceptabil dacă „folosirea de tehnici științifice moderne ar fi permisă cu orice preț și fără realizarea unui echilibru între beneficiile folosirii extensive a acestor tehnici și interesele importante legate de viața privată, iar orice stat care pretinde să aibă un rol de pionier în dezvoltarea noilor tehnologii poartă responsabilitatea obținerii unui echilibru corect în această problemă.”

Prin urmare, astfel cum au precizat reprezentanții instituție publice prin acțiunea introdusă la instanța de judecată, conducătorul instituției „are libertatea de a dispune acele măsuri pe care le consideră oportune și eficiente în scopul evidențierii corecte a timpului de lucru a angajaților”, dar numai cu condiția de a nu prejudicia drepturile și libertățile persoanelor vizate (în speță, angajați).

Pentru faptele constatate cu ocazia efectuării investigației la instituția publică, președintele Autorității de supraveghere a emis o decizie prin care a dispus încetarea prelucrării datelor biometrice ale angajaților și ștergerea datelor respective, prelucrate anterior datei comunicării deciziei.

Instanța judecătorească a respins ca neîntemeiată acțiunea formulată de operatorul care a contestat decizia emisă de președintele Autorității, consfințind astfel că Autoritatea de Supraveghere în mod corect și legal a aplicat măsurile respective.

#### ***❖ Publicarea pe internet a datelor cu caracter personal de către instituții publice***

Autoritatea de Supraveghere a efectuat o serie de investigații la instituții publice urmare a unor plângeri referitoare la faptul că acești operatori au publicat pe internet liste ale contribuabililor cărora li s-au emis decizii de impunere, respectiv somații și titluri executorii, privind obligațiile de plată la Fondul Național Unic de Asigurări Sociale de Sănătate. Listele

cuprindeau date personale aparținând unui număr de semnificativ de persoane, cu menționarea numelui, prenumelui, adresei complete, a numărului și a datei emiterii, respectiv, a numelui, prenumelui, adresei complete, a numărului somației, numărului titlului executoriu și a datei emiterii.

De asemenea, din alte verificări ale site-ului unuia dintre operatorii controlați, a rezultat că, în cazul asiguraților persoane fizice, sunt publicate, de asemenea, anunțuri colective în baza art. 44 din Codul de procedură fiscală, pentru decizii de impunere sau pentru somații și titluri executorii, cuprinzând data, nume și prenume contribuabil, județ, localitate, adresa propriu-zisă fiind obturată complet. Cu toate acestea, în urma operațiunii de imprimare a unui extras din această listă, s-a constatat că sunt vizibile integral adresele contribuabililor.

S-a constatat că operatorii nu au încercat, în prealabil, modalitatea de comunicare a actelor administrative fiscale către contribuabili, modalitate curentă (adică prin poștă), prevăzută atât de Codul de procedură fiscală cât și de dreptul comun, de natură a permite transmiterea și primirea acestora în condiții de confidențialitate, motivând „lipsa resurselor financiare”. Numai ulterior epuizării acesteia sau celorlalte modalități stabilite de Codul de procedură fiscală, în mod excepțional operatorii ar fi putut să procedeze la comunicarea prin publicitate pe Internet, dar numai cu respectarea regulilor de protecție a datelor cu caracter personal.

Astfel, publicitatea actelor administrative fiscale prin Internet este reglementată de Ordinul ministrului finanțelor publice nr. 94/2006 privind aprobarea modelului și conținutului formularelor și a instrucțiunilor de completare a acestora în vederea îndeplinirii procedurii de comunicare a actelor administrative fiscale prin publicitate, ca o ultimă și subsidiară modalitate de comunicare a acestor acte.

Curtea Constituțională a reținut că modalitățile de comunicare a actelor administrative fiscale sunt menționate într-o ordine de prioritate în ceea ce privește aplicarea lor. Astfel, prima dintre acestea, care asigură certitudinea absolută a luării la cunoștință a contribuabilului de conținutul actului administrativ fiscal, este cea de constând în prezentarea contribuabilului la sediul organului fiscal emitent și primirea actului administrativ fiscal de către acesta sub semnătură. De asemenea, un grad înalt de certitudine îl conferă și remiterea către contribuabil, sub semnătură, a actului administrativ fiscal de către persoanele împuternicite ale organului fiscal. Urmează, comunicarea prin poștă, la domiciliul fiscal al contribuabilului, cu scrisoare recomandată cu confirmare de primire, precum și prin alte mijloace, cum sunt fax, e-mail, dacă se asigură transmiterea textului actului administrativ fiscal și confirmarea primirii

acestui. În fine, se menționează comunicarea prin publicitate, a cărei descriere se găsește în textul de lege criticat în cauza de față.

În mod evident, intenția legiuitorului a fost de a institui o anumită ordine pentru modalitățile de comunicare a actelor administrative fiscale, prefigurând, prin succesiunea susmenționată, obligația organului fiscal de a proceda la comunicare doar cu respectarea ordinii de utilizare a acestora prevăzută în art. 44 alin. (2).

Curtea a observat că Ordonanța Guvernului nr. 92/2003 privind Codul de procedură fiscală reprezintă o lege specială, care instituie unele reguli derogatorii de la cele stabilite de dreptul comun, reprezentat de Codul de procedură civilă. Interesul organelor fiscale de aducere la cunoștința contribuabilului a existenței unei obligații fiscale al cărei creditor este însuși statul implică necesitatea comunicării actului administrativ în care aceasta este consemnată prin modalități care să asigure aducerea efectivă la cunoștința contribuabilului despre existența unor obligații fiscale în sarcina sa.

Așa fiind, legiuitorul a prevăzut că actele administrative fiscale pot fi comunicate prin publicitate și în cazul în care domiciliul contribuabilului este cunoscut. În acest caz, însă, trebuie ca, anterior recurgerii la această modalitate, să fi fost respectată cu strictețe ordinea prevăzută în art. 44 alin. (2) lit. a) - c) din Ordonanța Guvernului nr. 92/2003, astfel încât comunicarea prin publicitate să reprezinte doar o modalitate ultimă și subsidiară, după cum a remarcat și Curtea Constituțională în jurisprudența mai sus citată.

Conform Legii nr. 677/2001 operatorii controlați trebuiau să prelucreze datele cu bună-credință și în conformitate cu dispozițiile legale în vigoare.

Instanța a respins acțiunea, iar hotărârea pronunțată în favoarea Autorității a rămas definitivă.

## CAPITOLUL AL V-LEA

### ACTIVITATEA DE RELAȚII EXTERNE

Datorita restricțiilor de ordin bugetar, Autoritatea de Supraveghere s-a aflat și în cursul anului 2011, de cele mai multe ori, în imposibilitatea de a asigura reprezentarea în cadrul reuniunilor la care a fost invitată să participe.

Luând în considerare obiectivul asumat de România de aderare la spațiul Schengen, precum și importanța acestuia, Autoritatea de Supraveghere și-a îndeplinit obligația legală de a participa, în calitate de observator, la reuniunile Autorității Comune de Control Schengen, iar în calitate de membru cu drepturi depline, la reuniunile organismelor comunitare de control Europol, Eurodac, Vămi, Cooperare polițienească și judiciară – foruri ce reunesc, în principal, reprezentanți ai autorităților naționale responsabile de protecția datelor personale din fiecare stat al Uniunii Europene.

Subiectele dezbătute în cadrul acestor reuniuni au vizat în special aspecte privind consolidarea capacității de exercitare a controlului independent de către autoritățile naționale de protecția datelor personale, exercitarea dreptului de acces de către persoanele vizate, stabilirea competențelor de supraveghere ale autorităților comune de control, modalitățile de implementare a Acordului TFTP în cadrul Programului de urmărire a finanțării în scopuri teroriste, precum și probleme specifice întâmpinate în utilizarea sistemelor informatice.

Autoritatea de Supraveghere a fost, de asemenea, invitată să participe în aprilie 2011 la misiunea de evaluare Schengen a Liechtenstein-ului în vederea aderării acestui stat la spațiul Schengen. Aceasta a reprezentat o recunoaștere a capacității instituționale a Autorității române de supraveghere, evenimentul constituind totodată un mijloc de consolidare a experienței dobândite de către Autoritatea de Supraveghere în desfășurarea activităților specifice în perioada premergătoare și ulterioară aderării României la spațiul Schengen.

Dezbaterile pe marginea propunerilor de modificare a cadrului legal referitor la protecția datelor existente la nivel european au reprezentat un alt element al activității Autorității de Supraveghere la nivel internațional.

A fost, astfel, identificată necesitatea unei abordări principiale în elaborarea noului cadru al Uniunii, dar și a unei aplicabilități practice a principiilor ce vor fi statuate, pornind de la principiile existente în Tratatul UE. Astfel, egalitatea de tratament a cetățenilor UE și independența autorităților de protecție a datelor personale sunt două elemente cheie a viitoarei reglementări.

Unitatea aplicării legii este piesa de bază a funcționării UE, întrucât cetățenii UE așteaptă să fie tratați egal. Ca atare, este atributul legislației UE să asigure aplicarea acesteia în toate țările membre, fără a uita însă de aspectul competitivității în domeniul privat în aceste țări.

Luând în considerare necesitatea implementării principiilor referitoare la protecția datelor într-o societate aflată în continuă schimbare, a fost subliniată utilitatea includerii în noua reglementare la nivel Uniunii Europene a unor principii precum *privacy by design* sau principiul răspunderii operatorilor, deoarece operatorii nu au doar obligația de informare a persoanelor, ci trebuie să demonstreze că au luat toate măsurile ce se impun pentru asigurarea unei prelucrări adecvate principiilor de prelucrare a datelor personale. Atunci când sunt create noi produse sau servicii, trebuie să fie stabilite încă de la început reguli de protecție a datelor pentru a crea un climat de încredere în relația cu consumatorul. Autoritățile de protecția datelor intervin doar la finalul procesului de relaționare operator-consumator, pentru a verifica măsurile luate.

Principiile referitoare la protecția datelor reprezintă, de asemenea, un element important în cadrul procesului de modificare a cadrului normativ privind protecția datelor. A fost, astfel, indicată necesitatea stabilirii unor principii clare de protecție a datelor, precum și a respectării acestora în cadrul tuturor prelucrărilor de date, în special celor al proporționalității și al necesității.

Evoluțiile noilor tehnologii, în special cele referitoare la tehnologia informației, au impus pe agenda de lucru a autorităților de supraveghere din întreg spațiul european subiecte privind: cloud computing - tehnologie utilizată din ce în ce mai des la nivel internațional, inclusiv de către autorități publice, în vederea reducerii costurilor operaționale, întrucât stocarea datelor sau accesarea aplicațiilor de la distanță reduce necesitatea unei infrastructuri tehnologice proprii, a suportului IT și a personalului specializat; rețelele de socializare pe internet – activitățile desfășurate pe marginea acestui aspect vizând asigurarea respectării principiilor de protecție a datelor în cadrul acestui gen de prelucrări de date, în special în ceea ce privește informarea în mod corect a persoanelor vizate, precum și obținerea consimțământului expres și neechivoc al acestora; datele de geo-localizare – în acest sens fiind urmărită clarificarea cadrului legal aplicabil serviciilor de localizare geografică care sunt disponibile sau sunt generate de către dispozitive mobile precum GPS-uri sau telefoane mobile „inteligente”/smart phone.

Reuniunile autorităților de supraveghere ale statelor membre UE de tipul seminariilor de cazistică au constituit un forum de dezbatere a unor subiecte comune, întâlnite în

activitatea curentă a autorităților. Un exemplu în acest sens a fost reprezentat de prelucrarea datelor angajaților la locul de muncă, fie prin mijloace de supraveghere audio/video sau prin urmărirea activității on-line în cadrul programului de lucru, fie prin utilizarea unor mijloace disproporționate (spre exemplu prelucrarea datelor biometrice/amprente digitale) în raport cu scopul în care datele erau colectate și prelucrate (asigurarea accesului la locul de muncă/pontajul orelor lucrate).



## CAPITOLUL AL VI-LEA

### COMUNICARE ȘI RELAȚII PUBLICE

#### Secțiunea 1: Activitatea de comunicare și relații publice

Autoritatea de Supraveghere a fost nevoită să restrângă activitățile de comunicare destinate informării publicului cu privire la regulile specifice protecției datelor cu caracter personal pentru încadrarea în limitele bugetului alocat.

Dintre evenimentele semnificative în care Autoritatea de supraveghere a fost implicată prin susținerea unor prezentări specifice, evidențiem:

- Conferința internațională „Supravegherea în societățile post-totalitare: Fantomele supravegherii”

La invitația Universității Alexandru Ioan Cuza din Iași, reprezentanții Autorității de supraveghere au participat în perioada 3-5 mai 2011, la conferința internațională desfășurată în cadrul proiectului European COST, eveniment ce a urmărit evoluția fenomenului supravegherii la nivelul societății, inclusiv sub forma video/audio.

Reprezentanții Autorității au realizat o prezentare a cadrului normativ în domeniul protecției datelor și a competențelor Autorității.

- Conferința Internațională „Rolul și locul dreptului într-o societate bazată pe cunoaștere”

În colaborare cu Masaryk University (Cehia) și sub patronajul Uniunii Naționale a Juriștilor din România, Universitatea Constantin Brâncuși din Tg. Jiu a organizat, în perioada 13-14 mai 2011, în coordonarea domnului prof. univ. dr. Moise Bojincă –decanul Facultății de Științe Juridice și Litere, a șasea ediție a conferinței științifice internaționale, destinată să dezbată aspecte semnificative legate de protecția persoanei.

În considerarea tematicii abordate, reprezentanții Autorității au susținut în cadrul Conferinței trei prezentări intitulate „Dreptul la viață privată”, „Prelucrarea datelor personale și datele de geo-localizare” și „Drepturile persoanelor vizate”.

În considerarea anvergurii internaționale a evenimentului, la invitația Autorității de Supraveghere, a participat la manifestare o delegație din Macedonia a autorității pentru protecția datelor, condusă de comisarul acesteia.

- Reuniunea „Noile provocări globale de securitate cibernetică. Rolul structurilor de tip CERT”,

Organizată pe data de 29 septembrie 2011, la Palatul Parlamentului, de către Centrul Național de Răspuns la Incidentele de Securitate Cibernetică, evenimentul s-a constituit într-un prilej de dezbatere a unor aspecte de interes pentru companiile din domeniul privat, referitoare în special la confidențialitatea informațiilor și datelor utilizate, la modalități adecvate de asigurare a securității și confidențialității acestora adaptate noilor tehnologii.

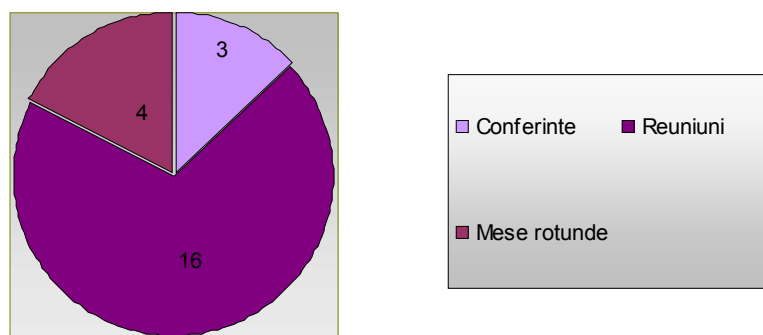
- Masa Rotundă „Protectia Datelor cu Caracter Personal și Politicile Antispam”

La invitația Asociației Române de Marketing Direct, pe data de 22 septembrie în București, a fost organizată o reuniune la care reprezentanții Autorității de Supraveghere au prezentat principalele aspecte specifice referitoare la prelucrarea datelor personale în domeniul marketingului direct.

În cursul manifestării s-au discutat situațiile cu care s-au confruntat operatorii în activitatea curentă și cele mai eficiente modalități de asigurare a respectării drepturilor persoanelor implicate.

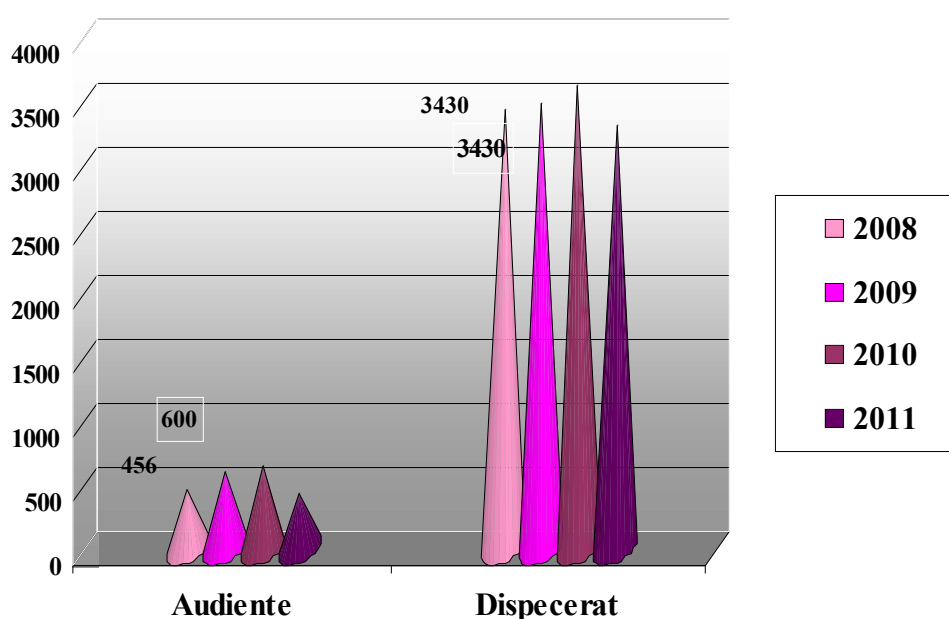
În cursul anului, acțiunile de informare au continuat prin organizarea a patru întruniri în municipiile Deva, Râmnicu-Vâlcea, Constanța și Zalău, cu sprijinul consiliilor județene respective.

Cu ocazia acestor evenimente la care au participat reprezentanți ai autorităților publice locale și ai serviciilor deconcentrate ale ministerelor, au fost analizate regulile ce reglementează prelucrarea datelor cu caracter personal, condițiile de legitimitate a prelucrărilor, măsurile de asigurare a confidențialității și securității acestora, precum și aspectele de aplicabilitate practică a prevederilor Legii nr. 677/2001.



La aceste evenimente au fost transmise participanților broșuri și pliante informative privind respectarea regulilor de prelucrare a datelor personale, editate în cadrul Autorității naționale de supraveghere.

Prin serviciile de dispecerat și audiențe s-a realizat informarea rapidă și eficientă a cetățenilor și a operatorilor, în sensul că au fost oferite, într-o manieră directă, informații utile cu privire la drepturile persoanelor vizate și obligațiile specifice operatorilor, lămuriri cu privire la condițiile prelucrării datelor și la dezvăluirea acestora către terți. Astfel s-au acordat **648** de audiențe și s-au primit **3612** apeluri telefonice referitoare la aspecte incidente asupra protecției datelor personale.



O altă expresie a creșterii gradului de conștientizare a publicului cu privire la drepturile lor, dar și a preocupării operatorilor asupra modului de folosire a datelor personale, este reprezentată de primirea de către instituția noastră, în anul 2010, a unui număr total de 1213 de cereri prin care s-au solicitat informații cu privire la aplicarea Legii nr. 677/2001.

În scopul popularizării activității instituției și a reglementărilor specifice în materie, au fost publicate, pe site-ul [www.dataprotection.ro](http://www.dataprotection.ro), numeroase comunicate de presă, prin care au fost semnalate aspecte semnificative din implicarea autorității în anumite evenimente, pozițiile publice față de anumite proiecte de acte normative sau alte manifestările în care a fost implicată Autoritatea de supraveghere .

Prin intermediul site-ului Autorității s-a urmărit asigurarea unei informări adecvate a persoanelor fizice, cât și a operatorilor care pot solicita opinia Autorității, utilizând inclusiv adresa de e-mail pusă la dispoziție în acest sens: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro) .

## **Secțiunea a 2-a: Relația cu mass-media**

Domeniul protecției datelor personale și activitatea Autorității de supraveghere s-a aflat și în acest an în atenția mass-mediei. Aceasta s-a reflectat în articolele de presă publicate, pe teme specifice diverse, în emisiuni radiofonice și televizate, ceea ce denotă interesul manifestat al mass-mediei pentru aspectele ce implică folosirea adecvată a datelor personale.

Presa scrisă a solicitat punctul de vedere al Autorității de supraveghere și a reflectat activitatea acesteia, în special investigațiile efectuate și măsurile aplicate.

Răspunsurile date la solicitările primite s-au concretizat în mai multe articole care au adus în atenția publicului larg poziția instituției noastre în ceea ce privește activitatea instituțiilor bancare de raportare a debitorilor la biroul de credit, condițiile de dezvoltare a datelor personale, drepturile de care beneficiază cetățenii în acest domeniu (în special dreptul la informare și la plângere), posibilitățile de valorificare a acestora și rolul autorității de supraveghere.

Aceste articole au fost publicate în presa centrală (Curierul Național, Adevărul, Jurnalul Național, Evenimentul Zilei), locală (Sălăjeanul) și de către portalurile de informații (www.hotnews.ro, www. b365, www. citynews.ro ). S-au acordat interviuri în legătură cu anumite aspecte referitoare la asigurarea protecției datelor personale (Antena 3, PRO TV, Europa FM).

Mass-media continuă să reprezinte un sprijin important în activitatea instituției noastre destinată atingerii obiectivului sensibilizare a publicului larg cu privire la principiile de protecției a datelor personale.

## CAPITOLUL AL VII-LEA

### MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

Pentru anul 2011 Autoritatea de Supraveghere a avut alocate fonduri prin Legea bugetului de stat pe anul 2011 nr. 286/2010, cu modificările și completările ulterioare, structura finală fiind următoarea:

Denumire indicator	Cod	Mii lei		
		Buget actualizat la 31.12.2011	Sume cheltuite până la 31.12.2011	Execuție (%)
Total cheltuieli din care:		3.332	3.284	98,56%
Cheltuieli de personal	10	2.178	2.169	99,59%
Bunuri și servicii	20	1.107	1.091	98,55%
Cheltuieli de capital	70	47	24	51,00%

Restricțiunile existente în execuția bugetară au impus permanenta actualizare a priorităților pentru realizarea celor mai importante proiecte cu fondurile existente. Ele au avut ca efect renunțarea la efectuarea unor achiziții de bunuri și a unor investigații pe teren.

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

Suma aferentă cheltuielilor de personal ale Autorității de Supraveghere a constituit un procent de 65% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 2.169 mii lei. Majoritatea cheltuielilor de personal au fost aferente plăților făcute pentru munca salariată a angajaților din departamentele de specialitate.

Cheltuielile cu deplasările au reprezentat 5,8 % din totalul cheltuielilor pe anul 2011. Trebuie menționat aici faptul că Autoritatea de Supraveghere își realizează obiectul principal de activitate prin investigații și controale la operatorii situați pe teritoriul României, precum și la consulatele României.

La nivelul Uniunii Europene, Autoritatea de Supraveghere are obligația de a participa la lucrările Grupului de lucru Art. 29 și la grupurile de lucru pe domeniul protecției datelor constituite la acest nivel și ale autorităților comune de control (Schengen, Europol, Eurodac) și la lucrările Consiliului Europei în domeniu. Sumele alocate pentru deplasări cuprind și aceste cheltuieli.

Nivelul relativ scăzut al celorlalte cheltuieli cu bunurile și serviciile achiziționate este rezultatul mai multor factori, dintre care menționăm: criteriul prețului cel mai scăzut aplicat în

procedurile de achiziții, alături de cerințe tehnice atent stabilite, precum și restricțiile bugetare.

Execuția bugetară aferentă cheltuielilor de investiții a fost de 51% datorită timpului foarte scurt dintre mutarea instituției în spațiul pus la dispoziție de RAPPs și sfârșitul anului bugetar, unele achiziții cu timpi mari de execuție neputând fi efectuate.

Fondurile bugetare au fost utilizate cu maximă eficiență și printr-o atentă administrare a sumelor alocate instituției noastre.

