32000D0520

DECIZIA COMISIEI
din 26 iulie 2000
în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al S.U.A.

[notificată cu numărul C(2000) 2441]

(Text cu relevanță pentru SEE)

(2000/520/CE)

COMISIA COMUNITĂȚILOR EUROPENE,

având în vedere Tratatul de instituire a Comunității Europene,

având în vedere Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date [1] și, în special, articolul 25 alineatul (6) al acesteia,

întrucât:

(1) În temeiul Directivei 95/46/CE, statelor membre li se cere să ia măsuri astfel încât transferul datelor cu caracter personal către o țară terță să poată avea loc numai în cazul în care țara terță în cauză asigură un nivel adecvat de protecție și în cazul în care legile statelor membre care pun în aplicare alte dispoziții ale directivei sunt respectate înainte de transfer.

(2) Comisia poate constata că o țară terță asigură un nivel adecvat de protecție. În acest caz, datele cu caracter personal pot fi transferate din statele membre fără a mai fi necesare garanții suplimentare.

(3) În temeiul Directivei 95/46/CE, nivelul de protecție a datelor trebuie evaluat având în vedere toate circumstanțele în care se desfășoară o operațiune de transfer de date sau un set de operațiuni de transfer de date și ținând seama de condițiile date. Grupul de lucru privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, înființat în temeiul directivei menționate anterior [2], a emis indicații referitoare la efectuarea acestor evaluări [3].

(4) Ținând seama de diferitele abordări ale protecției datelor în țările terțe, ar trebui efectuată evaluarea caracterului adecvat al acestei protecții, iar orice decizie întemeiată pe articolul 25 alineatul (6) din Directiva 95/46/CE ar trebui aplicată astfel încât să nu producă discriminări arbitrare sau nejustificate împotriva țărilor terțe sau între acestea acolo unde există condiții similare și nici să nu constituie o barieră ascunsă în calea comerțului, ținând seama de angajamentele internaționale actuale ale Comunității.

(5) Nivelul adecvat de protecție pentru transferul de date din Comunitate către Statele Unite ale Americii, recunoscut prin prezenta decizie, ar trebui obținut în cazul în care organizațiile respectă principiile „sferei de siguranță" privind protecția vieții private pentru protecția datelor cu caracter personal transferate dintr-un stat membru în Statele Unite ale Americii (denumite în continuare „principiile") și întrebările de bază, „frequently asked questions" (denumite în continuare „FAQ"), care oferă indicații pentru punerea în aplicare a principiilor publicate de Guvernul Statelor Unite ale Americii la 21 iulie 2000. Mai mult, organizațiile ar trebui să-și facă publice politicile de confidențialitate și să se supună jurisdicției Comisiei Federale pentru Comerț (Comisia Federală pentru Comerț – FTC) în temeiul articolului 5 din Federal Trade Commission Act care interzice actele sau practicile neloiale sau frauduloase în comerț sau care afectează comerțul, sau altui organism oficial care asigură punerea în aplicare cu eficacitate a principiilor în conformitate cu FAQ.

(6) Sectoarele și/sau prelucrarea de date care nu intră sub jurisdicția nici unuia dintre organismele administrative ale Statelor Unite ale Americii enumerate în anexa VII la prezenta decizie ar trebui să nu intre în domeniul de aplicare al prezentei decizii.

(7) Pentru a asigura buna aplicare a prezentei decizii, este necesar ca organizațiile care aderă la principii și la FAQ să poată fi recunoscute de către părțile interesate, ca de exemplu persoanele vizate, exportatorii de date și autoritățile însărcinate cu protecția datelor. În acest scop, Departamentul Comerțului al Statelor Unite ale Americii sau reprezentantul acestuia ar trebui să își ia angajamentul

---

[1] JO L 281, 23.11.1995, p. 31.

[2] Adresa web a grupului de lucru este: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

[3] WP 12: Transferurile de date cu caracter personal către țări terțe: aplicarea articolelor 25 și 26 din Directiva UE privind protecția datelor, document adoptat de grupul de lucru la 24 iulie 1998.

de a păstra și a face publică o listă a organizațiilor care își declară adeziunea la principiile puse în aplicare în conformitate cu FAQ și care intră sub jurisdicția a cel puțin unuia dintre organismele administrative enumerate în anexa VII la prezenta decizie.

(8) În scopul transparenței și pentru a permite autorităților competente din statele membre să asigure protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, este necesar ca în prezenta decizie să se indice circumstanțele excepționale în care suspendarea anumitor fluxuri de date ar fi justificată în ciuda constatării unei protecții adecvate.

(9) Ar putea fi necesar ca „sfera de siguranță" creată de principii și de FAQ să fie revizuită în lumina experienței, a evoluției protecției vieții private în circumstanțe în care tehnologia facilitează din ce în ce mai mult transferul și prelucrarea datelor cu caracter personal și în lumina rapoartelor privind punerea în aplicare elaborate de autoritățile competente.

(10) Grupul de lucru privind protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal înființat în temeiul articolului 29 din Directiva 95/46/CE a emis avize privind nivelul de protecție pe care îl asigură principiile „sferei de siguranță" în Statele Unite ale Americii, avize luate în considerare la elaborarea prezentei decizii ([1]).

(11) Măsurile prevăzute de prezenta decizie sunt conforme cu avizul comitetului constituit în temeiul articolului 31 din Directiva 95/46/CE.

(12) În temeiul Deciziei 1999/468/CE a Consiliului și, în special, al articolului 8 din aceasta, la 5 iulie 2000 Parlamentul European a adoptat Rezoluția A5-0177/2000 cu privire la proiectul de decizie a Comisiei privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al Statelor Unite ale Americii ([2]). Comisia a reexaminat proiectul de decizie în lumina acelei rezoluții și a concluzionat că, deși Parlamentul European și-a exprimat opinia că sunt necesare anumite îmbunătățiri ale principiilor „sferei de siguranță" și întrebărilor de bază aferente înainte de a putea considera că oferă o „protecție adecvată", acesta nu a stabilit că s-ar depăși competențele Comisiei în cazul în care aceasta adoptă decizia,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

(1) În sensul articolului 25 alineatul (2) din Directiva 95/46/CE, pentru toate activitățile care intră în domeniul de aplicare al acelei directive, principiile „sferei de siguranță" privind protecția vieții private (denumite în continuare „principiile"), cuprinse în anexa I la prezenta decizie, puse în aplicare în conformitate cu orientările furnizate de întrebările de bază („frequently asked questions" – denumite în continuare „FAQ") publicate de Departamentul Comerțului al Statelor Unite ale Americii la 21 iulie 2000, cuprinse în anexa II la prezenta decizie, asigură un nivel adecvat de protecție a datelor personale transferate din Comunitate către organizații stabilite în Statele Unite ale Americii, ținând seama de următoarele documente emise de Departamentul Comerțului al Statelor Unite ale Americii:

(a) studiul privind punerea în aplicare a principiilor „sferei de siguranță" menționat la anexa III;

(b) un memorandum privind despăgubirile pentru încălcarea vieții private și autorizațiile exprese prevăzute de legislația Statelor Unite ale Americii, menționat la anexa IV;

(c) o scrisoare din partea Comisiei Federale pentru Comerț, menționată la anexa V;

(d) o scrisoare din partea Departamentului Transporturilor al Statelor Unite ale Americii, menționată la anexa VI.

(2) În ceea ce privește fiecare transfer de date, trebuie respectate următoarele condiții:

(a) organizația care primește datele își declară în mod public și clar angajamentul de a respecta principiile puse în aplicare în conformitate cu FAQ și

(b) organizația intră sub jurisdicția unui organism administrativ din Statele Unite ale Americii menționat la anexa VII la prezenta decizie care este împuternicit să ancheteze plângerile și să obțină măsuri de reparare împotriva practicilor neloiale sau frauduloase precum și despăgubirea persoanelor în cauză, indiferent de țara de reședință sau de cetățenia acestora, în cazul nerespectării principiilor puse în aplicare în conformitate cu FAQ.

(3) Se consideră că sunt îndeplinite condițiile prevăzute la alineatul (2) de fiecare organizație care își declară adeziunea la principiile puse în aplicare în conformitate cu FAQ, de la data la care organizația notifică Departamentului Comerțului al Statelor Unite ale Americii (sau reprezentantului acestuia) declararea publică a angajamentului menționat la alineatul (2) litera (a) și identitatea organismului administrativ menționat la alineatul (2) litera (b).

([1]) WP 15: Avizul 1/99 privind nivelul de protecție a datelor în Statele Unite și discuțiile în curs dintre Comisia Europeană și Statele Unite.
WP 19: Avizul 2/99 privind caracterul adecvat al principiilor internaționale ale „sferei de siguranță" publicat de Departamentul Comerțului al Statelor Unite la 19 aprilie 1999.
WP 21: Avizul 4/99 privind „întrebările de bază" care urmează să fie publicate de Departamentul Comerțului al Statelor Unite în legătură cu principiile „sferei de siguranță" propuse în legătură cu caracterul adecvat al principiilor „sferei de siguranță".
WP 23: Document de lucru privind stadiul actual al discuțiilor dintre Comisia Europeană și Guvernul Statelor Unite cu privire la principiile „sferei de siguranță".
WP 27: Avizul 7/99 privind nivelul de protecție a datelor oferit de principiile „sferei de siguranță", publicate alături de „întrebările de bază" (Frequently Asked Questions – FAQ) și alte documente conexe la 15 și 16 noiembrie 1999 de Departamentul Comerțului al Statelor Unite.
WP 31: Avizul 3/200 privind dialogul UE/SUA referitor la acordul privind „sfera de siguranță".
WP 32: Avizul 4/2000 privind nivelul de protecție oferit de „principiile sferei de siguranță".

([2]) Rezoluția nu a fost încă publicată în Jurnalul Oficial.

Articolul 2

Prezenta decizie se referă numai la caracterul adecvat al protecției oferite în Statele Unite ale Americii de principiile puse în aplicare în conformitate cu FAQ în vederea respectării cerințelor prevăzute la articolul 25 alineatul (1) din Directiva 95/46/CE și nu afectează aplicarea altor dispoziții din directiva menționată care privesc prelucrarea de date cu caracter personal în statele membre, în special articolul 4.

Articolul 3

(1) Fără a aduce atingere competențelor lor de a lua măsuri în vederea asigurării respectării dispozițiilor naționale adoptate în temeiul unor dispoziții altele decât cele prevăzute la articolul 25 din Directiva 95/46/CE, autoritățile competente din statele membre își pot exercita competențele de care dispun pentru a suspenda fluxurile de date către o organizație care și-a declarat adeziunea la principiile puse în aplicare în conformitate cu FAQ în vederea protejării persoanelor cu privire la prelucrarea datelor cu caracter personal ale acestora în cazurile în care:

(a) organismul administrativ din Statele Unite ale Americii menționat la anexa VII la prezenta decizie sau o instanță de recurs independentă în sensul literei (a) din principiul de punere în aplicare menționat la anexa I la prezenta decizie a constatat că organizația încalcă principiile puse în aplicare în conformitate cu FAQ sau

(b) este foarte probabil ca principiile să fie încălcate; există motive serioase pentru a crede că organismul de aplicare în cauză nu ia sau nu va lua din timp măsuri adecvate pentru a soluționa cauza respectivă; continuarea transferului ar crea pentru persoanele în cauză un risc iminent de a suferi prejudicii grave; iar autoritățile competente din statul membru au depus eforturi rezonabile, ținând seama de circumstanțe, de a avertiza organizația și a îi oferi posibilitatea de a răspunde.

Suspendarea încetează de îndată ce se asigură respectarea principiilor puse în aplicare în conformitate cu FAQ, iar autoritățile competente în cauză din Comunitate sunt informate în consecință.

(2) Statele membre informează fără întârziere Comisia atunci când sunt adoptate măsuri în temeiul alineatului (1).

(3) De asemenea, statele membre și Comisia se informează reciproc asupra cazurilor în care măsurile luate de organismele însărcinate cu asigurarea respectării principiilor puse în aplicare în conformitate cu FAQ în Statele Unite ale Americii nu asigură această respectare.

(4) În cazul în care informațiile strânse în aplicarea alineatelor (1), (2) și (3) demonstrează că un organism însărcinat cu asigurarea respectării principiilor puse în aplicare în conformitate cu FAQ în Statele Unite ale Americii nu își îndeplinește eficient rolul, Comisia informează Departamentul Comerțului al Statelor Unite ale Americii și, în cazul în care este necesar, prezintă un proiect de măsuri în conformitate cu procedura menționată la articolul 31 din Directiva 95/46/CE în vederea abrogării sau suspendării prezentei decizii ori a limitării domeniului de aplicare al acesteia.

Articolul 4

(1) Prezenta decizie poate fi oricând adaptată în lumina experienței dobândite în timpul punerii ei în aplicare și/sau în cazul în care nivelul de protecție oferit de principii și FAQ este depășit de exigențele legislației SUA.

În orice caz, Comisia evaluează punerea în aplicare a prezentei decizii pe baza informațiilor disponibile la trei ani de la notificarea ei statelor membre și raportează comitetului înființat în temeiul articolului 31 din Directiva 95/46/CE orice constatare pertinentă, inclusiv orice dovadă care ar putea afecta evaluarea conform căreia dispozițiile de la articolul 1 din prezenta decizie asigură un nivel adecvat de protecție în sensul articolului 25 din Directiva 95/46/CE și orice dovadă care indică faptul că prezenta decizie este aplicată în mod discriminatoriu.

(2) În cazul în care este necesar, Comisia prezintă un proiect de măsuri în conformitate cu procedura menționată la articolul 31 din Directiva 95/46/CE.

Articolul 5

Statele membre iau toate măsurile necesare pentru a se conforma prezentei decizii în termen de 90 de zile de la data notificării acesteia către statele membre.

Articolul 6

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 26 iulie 2000.

Pentru Comisie

Frederik BOLKESTEIN

Membru al Comisiei

ANEXA I

PRINCIPIILE „SFEREI DE SIGURANȚĂ" PRIVIND PROTECȚIA VIEȚII PRIVATE

publicate de Departamentul Comerțului al Statelor Unite ale Americii la 21 iulie 2000

Directiva europeană privind protecția datelor (denumită în continuare „directiva"), care constituie un cadru legislativ detaliat în ceea ce privește protecția vieții private, a intrat în vigoare la 25 octombrie 1998. Aceasta prevede că datele cu caracter personal nu pot fi transferate decât către țări terțe care asigură un nivel „adecvat" de protecție a vieții private. Deși Statele Unite ale Americii și Uniunea Europeană au ca obiectiv comun asigurarea unei mai bune protecții a vieții private a cetățenilor lor, Statele Unite ale Americii abordează în mod diferit acest domeniu față de Uniunea Europeană. Statele Unite ale Americii utilizează o abordare sectorială care se bazează pe un ansamblu de dispoziții legislative, regulamente și coduri de auto-reglementare. Date fiind aceste diferențe, multe organizații din Statele Unite ale Americii și-au exprimat incertitudinea cu privire la impactul „nivelului adecvat de protecție" cerut de Uniunea Europeană asupra transferurilor de date cu caracter personal din Uniunea Europeană către Statele Unite ale Americii.

Pentru a reduce această incertitudine și pentru a oferi un cadru mai clar pentru astfel de transferuri de date, Departamentul Comerțului publică prezentul document („principiile") precum și „întrebările de bază" („FAQ") în calitate de autoritate competentă cu scopul de a stimula, promova și dezvolta comerțul internațional. Principiile au fost elaborate prin consultări cu întreprinderile și publicul larg în scopul facilitării comerțului și relațiilor de afaceri dintre Statele Unite ale Americii și Uniunea Europeană. Ele sunt destinate exclusiv organizațiilor din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană cu scopul de a permite acestor organizații să îndeplinească condițiile privind „sfera de siguranță" și prezumția de „nivel de protecție adecvat" pe care aceasta o creează. Deoarece principiile au fost concepute pentru a servi exclusiv acestui scop, adoptarea lor în alte scopuri ar putea fi inadecvată. Principiile nu pot înlocui dispozițiile naționale de punere în aplicare a directivei care se aplică prelucrării datelor cu caracter personal în statele membre.

Îndeplinirea sau nu a condițiilor privind „sfera de siguranță" rămâne la latitudinea organizațiilor, care dispun de diferite mijloace pentru a se conforma acestor condiții. Organizațiile care decid să adere la principii trebuie să le respecte pentru a obține și a păstra avantajele „sferei de siguranță" și trebuie să-și anunțe public decizia. De exemplu, în cazul în care o organizație participă la un program privind protecția confidențialității pus la punct de sectorul privat care aderă la principii, aceasta îndeplinește condițiile menționate anterior. De asemenea, organizațiile se pot conforma acestor condiții și prin elaborarea propriilor regulamente privind protecția datelor, cu condiția ca acestea să fie conforme cu principiile. Orice organizație care a optat pentru una din aceste două soluții și care încalcă principiile trebuie sancționată în conformitate cu articolul 5 din Federal Trade Commission Act care interzice practicile neloiale sau frauduloase, sau în conformitate cu altă lege de acest tip (a se vedea, în anexă, lista organismelor competente americane recunoscute de UE). Pe lângă aceasta, organizațiile care se supun unui ansamblu de dispoziții juridice, de reglementare, administrative sau de alt tip (ori unui ansamblu de reguli) care asigură o protecție eficientă a datelor cu caracter personal, pot, de asemenea, beneficia de avantajele „sferei de siguranță". În toate cazurile, fiecare organizație beneficiază de aceste avantaje de la data la care a notificat Departamentului Comerțului (sau reprezentantului acestuia) aderarea sa la principii, în conformitate cu recomandările stabilite în FAQ cu privire la autocertificare.

Aderarea la aceste principii poate fi limitată de: (a) cerințele privind securitatea națională, interesul public și respectarea legilor Statelor Unite ale Americii; (b) textele legislative, regulamentele administrative sau jurisprudența care creează obligații contradictorii sau prevăd autorizații exprese, cu condiția ca organizația care a recurs la o asemenea autorizație să poată demonstra că nerespectarea principiilor se limitează la măsurile necesare pentru garantarea intereselor legitime superioare pe care această autorizație urmărește să le servească; (c) excepțiile sau derogările prevăzute de directivă sau de legislația statului membru, cu condiția ca aceste excepții sau derogări să fie aplicate în contexte comparabile. În conformitate cu obiectivul de a consolida protecția vieții private, organizațiile trebuie să facă eforturi să aplice aceste principii integral și transparent, inclusiv să indice în codurile lor de protejare a vieții private domeniile în care excepțiile menționate la litera (b) de mai sus se vor aplica cu regularitate. Din același motiv, atunci când principiile și/sau legile Statelor Unite ale Americii permit organizațiilor să aleagă, acestea sunt invitate să opteze, în limita posibilului, pentru nivelul cel mai înalt de protecție.

Din motive practice sau de altă natură, unele organizații vor dori poate să aplice principiile ansamblului datelor lor, însă ele nu sunt obligate să le aplice decât pentru datele transferate ulterior aderării lor la „sfera de siguranță". Pentru integrarea acesteia, nu este necesară aplicarea principiilor la datele prelucrate manual. Organizațiile care doresc să beneficieze de avantajele „sferei de siguranță" pentru a accesa date ce provin din fișiere ale Uniunii Europene prelucrate manual trebuie să aplice principiile oricărei informații transferate după aderarea la principiile menționate anterior.

Organizațiile care doresc să extindă avantajele „sferei de siguranță” la informațiile cu caracter personal obținute din fișiere de tip „resurse umane” provenind din Uniunea Europeană pentru a le utiliza în cadrul unui raport de muncă trebuie să menționeze această intenție atunci când își autocertifică angajamentul la Departamentul Comerțului (sau la reprezentantul acestuia) și trebuie să se conformeze cerințelor stabilite în FAQ privind autocertificarea. De asemenea, organizațiile vor putea furniza garanțiile prevăzute la articolul 26 din directivă în cazul în care aplică principiile, în cadrul acordurilor încheiate în scris cu părțile care transferă date din Uniunea Europeană, dispozițiilor normative privind protecția vieții private, după ce celelalte dispoziții privind aceste contracte-tip sunt aprobate de Comisie și statele membre.

Se aplică legislația americană în ceea ce privește interpretarea și respectarea principiilor „sferei de siguranță” (inclusiv „întrebările de bază”) și a măsurilor de protecție a vieții private puse în aplicare de organizațiile care aderă la „sfera de siguranță”, cu excepția cazurilor în care organizațiile s-au angajat să coopereze cu autoritățile europene însărcinate cu protecția datelor. Cu excepția cazurilor în care se prevede altfel, sunt aplicabile toate dispozițiile „sferei de siguranță” și ale „întrebărilor de bază”.

Prin „date sau informații cu caracter personal” trebuie înțeles orice dată sau informație despre o persoană identificată sau identificabilă care intră în domeniul de aplicare al directivei, transferată din Uniunea Europeană către o organizație din Statele Unite ale Americii și înregistrată sub orice formă.

NOTIFICAREA

Orice organizație trebuie să informeze persoanele în cauză cu privire la motivele strângerii și utilizării informațiilor cu caracter personal, la modul în care pot contacta organizația pentru orice întrebări sau plângeri, la terții cărora le sunt comunicate informațiile, la opțiunile și mijloacele pe care organizația le oferă persoanelor în cauză pentru limitarea utilizării și divulgării acestor date. Notificarea trebuie formulată într-un limbaj clar și lizibil. Trebuie comunicată persoanelor în cauză atunci când acestea sunt invitate pentru prima dată să furnizeze informații cu caracter personal sau cât mai curând posibil după această invitație, dar, în orice caz, înainte ca datele să fie folosite într-un scop diferit de cel pentru care au fost inițial strânse sau prelucrate de organizația care a efectuat transferul sau înainte ca ele să fie comunicate pentru prima dată unui terț ([1]).

OPȚIUNEA

Orice organizație trebuie să ofere persoanelor în cauză posibilitatea de a decide (refuza) dacă informațiile lor cu caracter personal (a) pot fi divulgate unui terț ([1]) sau (b) pot fi utilizate într-un scop incompatibil cu scopul sau scopurile pentru care au fost inițial strânse sau într-un scop aprobat ulterior de persoana în cauză. Persoanele în cauză trebuie să dispună de mecanisme clare și vizibile, ușor accesibile și cu un cost rezonabil pentru a-și exercita opțiunea.

În ceea ce privește informațiile sensibile (de exemplu datele privind dosarul medical sau starea de sănătate a unei persoane, originea rasială sau etnică, opiniile politice, credințele religioase sau convingerile filosofice, apartenența sindicală sau orientarea sexuală), orice persoană trebuie să aibă în mod pozitiv sau expres posibilitatea de a decide (consimțământ) dacă datele pot fi divulgate unui terț sau pot fi utilizate într-un scop care diferă de obiectivul inițial pentru care au fost strânse sau într-un scop aprobat ulterior de persoana în cauză prin exercitarea dreptului de consimțământ. În orice caz, o organizație va considera drept informații sensibile orice informații primite de la un terț în cazul în care terțul arată că această informație este sensibilă și o tratează în consecință.

TRANSFERUL ULTERIOR

Pentru a divulga informații unui terț, organizațiile trebuie să aplice principiile notificării și opțiunii. Organizațiile care doresc pot transfera informații unui terț care acționează ca mandatar, în conformitate cu descrierea cuprinsă în nota finală, în cazul în care certifică în prealabil faptul că terțul subscrie la principiile „sferei de siguranță” sau se supune dispozițiilor directivei sau a altui mecanism care atestă nivelul adecvat de protecție sau în cazul în care încheie un acord scris cu acest terț prin care acesta se angajează să ofere cel puțin același nivel de protecție ca acela prevăzut în principii. În cazul în care organizația se conformează acestor cerințe, nu este considerată responsabilă (decât în cazul în care decide altfel) în cazul în care un terț căruia organizația îi transferă asemenea date le prelucrează într-un mod contrar dispozițiilor sau restricțiilor convenite, excepție făcând cazurile în care organizația avea cunoștință sau ar fi trebuit să aibă cunoștință de faptul că terțul le va prelucra într-un asemenea mod, iar organizația nu a luat măsurile necesare pentru a preveni sau a opri această prelucrare.

([1]) Nu este necesară notificarea sau opțiunea în cazul în care informațiile sunt comunicate unui terț care este însărcinat să îndeplinească sarcini în numele organizației și în conformitate cu instrucțiunile acesteia. Pe de altă parte, principiul transferului ulterior se aplică în asemenea cazuri.

SECURITATEA

Organizațiile care creează, administrează, utilizează sau difuzează date cu caracter personal trebuie să ia măsurile necesare pentru a preveni pierderea, utilizarea abuzivă, consultarea neautorizată, divulgarea, modificarea și distrugerea acestor date.

INTEGRITATEA DATELOR

Ținând seama de aceste principii, informațiile cu caracter personal trebuie să fie relevante pentru scopurile cărora le sunt destinate. O organizație nu poate prelucra date cu caracter personal într-un mod incompatibil cu scopul pentru care acestea au fost strânse sau cu scopurile aprobate ulterior de persoana în cauză. În limita acestor obiective, orice organizație trebuie să ia măsurile necesare pentru a asigura fiabilitatea datelor în raport cu utilizarea prevăzută, precum și acuratețea, exhaustivitatea și actualitatea lor.

ACCESUL

Persoanele trebuie să aibă acces la informațiile cu caracter personal pe care le deține în legătură cu ele o organizație și să le poată corecta, modifica sau șterge atunci când sunt incorecte, cu excepția cazurilor în care eforturile sau costurile ocazionate de acordarea dreptului de acces sunt disproporționate în raport cu riscurile pe care le creează pentru viața privată a persoanei în cauză sau a cazurilor în care ar fi încălcate drepturile altor persoane.

APLICAREA

Pentru o protecție eficientă a vieții private trebuie puse la punct mecanisme care să permită asigurarea respectării principiilor „sferei de siguranță”, posibilitatea de recurs pentru persoanele în cauză care au fost afectate de nerespectarea principiilor și de sancționare a organizațiilor care nu au respectat principiile atunci când s-au angajat să le aplice. Aceste mecanisme trebuie să includă cel puțin: (a) mecanisme independente de recurs, ușor accesibile și necostisitoare, care să permită studierea și rezolvarea oricăror plângeri și litigii care fac trimitere la principii, și acordarea de despăgubiri în cazurile prevăzute de legea aplicabilă sau de inițiativele din sectorul privat; (b) proceduri de monitorizare pentru verificarea exactității informațiilor și indicațiilor pe care societățile comerciale le furnizează cu privire la practicile lor în ceea ce privește protecția vieții private și pentru verificarea punerii în aplicare a acestor practici în conformitate cu declarațiile întreprinderilor; (c) declarații care obligă organizațiile care subscriu la principii să rezolve problemele care izvorăsc din nerespectarea principiilor și declarații care prevăd sancțiuni pentru contravenienți. Aceste sancțiuni trebuie să fie suficient de severe pentru a garanta respectarea principiilor.

ANEXĂ

Lista organismelor oficiale ale Statelor Unite ale Americii recunoscute de Uniunea Europeană

Uniunea Europeană recunoaște următoarele organisme guvernamentale ale Statelor Unite ale Americii ca fiind autorizate să analizeze plângeri și să beneficieze de asistență împotriva practicilor neloiale, precum și pentru despăgubirile pentru persoane în cazul nerespectării principiilor în vigoare în conformitate cu FAQ:

— Comisia Federală pentru Comerț, pe baza atribuțiilor care îi sunt conferite în temeiul articolului 5 din Federal Trade Commission Act;

— Departamentul Transporturilor, pe baza atribuțiilor care îi sunt conferite în temeiul titlului 49 din United States Code articolul 41712.

ANEXA II

ÎNTREBĂRI DE BAZĂ (FAQ)

FAQ 1 – Datele sensibile

Î: *O organizație trebuie să ofere întotdeauna o opțiune expresă (consimțământ) cu privire la datele sensibile?*

R: Nu, o asemenea opțiune nu este obligatorie atunci când prelucrarea: (1) este în interesul vital al persoanei în cauză sau al unei alte persoane; (2) este necesară pentru stabilirea unui drept sau a unei apărări în justiție; (3) este necesară în vederea acordării îngrijirii medicale sau a stabilirii unui diagnostic; (4) este efectuată în cadrul activităților legitime de către o fundație, o asociație sau orice alt organism cu scop nelucrativ și cu un obiectiv politic, filosofic, religios sau sindical și cu condiția ca prelucrarea să privească exclusiv membrii acestui organism sau persoanele care au contacte frecvente cu acesta în legătură cu scopurile sale, iar datele să nu fie comunicate unor terți fără consimțământul persoanelor în cauză; (5) este necesară pentru respectarea obligațiilor organizației în domeniul dreptului muncii; (6) are legătură cu date care sunt în mod clar făcute publice de către persoana în cauză.

FAQ 2 – Excepțiile jurnalistice

Î: *Ținând seama de garanțiile pe care le oferă Constituția Statelor Unite ale Americii în ceea ce privește libertatea presei și derogările din directivă cu privire la informațiile utilizate de jurnaliști, se aplică principiile „sferei de siguranță" informațiilor cu caracter personal strânse, păstrate sau difuzate în scopuri jurnalistice?*

R: Atunci când drepturile presei menționate la primul amendament al Constituției Statelor Unite ale Americii nu sunt compatibile cu protecția vieții private, primul amendament trebuie să primeze pentru activitățile persoanelor sau organizațiilor din Statele Unite ale Americii. Informațiile cu caracter personal care sunt strânse în vederea publicării, difuzării sau comunicării publice prin alte forme, indiferent dacă sunt utilizate sau nu, precum și informațiile care au fost publicate anterior și apoi arhivate nu sunt supuse principiilor „sferei de siguranță".

FAQ 3 – Responsabilitatea secundară

Î: *Furnizorii de servicii de internet (FSI), societățile de telecomunicații și alte organisme se supun principiilor „sferei de siguranță" atunci când se limitează la transmiterea, direcționarea, înlocuirea sau mascarea, pe seama altui organism, a informațiilor care pot să contravină acestor principii?*

R: Nu. La fel ca în cazul directivei, „sfera de siguranță" nu creează o responsabilitate secundară. În măsura în care un organism funcționează doar ca vector pentru datele transmise de terți și nu stabilește nici obiectivele și nici mijloacele de prelucrare a acestor date cu caracter personal, responsabilitatea sa nu este angajată.

FAQ 4 – Băncile de investiții și auditul

Î: *Activitățile auditorilor și ale băncilor de investiții pot presupune prelucrarea de date cu caracter personal fără consimțământul sau cunoștința persoanei. Care sunt circumstanțele în principiile notificării, opțiunii și accesului care permit aceasta?*

R: Băncile de investiții și auditorii pot prelucra informații fără cunoștința persoanei în cauză numai în măsura și pe perioada necesară îndeplinirii dispozițiilor de reglementare sau cerințelor legate de interesul general, precum și în alte circumstanțe în care aplicarea acestor principii ar aduce atingere intereselor legitime ale organismului. Aceste interese legitime includ supravegherea respectării de către societățile comerciale a obligațiilor lor legale, a activităților lor contabile legitime și a confidențialității care trebuie să fie respectată în contextul eventualelor achiziții, fuziuni, asociații în participațiune sau al altor tranzacții similare efectuate de băncile de investiții sau de auditori.

FAQ 5 – Rolul autorităților însărcinate cu protecția datelor [1]

Î: *Cum pot întreprinderile care doresc să coopereze cu autoritățile însărcinate cu protecția datelor din Uniunea Europeană (DPA) să își ia acest angajament și cum vor fi acestea puse în aplicare?*

R: În cadrul „sferei de siguranță", organizațiile din Statele Unite ale Americii care primesc date cu caracter personal din Uniunea Europeană trebuie să își ia angajamentul de a utiliza mecanisme eficiente pentru a garanta respectarea principiilor „sferei de siguranță". Mai exact, după cum prevede principiul punerii în aplicare, aceste mecanisme trebuie să prevadă: (a) căi de recurs pentru persoanele la care se referă aceste date; (b) proceduri de urmărire pentru verificarea veridicității afirmațiilor și declarațiilor pe care le fac organizațiile cu privire la respectarea vieții private și (c) dispoziții privind condițiile în care organizațiile trebuie să remedieze problemele care decurg din nerespectarea principiilor, precum și asumarea consecințelor care rezultă din aceasta. O organizație trebuie să îndeplinească literele (a) și (c) din principiul punerii în aplicare în cazul în care aderă la angajamentul de cooperare cu DPA menționat de prezenta FAQ.

O organizație își poate lua angajamentul de a coopera cu DPA declarând în certificarea sa de aderare la „sfera sa de siguranță" adresată Departamentului Comerțului (vezi FAQ 6 privind autocertificarea) că organizația:

1. decide să îndeplinească cerințele de la literele (a) și (c) ale principiului punerii în aplicare a „sferei de siguranță", luându-și angajamentul de a coopera cu DPA;

2. va coopera cu DPA la analizarea și soluționarea plângerilor înaintate în temeiul „sferei de siguranță";

3. va respecta orice aviz emis de DPA conform căruia organizația trebuie să adopte măsuri specifice în vederea respectării principiilor „sferei de siguranță", inclusiv măsuri de despăgubire sau reparație în beneficiul persoanelor afectate de nerespectarea principiilor, și va informa DPA în scris de măsurile adoptate în acest sens.

Cooperarea DPA-urilor se traduce prin informații și avize acordate în modul următor:

— DPA vor fi consultate prin intermediul unui comitet neoficial al DPA înființat la nivel european care, *inter alia*, va contribui la elaborarea unei abordări armonizate și coerente;

— comitetul va oferi sfaturi organizațiilor din Statele Unite ale Americii cu privire la plângerile nesoluționate din partea unor persoane privind prelucrarea informațiilor cu caracter personal care au fost transferate din Uniunea Europeană în temeiul „sferei de siguranță". Aceste sfaturi au ca obiectiv asigurarea unei aplicări corecte a principiilor „sferei de siguranță" și privesc, de asemenea, mecanismele de reglementare a litigiilor pe care DPA le consideră corespunzătoare pentru persoana (persoanele) în cauză;

— comitetul își va da avizul ca răspuns la trimiterile organizațiilor în cauză și/sau la plângerile introduse direct de persoane fizice împotriva organizațiilor care și-au luat angajamentul de a coopera cu DPA în sensul respectării principiilor „sferei de siguranță", încurajând și ajutând, după caz, aceste persoane fizice să utilizeze mai întâi mecanismele interne de instrumentare a plângerilor pe care le oferă organizația;

— avizul va fi emis numai după ce ambele părți au avut posibilitatea de a-și prezenta observațiile și, după caz, de a aduce toate dovezile pe care doresc să le prezinte. Comitetul va încerca să emită avizul cât mai repede posibil, respectând totodată principiile procesului echitabil. În principiu, comitetul se va pronunța în termen de cel mult 60 de zile de la primirea plângerii sau a trimiterilor;

— în cazul în care consideră necesar, comitetul va face publice rezultatele analizelor plângerilor care îi sunt înaintate;

— avizul comitetului nu creează obligații pentru comitet sau pentru oricare dintre DPA.

[1] Includerea acestei FAQ în acord depinde de acordul DPA-urilor. Acestea au examinat prezentul text în cadrul grupului de lucru menționat la articolul 29 și cele mai multe dintre ele l-au considerat acceptabil, dar încă nu doresc să se pronunțe definitiv decât în contextul avizului global pe care grupul de lucru îl va emite în acordul final.

Organizațiile care optează pentru acest mod de soluționare a litigiilor trebuie să-și ia angajamentul de a se conforma avizului emis de DPA. În cazul în care o organizație nu se conformează în termen de 25 de zile de la notificarea avizului și nu oferă o explicație satisfăcătoare, comitetul ar putea decide să înainteze cauza către Comisia Federală pentru Comerț sau către un alt organism de reglementare din Statele Unite ale Americii menționat în anexa la principiile „sferei de siguranță" sau să constate că angajamentul de cooperare a fost grav încălcat și prin urmare trebuie considerat nul și neavenit. În acest ultim caz, comitetul informează Departamentul Comerțului (sau pe reprezentantul acestuia) astfel încât lista participanților la „sfera de siguranță" să poată fi modificată în consecință. Orice încălcare a angajamentului de cooperare cu comitetul, precum și orice nerespectare a principiilor „sferei de siguranță" se consideră elemente constitutive ale unui act fraudulos în temeiul articolului 5 din Federal Trade Commission Act sau în temeiul unui text legislativ similar.

Organizațiile care optează pentru această formulă trebuie să plătească o cotizație anuală care să acopere costurile de gestionare ale comitetului și, după caz, vor fi invitate să participe la costurile pentru traducerile pe care le presupune analizarea de către comitet a acțiunilor și a plângerilor depuse împotriva lor. Cotizația anuală nu poate depăși 500 USD, iar în cazul societăților comerciale mai mici se acordă o reducere.

Posibilitatea cooperării cu DPA este oferită organizațiilor care aderă la „sfera de siguranță" în cursul unei perioade de trei ani. DPA va revizui dispozițiile înainte de expirarea acestei perioade în cazul în care numărul de organizații din Statele Unite ale Americii care optează pentru această formulă se dovedește a fi excesiv.

FAQ 6 – Autocertificarea

Î: *Cum autocertifică o organizație faptul că aderă la principiile „sferei de siguranță"?*

R: Avantajele „sferei de siguranță" sunt asigurate de la data la care o organizație autocertifică Departamentului Comerțului (sau reprezentantului acestuia) că aderă la principii în conformitate cu normele de mai jos.

Pentru autocertificarea aderării la „sfera de siguranță", organizațiile pot adresa Departamentului Comerțului (sau reprezentantului acestuia) o scrisoare semnată de un funcționar al organizației care trebuie să conțină cel puțin următoarele informații:

1. numele organizației, adresa poștală, adresa electronică, numerele de telefon și de fax ale acesteia;

2. descrierea activităților organizației cu privire la informațiile cu caracter personal primite din Uniunea Europeană;

3. descrierea dispozițiilor organizației cu privire la protecția vieții private în cazul informațiilor menționate anterior, precizând: (a) locul în care textul acestor dispoziții poate fi consultat de către public; (b) data punerii în aplicare a acestor dispoziții; (c) serviciul care poate fi contactat pentru rezolvarea plângerilor, pentru cererile de acces sau pentru orice altă problemă legată de „sfera de siguranță"; (d) denumirea instanței de reglementare specifice care este însărcinată să hotărască în privința plângerilor depuse, după caz, împotriva organizației pentru practici neloiale sau frauduloase și pentru încălcări ale legilor sau reglementărilor privind protecția vieții private (și care este menționată în anexa la principii); (e) numele oricărui program privind protecția vieții private la care participă organizația; (f) metoda de verificare (de exemplu internă sau printr-un terț) [1] și (g) instanța independentă de recurs care poate ancheta plângerile nesoluționate.

O organizație poate extinde avantajele „sferei sale de siguranță" la informații de tip „resurse umane" transferate din UE pentru a fi utilizate în cadrul raporturilor de muncă, atunci când una dintre instanțele de reglementare menționată în anexa la principii are competența de a ancheta plângerile depuse, după caz, împotriva organizației menționate în domeniul informațiilor de tip „resurse umane". Pe lângă aceasta, organizația trebuie să indice în scrisoarea sa de autocertificare că dorește acest lucru, că se angajează să coopereze cu autoritățile competente ale Uniunii Europene în conformitate cu FAQ 9 și FAQ 5 și că se conformează sfaturilor date de aceste autorități.

Departamentul (sau reprezentantul acestuia) va păstra o listă a tuturor organizațiilor care urmează această procedură, garantând astfel avantajele „sferei de siguranță", și va actualiza această listă pe baza scrisorilor și notificărilor anuale primite în conformitate cu FAQ 11. Aceste scrisori de autocertificare vor fi trimise cel puțin o dată pe an. În caz contrar, organizația va fi ștearsă de pe listă și avantajele „sferei de siguranță" nu îi vor mai fi asigurate. Lista și scrisorile de autocertificare prezentate de organizații vor fi făcute publice. Orice

[1] A se vedea FAQ 7 cu privire la verificare.

organizațiile care își autocertifică aderarea la principiile „sferei de siguranță” trebuie, de asemenea, să indice în declarațiile sale publice referitoare la politica sa în ceea ce privește protecția vieții private faptul că aderă la principiile „sferei de siguranță”.

Angajamentul de aderare la principii nu este limitat în timp în ceea ce privește datele primite pe perioada în care organizația beneficiază de avantajele „sferei de siguranță”. Angajamentul luat de o organizație înseamnă că va continua să aplice principiile acestor date pe toată perioada în care organizația le păstrează, le utilizează sau le divulgă, chiar dacă părăsește ulterior, dintr-un motiv sau altul, „sfera de siguranță”.

Atunci când o organizație încetează să existe ca persoană juridică distinctă, ca urmare a unei fuziuni sau absorbții, trebuie să notifice înainte acest lucru Departamentului Comerțului (sau reprezentantului acestuia). Notificarea trebuie, de asemenea, să indice dacă entitatea care o absoarbe sau entitatea care rezultă în urma fuziunii (1) rămâne supusă în continuare principiilor „sferei de siguranță” în virtutea dispozițiilor juridice care reglementează absorbția sau fuziunea sau (2) decide să-și autocertifice aderarea la principiile „sferei de siguranță” sau oferă alte garanții, ca de exemplu un acord scris privind aderarea sa la aceste principii. În cazul în care nu este pusă în aplicare nici una dintre soluțiile menționate la punctele (1) și (2), orice date care au fost obținute în cadrul „sferei de siguranță” trebuie șterse fără întârziere.

O organizație nu este obligată să aplice principiile „sferei de siguranță” tuturor informațiilor cu caracter personal, dar trebuie să supună principiilor „sferei de siguranță” ansamblul datelor cu caracter personal primite de la Uniunea Europeană după aderarea sa la „sfera de siguranță”.

Orice declarație falsă adresată publicului general cu privire la aderarea unei organizații la principiile „sferei de siguranță” poate da naștere unei acțiuni intentate la Comisia Federală pentru Comerț sau altă instanță administrativă competentă. Orice declarație falsă adresate Departamentului Comerțului (sau reprezentantului acestuia) poate da naștere unei acțiuni intentate în temeiul legii privind declarațiile false (18 U.S.C., articolul 1001).

FAQ 7 – Verificarea

Î: *Care sunt practicile de monitorizare utilizate de organizații pentru a verifica dacă atestările și declarațiile întreprinderilor cu privire la practicile lor în ceea ce privește protecția vieții private în cadrul „sferei de siguranță” sunt adevărate și dacă aceste practici au fost puse în aplicare în conformitate cu declarațiile acestora și cu principiile „sferei de siguranță”?*

R: Pentru a răspunde cerințelor de verificare a principiului punerii în aplicare, organizațiile pot să verifice asemenea atestări și declarații prin organizarea unei autoevaluări sau a unui control extern al conformității.

În cadrul autoevaluării, verificarea ar trebui să indice faptul că politica privind protecția vieții private, în ceea ce privește informațiile cu caracter personal primite de la Uniunea Europeană, care este făcută publică de organizație, este exactă, completă, prezentată în mod vizibil, pusă în aplicare în totalitate și accesibilă. De asemenea, ar trebui să arate că această politică este conformă cu principiile „sferei de siguranță”, că persoanele sunt informate de existența mecanismelor interne de rezolvare a plângerilor și a mecanismelor independente prin intermediul cărora pot depune plângeri, că organizația dispune de proceduri de formare a angajaților în acest scop și de sancționare a acestora în cazul în care nu le respectă, și că există proceduri interne privind controlul obiectiv și periodic al respectării acestei politici. O declarație care verifică autoevaluarea trebuie semnată cel puțin o dată pe an, de către un funcționar al organizației sau de un alt reprezentant autorizat al acesteia și trebuie pusă la dispoziția persoanelor în cauză la cerere sau în cadrul unei anchete sau al unei plângeri pentru neconformitate.

Organizațiile trebuie să păstreze arhive privind punerea în aplicare a practicilor lor cu privire la protecția vieții private în „sfera de siguranță” și să le pună la dispoziție, la cerere, organismului independent însărcinat cu analizarea reclamațiilor sau agenției cu competență în materie de practici neloiale și frauduloase, în cadrul unei anchete sau al unei plângeri pentru neconformitate.

În cazul în care organizația optează pentru controlul extern al conformității, acest control trebuie să demonstreze că politica organizației în ceea ce privește protecția vieții private cu privire la informațiile primite de la Uniunea Europeană respectă principiile „sferei de siguranță”, că această politică este respectată și că persoanele sunt informate cu privire la mecanismele prin care își pot depune plângerile. Metodele de control sunt diverse și pot include (listă neexhaustivă) un audit, o verificare aleatorie, utilizarea de „momeli” sau diferite alte instrumente tehnologice. O declarație care confirmă că a fost efectuat un control extern al conformității

trebuie semnată, cel puțin o dată pe an, de către cel care a efectuat controlul, de către responsabilul organizației sau de către orice alt reprezentat al acesteia și trebuie transmisă, la cerere, persoanelor în cauză sau în cadrul unei anchete sau al unei reclamații pentru neconformitate.

FAQ 8 – Accesul

Principiul accesului:

Orice persoană trebuie să aibă acces la informațiile cu caracter personal pe care le deține o organizație despre ea și să poată corecta, modifica sau șterge aceste informații în cazul în care sunt inexacte, cu excepția cazurilor în care acest acces nu implică o dificultate sau costuri disproporționate în raport cu riscurile la adresa protecției vieții private a persoanei în cauză sau încălcarea drepturilor legitime ale unor terți.

Î 1: *Dreptul de acces este absolut?*

R 1: Nu. În conformitate cu principiile „sferei de siguranță", dreptul de acces este fundamental pentru protecția vieții private. Acesta permite fiecărei persoane să verifice acuratețea informațiilor care îl privesc. Cu toate acestea, obligația care incumbă unei organizații de a oferi acces la informațiile cu caracter personal pe care le deține depinde de principiul proporționalității sau de caracterul rezonabil al cererii de acces și trebuie limitată în anumite cazuri. Într-adevăr, expunerea de motive la liniile directoare ale OCDE privind protecția vieții private (1980) specifică faptul că obligația unei organizații de a asigura accesul nu este absolută. Dreptul de acces nu necesită o investigare la fel de aprofundată ca, de exemplu, pentru o citație și nici nu înseamnă acces la toate formele de păstrare a datelor de către organizație.

Experiența a arătat că, atunci când răspunde cererilor de acces individuale, organizația trebuie, înainte de toate, să fie ghidată de motivul (motivele) autorului solicitării. De exemplu, în cazul în care o cerere de acces este vagă sau extrem de amplă, organizația poate iniția un dialog cu solicitantul pentru a înțelege mai bine motivele acestui demers și pentru a găsi informațiile pertinente. Organizația poate încerca să stabilească cu care din serviciile organizației a avut contacte persoana în cauză și/sau care este natura (sau utilizarea) informațiilor care fac obiectul cererii de acces. Cu toate acestea, nimeni nu este obligat să justifice o cerere de acces cu privire la propriile date.

Costurile și dificultatea sunt factori importanți care trebuie luați în considerare, dar care nu au un rol decisiv în stabilirea caracterului rezonabil al accesului. Astfel, în conformitate cu celelalte dispoziții din prezentele FAQ, în cazul în care informațiile sunt utilizate în scopul luării unor decizii care vor avea consecințe importante asupra persoanei în cauză (de exemplu, refuzarea sau acordarea unor avantaje importante, precum o asigurare, o ipotecă sau un loc de muncă), atunci organizația trebuie să le comunice, chiar dacă acest lucru este destul de dificil sau presupune costuri ridicate.

Atunci când informațiile solicitate nu sunt sensibile sau nu sunt utilizate în scopul luării unor decizii care vor avea consecințe importante asupra persoanei în cauză (de exemplu, date de marketing care nu sunt sensibile, utilizate pentru trimiterea de cataloage), dar sunt ușor accesibile iar transmiterea lor este puțin costisitoare, organizația trebuie să permită oricărei persoane accesul la informațiile factuale care privesc persoana respectivă. Informațiile în cauză pot include date obținute de la persoană, date obținute în urma unei tranzacții sau date transmise de terți care au avut o legătură cu persoana în cauză.

Dreptul la acces fiind un element fundamental al protecției vieții private, organizațiile trebuie să facă întotdeauna eforturi de bună credință pentru a furniza accesul. De exemplu, în cazul în care anumite informații trebuie protejate și pot fi separate cu ușurință de informațiile care fac obiectul unei cereri de acces, organizația trebuie să separe datele confidențiale și să răspundă la cerere făcând disponibile celelalte informații. În cazul în care organizația decide să refuze accesul într-un anumit caz, aceasta trebuie să își motiveze decizia și să comunice datele unei persoane de contact pentru informații suplimentare.

Î 2: *Ce sunt informațiile comerciale confidențiale și organizațiile pot refuza accesul la acestea din motive de salvgardare?*

R 2: Informațiile comerciale confidențiale (în sensul Codului federal de procedură privind comunicarea de date) sunt informații pe care o organizație veghează să nu fie divulgate întrucât ar favoriza concurenții săi de pe piață. Poate fi vorba de un anumit program de calculator (de exemplu un program de modelare) sau detaliile despre acest program. În cazul în care informațiile comerciale confidențiale pot fi separate ușor de informațiile care fac obiectul unei cereri de acces, organizația trebuie să separe datele confidențiale și să răspundă

la cerere. Organizațiile pot refuza sau limita accesul în cazul în care acordarea acestuia ar conduce la divulgarea propriilor sale informații comerciale confidențiale, în sensul definiției de mai sus – în special concluziile sau clasificările comerciale stabilite de organizație – sau a informațiilor comerciale confidențiale aparținând altor organizații, în cazul în care aceste informații fac obiectul unei obligații contractuale de confidențialitate în cazurile în care o asemenea obligație ar fi în mod normal pusă în aplicare sau impusă.

Î 3: *Atunci când acordă accesul, o organizație poate comunica persoanelor în cauză informații cu caracter personal extrase din bazele sale de date sau poate permite accesul la această bază de date?*

R 3: Accesul poate fi furnizat sub forma unui transfer de informații către persoana în cauză și nu implică obligatoriu consultarea bazei de date a organizației.

Î 4: *Organizația trebuie să-și restructureze bazele de date pentru a permite accesul?*

R 4: Accesul trebuie furnizat numai în măsura în care organizația stochează informațiile. Principiul accesului în sine nu creează nici o obligație de conservare, gestionare, reorganizare sau restructurare a fișierelor care cuprind informații cu caracter personal.

Î 5: *Aceste răspunsuri stabilesc în mod clar că accesul poate fi refuzat în anumite circumstanțe. În ce alte circumstanțe poate refuza o organizație acordarea unei persoane dreptul de acces la informațiile cu caracter personal?*

R 5: Aceste circumstanțe sunt limitate, iar motivele pentru care accesul este refuzat trebuie specificate. Organizația poate refuza accesul la anumite informații în măsura în care difuzarea acestora riscă să aducă atingere unor importante interese publice, cum ar fi siguranța națională, apărarea sau siguranța publică. Atunci când informațiile cu caracter personal sunt prelucrate exclusiv în scopuri statistice sau de cercetare, accesul poate fi, de asemenea, refuzat. Alte motive pentru refuzarea sau restricționarea accesului:

a. o barieră în calea execuției sau punerii în aplicare a legii, inclusiv în calea prevenirii criminalității, detectării și anchetării infracțiunilor și delictelor sau în calea dreptului la un proces echitabil;

b. o barieră în calea acțiunilor civile în justiție, inclusiv în calea prevenirii și detectării acțiunilor în justiție și în calea dreptului la un proces echitabil;

c. difuzarea de informații care fac referință la una sau mai multe alte persoane în cazul în care aceste informații nu pot fi prelucrate;

d. încălcarea unui privilegiu sau a unei obligații legale sau profesionale;

e. încălcarea confidențialității necesare în cadrul negocierilor viitoare sau în curs, precum cele privind achiziționarea de societăți comerciale cotate la Bursă;

f. o barieră în calea anchetelor privind la securitatea angajaților și a procedurilor de arbitraj;

g. compromiterea confidențialității care poate fi necesară pe perioade limitate în legătură cu organizarea înlocuirilor și a restructurărilor;

h. faptul de a aduce atingere confidențialității care poate fi necesară în legătură cu funcțiile de control, de inspecție sau de reglementare în raport cu o gestiune economică sau financiară sănătoasă sau

i. alte circumstanțe în care accesul ar atrage o dificultate sau costuri disproporționate și în care ar avea loc încălcarea drepturilor sau intereselor legitime ale terților.

Organizația care invocă o excepție trebuie demonstreze aplicabilitatea acesteia (după cum se întâmplă în mod normal). După cum s-a arătat deja, solicitanților trebuie să li se indice motivele pentru refuzul sau restricționarea accesului și datele unei persoane de contact pentru informații suplimentare.

Î 6: *O organizație poate solicita o taxă pentru acordarea accesului pentru a-și acoperi cheltuielile?*

R 6: Da. Liniile directoare ale OCDE prevăd că organizațiile pot solicita o redevență, cu condiția ca aceasta să nu fie excesivă. Așadar, organizațiile pot stabili o participație echitabilă la cheltuielile de acces. Această taxă poate contribui și la descurajarea solicitărilor repetate și vexatorii.

Organizațiile specializate în vânzarea de informații accesibile publicului pot solicita taxa practicată în mod obișnuit de organizație ca răspuns la cererile de acces. De asemenea, fiecare persoană poate obține informațiile care o privesc adresându-se direct primei organizații care a adunat inițial datele.

Accesul nu poate fi refuzat pe motive legate de costuri în cazul în care persoana în cauză se oferă să plătească cheltuielile.

Î 7: *O organizație este obligată să permită accesul la informațiile cu caracter personal extrase din registrele publice?*

R 7: Trebuie precizat, întâi de toate, că registrele publice sunt registre păstrate de autorități guvernamentale sau de alte administrații publice la orice nivel și care pot fi consultate de publicul larg. Nu este necesar să se aplice principiile accesului în cazul acestor informații în cazul în care acestea nu sunt asociate cu alte date cu caracter personal, exceptând cazurile în care cantități mici de informații care nu au caracter public sunt utilizate pentru indexarea sau organizarea registrelor publice. Cu toate acestea, trebuie respectate condițiile privind consultarea acestora stabilite de instanțele competente. Atunci când informații din aceste registre sunt asociate cu alte date care nu au caracter public (altele decât cele menționate mai sus), organizația trebuie să permită accesul la aceste informații, în cazul în care aceste informații nu fac obiectul altor derogări.

Î 8: *Principiul accesului trebuie aplicat informațiilor cu caracter personal accesibile publicului?*

R 8: La fel ca în cazul informațiilor extrase din registrele publice (a se vedea Î 7), nu este necesar să se acorde accesul la informații care sunt deja disponibile publicului, atâta timp cât acestea nu sunt asociate cu alte date care nu sunt disponibile publicului.

Î 9: *Ce măsuri de protecție poate lua organizația împotriva solicitărilor repetate sau vexatorii?*

R 9: Organizația nu este obligată să răspundă la asemenea cereri de acces. Din acest motiv poate solicita plata unei taxe echitabile și poate stabili o limită acceptabilă a numărului de cereri de acces depuse într-o perioadă de timp dată. Atunci când stabilește aceste limite, organizația trebuie să ia în considerare factori precum frecvența actualizării informațiilor, scopul în care sunt utilizate datele și natura informațiilor.

Î 10: *Cum se poate proteja organizația împotriva cererilor de acces frauduloase?*

R 10: Organizația nu este obligată să ofere accesul în cazul în care nu primește informațiile necesare pentru identificarea solicitantului.

Î 11: *Există o limită de timp în care trebuie să se răspundă cererilor de acces?*

R 11: Da, organizațiile trebuie să răspundă într-un termen rezonabil. Această condiție poate fi îndeplinită în moduri diferite, conform expunerii de motive la liniile directoare ale OCDE privind protecția vieții private (din 1980). Astfel, un responsabil de date care furnizează cu regularitate informații persoanelor în cauză poate fi scutit de obligația de a răspunde imediat cererilor individuale.

FAQ 9 – Resursele umane

Î 1: *Sunt incluse în „sfera de siguranță" transferurile din Uniunea Europeană către Statele Unite ale Americii de informații cu caracter personal strânse în cadrul unui raport de muncă?*

R 1: Da, în cazul în care o societate comercială din Uniunea Europeană transferă informații cu caracter personal despre foștii sau actualii săi angajați și care au fost strânse în cadrul unui raport de muncă către o societate-mamă, afiliată sau neafiliată, care prestează servicii în Statele Unite ale Americii și care aderă la

principiile „sferei de siguranță”, acest transfer beneficiază de avantajele „sferei de siguranță”. În acest caz, colectarea de informații precum și prelucrarea lor înainte de transfer sunt supuse legilor naționale ale statului membru al Uniunii Europene în care are loc colectarea și toate condițiile sau restricțiile stabilite în domeniu de acesta trebuie să fie respectate.

Principiile „sferei de siguranță” sunt relevante numai în caz de transfer sau de acces la dosare identificate individual. Declarația statistică bazată pe date globale cu privire la ocuparea forței de muncă și/sau utilizarea datelor anonime sau pseudoanonime nu prezintă riscuri pentru viața privată.

Î 2: *Cum se aplică principiile notificării și opțiunii în cazul acestor date?*

R 2: O organizație din Statele Unite ale Americii care a primit din Uniunea Europeană informații despre angajați în cadrul „sferei de siguranță” le poate comunica unor terți și/sau le poate utiliza în alte scopuri numai în cazul în care principiul notificării și opțiunii sunt respectate. De exemplu, în cazul în care o organizație intenționează să utilizeze informațiile cu caracter personal strânse în cadrul unui raport de muncă într-un scop care nu are legătură cu acest raport de muncă – cum ar fi trimiterea de mesaje de marketing –, organizația trebuie în prealabil să lase persoanelor în cauză posibilitatea opțiunii, exceptând cazurile în care acestea și-au dat deja acceptul pentru utilizarea acestor informații în astfel de scopuri. Pe lângă aceasta, angajatorul nu poate utiliza opțiunile exprimate pentru a împiedica dezvoltarea carierei profesionale a angajaților săi sau pentru a lua sancțiuni împotriva lor.

Trebuie remarcat că anumite condiții cu aplicabilitate generală cu privire la transferul din unele state membre pot exclude alte utilizări ale acestor informații chiar și după transferul lor în afara Uniunii Europene, iar aceste condiții trebuie respectate.

De asemenea, angajatorii ar trebui să facă toate eforturile posibile pentru a ține seama de preferințele angajatului cu privire la protecția vieții sale private. Aceasta poate include restricționarea accesului la date, transformarea anumitor date în anonime sau atribuirea de coduri sau pseudonime atunci când numele reale nu sunt necesare în scopuri administrative.

În măsura și pe durata necesară, pentru a evita lezarea intereselor legitime ale organizației în cadrul promovărilor, angajamentelor sau altor decizii similare privind ocuparea forței de muncă, o organizație nu este obligată să respecte principiul notificării și pe cel al opțiunii.

Î 3: *Cum se aplică principiul accesului?*

R 3: Întrebările de bază referitoare la principiul accesului oferă indicații cu privire la motivele care pot justifica refuzarea sau limitarea accesului solicitat în contextul resurselor umane. Desigur, angajatorii din Uniunea Europeană trebuie să se conformeze regulamentelor locale și să se asigure că salariații din Uniunea Europeană au acces la aceste informații în conformitate cu legile din țările lor, indiferent de locul în care datele sunt prelucrate și păstrate. În contextul „sferei de siguranță” o organizație care prelucrează asemenea date în Statele Unite ale Americii trebuie să coopereze prin furnizarea acestui acces, fie direct, fie prin angajatorul din Uniunea Europeană.

Î 4: *Cum este asigurată punerea în aplicare cu privire la datele referitoare la salariați în cadrul „sferei de siguranță”?*

R 4: În măsura în care informațiile sunt utilizate numai în cadrul unui raport de muncă, responsabilitatea principală pentru date față de angajat revine societății comerciale din Uniunea Europeană. Din acest motiv, în cazul în care un salariat european depune o plângere cu privire la încălcarea dreptului său la protecția datelor și nu este mulțumit de rezultatele procedurilor interne de evaluare, de reclamație și de apel (sau orice procedură de arbitraj aplicabilă în temeiul unui contract încheiat cu un sindicat), trebuie orientat spre autoritățile naționale responsabile de problemele de muncă sau de protecția datelor în jurisdicția în care muncește angajatul. Aceasta include, de asemenea, cazurile în care pretinsa utilizare necorespunzătoare a informațiilor cu caracter personal a avut loc în Statele Unite ale Americii și este responsabilitatea organizației din Statele Unite ale Americii care a primit informațiile de la angajator, nu a angajatorului și prin urmare implică o pretinsă violare a principiilor „sferei de siguranță” și nu a actelor naționale cu putere de lege de transpunere a directivei. Acesta este modul cel mai eficient de soluționare a suprapunerilor care există adesea între drepturile și obligațiile stabilite de legislația muncii și de convențiile colective de muncă locale, precum și de legislația privind protecția datelor.

O organizație din Statele Unite ale Americii care aderă la principiile „sferei de siguranță” și care utilizează date din Uniunea Europeană privind resursele umane transferate din Uniunea Europeană în cadrul unui raport de muncă și care dorește ca aceste transferuri să fie reglementate de „sfera de siguranță” trebuie să își ia angajamentul în acest sens de a coopera la anchetele autorităților competente din Uniunea Europeană și să respecte avizele acestora. Autoritățile însărcinate cu protecția datelor care au consimțit să coopereze în acest

sens vor informa Comisia Europeană și Departamentul Comerțului. În cazul în care o organizație din Statele Unite ale Americii care aderă la principiile „sferei de siguranță” dorește să transfere date privind resursele umane dintr-un stat membru în care autoritatea însărcinată cu protecția datelor nu a încheiat un astfel de acord, se aplică dispozițiile de la FAQ 5.

FAQ 10 – Contracte în temeiul articolului 17

Î: *Transferul de date din Uniunea Europeană în Statele Unite ale Americii efectuat doar în scopul prelucrării necesită un contract independent de participarea responsabilului cu prelucrarea datelor la „sfera de siguranță”?*

R: Da. Responsabilii cu prelucrarea datelor din Uniunea Europeană au întotdeauna obligația de a încheia un contract când are loc un transfer pentru prelucrare de date, indiferent dacă această operațiune este efectuată în Uniunea Europeană sau în afara acesteia. Scopul contractului este de a proteja interesele responsabilului cu prelucrarea datelor, adică persoana sau organismul care stabilește obiectivele și mijloacele de procesare și care poartă întreaga responsabilitate pentru date față de persoanele în cauză. Prin urmare, contractul specifică prelucrarea care urmează să fie efectuată și măsurile necesare pentru a garanta siguranța datelor.

În consecință, o organizație din Statele Unite ale Americii reglementată de „sfera de siguranță” și care primește informații cu caracter personal din Uniunea Europeană pentru prelucrare nu este obligată să aplice principiile față de aceste informații deoarece responsabilul de prelucrarea datelor din Uniunea Europeană rămâne responsabil față de persoanele în cauză, în conformitate cu dispozițiile comunitare din domeniu (care pot fi mai riguroase decât principiile echivalente ale „sferei de siguranță”).

Întrucât participanții la „sfera de siguranță” asigură o protecție adecvată a datelor, contractele de prelucrare încheiate cu aceștia nu necesită o autorizație prealabilă (sau această autorizație este acordată automat de statele membre), contrar contractelor ai căror beneficiari nu participă la „sfera de siguranță” sau nu asigură o protecție adecvată.

FAQ 11 – Soluționarea litigiilor și punerea în aplicare a deciziilor

Î: *Cum trebuie puse în aplicare cerințele privind soluționarea litigiilor formulate în principiul punerii în aplicare și ce măsuri vor fi luate în cazul nerespectării repetate a principiilor de către o organizație?*

R: Principiul punerii în aplicare stabilește cerințele pentru punerea în aplicare a „sferei de siguranță”. Modul în care sunt îndeplinite cerințele de la litera (b) a principiului este prezentat în FAQ privind verificarea (FAQ 7). Prezenta FAQ 11 vizează literele (a) și (c), ambele necesitând instanțe de recurs independente. Aceste instanțe pot lua forme diferite, dar trebuie să îndeplinească cerințele principiului punerii în aplicare. Organizațiile care participă la „sfera de siguranță” pot satisface aceste cerințe în următoarele moduri: (1) participând la programele organizate de sectorul privat cu privire la protecția vieții private care integrează principiile „sferei de siguranță” în normele lor și care includ mecanisme de punere în aplicare eficiente de tipul celor descrise în principiul punerii în aplicare; (2) conformându-se instrucțiunilor organelor de supraveghere sau de reglementare legale care asigură prelucrarea plângerilor persoanelor și soluționarea litigiilor; (3) luându-și angajamentul de a coopera cu autoritățile însărcinate cu protecția datelor în cadrul Uniunii Europene sau cu reprezentanții autorizați ale acestora. Prezenta listă are valoare ilustrativă și nu este restrictivă. Sectorul privat poate elabora alte mecanisme de punere în aplicare, cu condiția ca acestea să întrunească cerințele principiului punerii în aplicare și ale FAQ. Trebuie remarcat faptul că cerințele principiului punerii în aplicare vin în completarea cerinței stabilite la paragraful al treilea din introducerea la principii, în conformitate cu care inițiativele de autoreglementare trebuie să fie aplicate în conformitate cu articolul 5 din Federal Trade Commission Act sau cu o lege similară.

Instanțe de recurs

Consumatorii ar trebui să fie încurajați să adreseze eventualele plângeri organizației în cauză înainte de a face apel la instanțe de recurs independente. Independența unei instanțe de recurs se apreciază în funcție de criterii obiective, cum ar fi transparența componenței sale și a finanțării sau un bilanț pozitiv în domeniul său de

activitate. În conformitate cu principiul punerii în aplicare, recursul disponibil persoanelor particulare trebuie să fie ușor disponibile și accesibile financiar. Organismele de instrumentare a litigiilor trebuie să analizeze fiecare plângere primită de la persoane particulare, exceptând cazurile în care acestea sunt în mod evident nefondate sau abuzive. Această condiție nu împiedică stabilirea, de către instanța de recurs, de criterii de eligibilitate, însă acestea trebuie să fie transparente și justificate (de exemplu, excluderea plângerilor care nu intră în domeniul de aplicare al programului sau care sunt de competența altei instanțe) și nu trebuie să aibă ca rezultat compromiterea angajamentului de a analiza plângerile legitime. Pe lângă aceasta, instanțele de recurs trebuie să ofere persoanelor particulare informații complete și ușor accesibile cu privire la modul în care funcționează procedura de soluționare a litigiilor când acestea depun o plângere. Aceste informații trebuie să includă o descriere a practicilor aplicate în materie de protecție a vieții private, în conformitate cu principiile „sferei de siguranță" ([1]). De asemenea, instanțele trebuie să coopereze pentru a pune la punct instrumente, cum ar fi formularele tip pentru plângeri, pentru a facilita procedura de soluționare a litigiilor.

Recursuri și sancțiuni

Orice recurs la organismul de instrumentare a litigiilor ar trebui să ducă la anularea sau corectarea, în măsura în care este posibil, a efectelor nerespectării principiilor de către organizație, la respectarea principiilor în timpul prelucrărilor viitoare de către aceeași organizație și, după caz, la încetarea prelucrării datelor cu caracter personal ale persoanei care a depus plângerea. Sancțiunile trebuie să fie suficient de severe pentru a garanta respectarea principiilor de către organizație. O serie de sancțiuni cu grade diferite de severitate va permite instanțelor de soluționare a litigiilor să răspundă în mod corespunzător diferitelor niveluri de nerespectare a principiilor. Sancțiunile trebuie să includă atât publicarea nerespectărilor cât și obligația de a șterge datele în anumite circumstanțe ([2]). Alte sancțiuni pot include suspendarea sau anularea mărcii de conformitate, despăgubirea persoanelor pentru pierderile suferite ca urmare a nerespectării principiilor, precum și injoncțiuni. Organismele de soluționare a litigiilor și de autoreglementare a sectorului privat trebuie să semnaleze tribunalelor sau organului administrativ competent, după caz, organizațiile care aderă la „sfera de siguranță" și care nu respectă deciziile lor și să informeze Departamentul Comerțului (sau reprezentantul acestuia).

Acțiunea FTC

FTC s-a angajat să acorde prioritate analizării sesizărilor prezentate de organizațiile de autoreglementare, precum BBBOnline și TRUSTe, precum și de statele membre ale Uniunii Europene în ceea ce privește nerespectarea principiilor „sferei de siguranță", pentru a stabili dacă a fost încălcat articolul 5 din Federal Trade Commission Act care interzice actele sau practicile comerciale neloiale sau frauduloase. În cazul în care FTC stabilește că există motiv(e) pentru a considera că articolul 5 a fost încălcat, poate soluționa această problemă obținând un ordin administrativ de încetare care să interzică practicile contestate sau depunând o plângere la un tribunal districtual federal, care, în cazul în care plângerea este soluționată favorabil, poate emite un ordin care să producă același efect. FTC poate cere sancțiuni civile pentru încălcarea unui ordin administrativ de încetare și poate urmări contravenientul pentru ultraj într-un tribunal civil sau penal în cazul încălcării ordinului unei curți federale. FTC informează Departamentul Comerțului de orice acțiune de acest tip întreprinsă. Departamentul Comerțului încurajează celelalte organisme administrative să îi comunice toate cauzele similare sau alte decizii care determină aderarea la principii.

Încălcarea sistematică a principiilor

În cazul în care o organizație încalcă sistematic principiile, aceasta nu mai are dreptul să beneficieze de avantajele „sferei de siguranță". Principiile sunt încălcate sistematic atunci când o organizație care și-a declarat aderarea la principii la Departamentul Comerțului (sau la reprezentantul acestuia) refuză să se conformeze unei decizii definitive luate de un organism de autoreglementare sau de un organism public sau atunci când un asemenea organism constată că aceasta încalcă frecvent principiile astfel încât declarația ei de aderare nu mai este credibilă. Organizația trebuie să informeze neîntârziat aceste fapte Departamentului Comerțului (sau reprezentantului acestuia). În caz contrar, este pasibilă de sancțiuni în temeiul False Statements Act (18 U.S.C. § 1001).

Departamentul Comerțului (sau reprezentantul acestuia) va introduce pe lista publică, pe care o gestionează, a organizațiilor care și-au declarat aderarea la principiile „sferei de siguranță" orice notificare de încălcare sistematică, indiferent dacă aceasta provine de la organizație însăși, de la un organism de autoreglementare sau de la un organism public, însă numai după ce a acordat organizației în cauză un preaviz de treizeci (30) de zile și posibilitatea de a răspunde. În consecință, lista publică gestionată de Departamentul Comerțului (sau de reprezentantul acestuia) va preciza care organizații beneficiază de avantajele „sferei de siguranță" și care organizații nu mai beneficiază de acestea.

([1]) Organismele pentru soluționarea litigiilor nu sunt obligate să respecte principiul punerii în aplicare. De asemenea, ele pot face excepții de la principii în cazurile în care se confruntă cu obligații contradictorii sau primesc autorizări exprese în timpul realizării misiunilor lor specifice.

([2]) Circumstanțele în care trebuie aplicate aceste sancțiuni sunt lăsate la aprecierea organismelor de soluționare a litigiilor. Atunci când se stabilește dacă trebuie cerută ștergerea datelor trebuie luat în considerare caracterul sensibil al informațiilor în cauză și trebuie stabilit dacă organizația a colectat, utilizat sau publicat informațiile încălcând în mod manifest principiile.

Orice organizație care solicită să fie supusă autorității unui organism de autoreglementare pentru a putea beneficia din nou de avantajele „sferei de siguranță" trebuie să furnizeze acestui organism informații complete cu privire la aderarea ei anterioară la principii.

FAQ 12 – Opțiune (dreptul de a refuza) – Când poate fi exercitat?

Î: *Principiul opțiunii permite persoanei în cauză să își exercite dreptul la opțiune numai la începutul unei relații sau în orice moment?*

R: În general, obiectivul principiului opțiunii este de a asigura că informațiile cu caracter personal sunt utilizate și comunicate în conformitate cu așteptările și opțiunile persoanelor în cauză. În consecință, atunci când informații cu caracter personal sunt utilizate în cadrul unei acțiuni de marketing direct, orice persoană ar trebui să poată să își exercite dreptul de a refuza (sau de opțiune) în orice moment, în anumite limite definite de organizație (de exemplu termenul pentru a permite organizației punerea în aplicare a refuzului). De asemenea, organizația poate solicita un anumit număr de informații pentru a confirma identitatea persoanei care și-a exprimat refuzul. În Statele Unite ale Americii, acest drept poate fi exercitat prin intermediul unui program central de refuz, cum ar fi „Mail Preference Service" al Direct Marketing Association. Organizațiile care participă la „Mail Preference Service" al Direct Marketing Association ar trebui să promoveze disponibilitatea acestuia în rândul consumatorilor care nu doresc să primească informații comerciale. În orice caz, exercitarea acestei opțiuni trebuie să fie ușor accesibilă și puțin costisitoare.

În mod similar, o organizație poate utiliza informații în anumite scopuri de marketing direct atunci când condițiile nu permit exprimarea opțiunii persoanelor în cauză înainte de utilizarea informațiilor, cu condiția ca organizația să ofere apoi, cu promptitudine, (și, la cerere, în orice moment) posibilitatea persoanelor în cauză de a refuza (fără a plăti vreo taxă) să primească orice alte informații de marketing direct și să se conformeze dorințelor acestor persoane.

FAQ 13 – Informații cu privire la călătorii

Î: *Când pot fi comunicate organizațiilor situate în afara Uniunii Europene informațiile cu privire la pasagerii din transporturile aeriene (furnizate în special în momentul rezervărilor), precum cele privind clienții frecvenți sau rezervările la hotel, precum și cererile speciale – de exemplu mâncăruri care sunt în conformitate cu anumite principii religioase sau cu o asistență fizică?*

R: Aceste informații pot fi transferate in diferite circumstanțe. În conformitate cu articolul 26 din directivă, datele cu caracter personal pot fi transferate spre o țară terță care nu asigură un nivel adecvat de protecție în sensul articolului 25 alineatul (2) cu condiția ca (1) transferul să fie necesar pentru prestarea serviciilor solicitate de client sau pentru execuția unui contract, cum este acordul „client frecvent al zborurilor aeriene"; sau (2) pasagerul și-a dat acordul în mod neechivoc. Organizațiile din Statele Unite ale Americii care aderă la „sfera de siguranță" oferă o protecție adecvată a datelor cu caracter personal și, în consecință, pot primi aceste date din Uniunea Europeană fără a îndeplini aceste condiții și nici alte condiții menționate la articolul 26 din directivă. Întrucât principiile „sferei de siguranță" cuprind reguli specifice cu privire la informațiile sensibile, acest tip de informație (care pot privi, de exemplu, necesitatea clientului de a beneficia de asistență fizică) poate fi inclusă în datele transferate organizațiilor care aderă la principiile „sferei de siguranță". Organizația care transferă informațiile trebuie să aplice legislația națională a statului membru al Uniunii Europene în care operează, care poate impune, *inter alia*, condiții speciale pentru prelucrarea datelor sensibile.

FAQ 14 – Produse farmaceutice și medicale

Î 1: *În cazul în care datele cu caracter personal sunt strânse în Uniunea Europeană și transferate către Statele Unite ale Americii pentru cercetare farmaceutică și/sau alte scopuri, se aplică legislațiile statelor membre sau principiile „sferei de siguranță"?*

R 1: Legislația statelor membre se aplică colectării de date cu caracter personal și oricărei prelucrări care are loc înainte de transferul către Statele Unite ale Americii. Principiile „sferei de siguranță" se aplică datelor atunci când au fost transferate către Statele Unite ale Americii. Datele utilizate pentru cercetarea farmaceutică și în alte scopuri trebuie transmise, după caz, anonime.

Î 2: *Datele cu caracter personal elaborate în cadrul studiilor medicale sau farmaceutice joacă de multe ori un rol important în cercetarea științifică. Atunci când datele cu caracter personal adunate pentru un studiu sunt transferate unei organizații din Statele Unite ale Americii care a aderat la „sfera de siguranță", poate această organizație să utilizeze datele pentru o nouă activitate de cercetare științifică?*

R 2: Da, în cazul în care au fost prevăzute de la început o notificare și o opțiune corespunzătoare. Notificarea trebuie să ofere informații cu privire la orice utilizare specifică viitoare a datelor, cum ar fi controlul periodic, studiile asociate sau comercializarea. Nu pot fi precizate toate utilizările viitoare ale datelor, întrucât o nouă examinare a datelor, descoperiri și progrese medicale noi și evoluția în domeniul sănătății publice și al reglementării ar putea determina noi utilizări ale datelor. Prin urmare, notificarea ar trebui să includă, după caz, o mențiune că datele cu caracter personal pot fi utilizate pentru activități medicale și farmaceutice de cercetare viitoare neanticipate. În cazul în care această utilizare a datelor nu este conformă cu scopurile de cercetare generale pentru care datele au fost inițial colectate sau pentru care persoana în cauză a consimțit, trebuie obținut un nou consimțământ al acestei persoane.

Î 3: *Ce se întâmplă cu datele cu caracter personal în cazul în care un participant decide voluntar sau la cererea sponsorului să se retragă din studiul clinic?*

R 3: Participanții pot decide sau pot fi rugați să se retragă dintr-un studiu clinic în orice moment. Totuși, datele colectate înaintea retragerii pot fi prelucrate în continuare împreună cu celelalte date colectate în cadrul studiului clinic, cu condiția ca acest fapt să fi fost comunicat participantului în notificare în momentul în care și-a dat acordul.

Î 4: *Societățile producătoare de aparate farmaceutice și medicale au dreptul de a furniza date cu caracter personal extrase din testele clinice efectuate în Uniunea Europeană către autoritățile din Statele Unite ale Americii în scopul reglementării și controlului. Acest tip de transferuri este permis și altor părți, cum ar fi întreprinderi și alți cercetători?*

R 4: Da, în conformitate cu principiile notificării și opțiunii.

Î 5: *Pentru a asigura obiectivitatea testelor clinice, accesul la informațiile privind tratamentul de care beneficiază fiecare pacient este interzis participanților și, deseori, chiar și cercetătorilor. Accesul la aceste informații ar periclita validitatea testului și a rezultatelor. Participanții la asemenea teste clinice (denumite „teste mascate") vor avea acces la datele privind tratamentul lor pe parcursul testului?*

R 5: Nu, accesul nu trebuie să fie acordat participantului în cazul în care această restricție i-a fost explicată la începutul testului și în cazul în care publicarea acestor informații ar periclita integritatea eforturilor de cercetare. Acordul de a participa la test în aceste condiții presupune renunțarea la dreptul de acces. La încheierea testului și după analizarea rezultatelor, participanții ar trebui să aibă acces la datele lor, dacă doresc acest lucru. Ar trebui să ceară aceste date în primul rând medicului sau altui prestator de servicii de sănătate de la care au primit tratamentul în cadrul testului clinic, sau, în al doilea rând, societății comerciale care a sponsorizat programul.

Î 6: *Societățile producătoare de aparate farmaceutice sau medicale trebuie să aplice în activitățile lor de control al securității și eficacității produsului principiile „sferei de siguranță" cu privire la notificare, opțiune, transfer și acces, inclusiv semnalarea incidentelor și urmărirea pacienților/subiecților care folosesc anumite medicamente sau aparate medicale (de exemplu, un stimulator cardiac)?*

R 6: Nu, în măsura în care respectarea acestor principii contravine cerințelor de reglementare. Acest lucru este valabil în ceea ce privește, de exemplu, rapoartele efectuate atât de prestatorii de servicii de sănătate către societățile comerciale producătoare de aparate farmaceutice și medicale, cât și cele efectuate de aceste din urmă societăți comerciale către agenții guvernamentale precum Food and Drug Administration (autoritatea pentru supravegherea alimentelor și medicamentelor).

Î 7: *Datele referitoare la cercetare sunt, de obicei, codificate la sursă de către cercetătorul principal pentru a nu fi dezvăluită identitatea părților interesate. Societățile comerciale farmaceutice care sponsorizează aceste cercetări nu primesc codul de acces. Codul de acces unic este deținut numai de către cercetător, astfel încât acesta/aceasta să poată identifica persoana în cauză în circumstanțe speciale (de exemplu în cazul în care este necesară o monitorizare medicală). Transferul din Uniunea Europeană către Statele Unite ale Americii de date cu caracter personal codificate în acest fel reprezintă un transfer de date supus principiilor „sferei de siguranță"?*

R 7: Nu. Acest transfer nu constituie un transfer de date cu caracter personal supus acestor principii.

FAQ 15 – Informații din registre publice și informații accesibile publicului

Î: *Este necesar să se aplice principiile notificării, opțiunii și transferului ulterior informațiilor din registrele publice sau informațiilor accesibile publicului?*

R: Nu este necesar să se aplice principiul notificării, opțiunii și transferului ulterior informațiilor din registrele publice, în cazul în care acestea din urmă nu sunt asociate cu informații care nu sunt accesibile publicului și în cazul în care sunt respectate toate condițiile de consultare stabilite de instanța competentă.

De asemenea, nu este necesară aplicarea principiilor notificării, opțiunii și transferului ulterior în cazul informațiilor accesibile publicului decât în cazul în care entitatea europeană care efectuează transferul indică faptul că aceste informații fac obiectul restricțiilor care necesită aplicarea acestor principii de către organizație în timpul utilizării lor. Organizația nu are nici o responsabilitate cu privire la modul în care sunt utilizate aceste informații de către cei care obțin aceste informații din materiale publicate.

În cazul în care se constată că o organizație a făcut publice în mod intenționat informații cu caracter personal încălcând principiile astfel încât ea însăși sau alte părți terțe să poată beneficia de aceste excepții, va fi exclusă din „sfera de siguranță”.

ANEXA III

Studiu privind punerea în aplicare a principiilor „sferei de siguranță"

Atribuțiile autorităților federale și ale statelor membre ale federației în domeniul practicilor neloiale și frauduloase și protecția vieții private

Prezentul memorandum prezintă o sinteză a atribuțiilor pe care le are Comisia Federală pentru Comerț (FTC) în temeiul articolul 5 din Federal Trade Commission Act (15 U.S.C. §§ 41-58, astfel cum a fost modificat) de a lua măsuri împotriva persoanelor care nu asigură protecția informațiilor cu caracter personal în conformitate cu declarațiile lor și/sau angajamentele luate în acest sens. De asemenea, tratează derogările de la aceste atribuții și posibilitățile de intervenție de care dispun alte agenții federale și ale statelor membre ale federației în cazurile care nu sunt de competența FTC ([1]).

Competența FTC în domeniul practicilor neloiale sau frauduloase

Articolul 5 din Federal Trade Commission Act declară ca ilegale „actele și practicile neloiale sau frauduloase din domeniul comerțului sau care afectează comerțul" [15 U.S.C. § 45 (a) (1)]. Articolul 5 conferă FTC puteri depline pentru a împiedica asemenea acte și practici [15 U.S.C. § 45 (a) (2)]. În consecință, FTC poate, la finalizarea unei audieri oficiale, să emită o dispoziție de întrerupere și încetare a activității pentru a pune capăt comportamentului infracțional [15 U.S.C. § 45 (b)]. În cazul în care este în interesul public, FTC poate, de asemenea, solicita instanțe federale districtuale din Statele Unite ale Americii emiterea unei dispoziții de încetare temporară a activității sau un ordin judecătoresc temporar sau permanent [15 U.S.C. § 53 (b)]. Atunci când actele sau practicile neloiale sau frauduloase au un caracter sistematic sau în cazul în care FTC a emis deja dispoziții de întrerupere și încetare a activității, aceasta poate adopta dispoziții administrative privind actele sau practicile în cauză [15 U.S.C. § 57 (a)].

Orice persoană care nu se conformează unei ordonanțe FTC este pasibilă de o amendă stabilită prin hotărâre judecătorească civilă de până la 11 000 USD, fiecare zi de continuare a încălcării constituind o încălcare separată ([2]) [15 U.S.C. § 45 (1)]. De asemenea, orice persoană care încalcă cu bună știință o dispoziție FTC este pasibilă de o amendă de 11 000 USD pentru fiecare încălcare [15 U.S.C. § 45 (m)]. Acțiunile vizând asigurarea aplicării legislației pot fi intentate fie de către Departamentul de Justiție sau, în lipsa acțiunii acestuia, de către FTC (15 U.S.C. § 56).

Competența FTC și protecția vieții private

Atunci când își exercită competențele în temeiul articolului 5, FTC consideră că orice declarație falsă cu privire la motivele pentru care sunt strânse informațiile de la consumatori și la modul în care informațiile vor fi utilizate constituie o practică frauduloasă ([3]). De exemplu, în 1998 FTC a depus o plângere împotriva societății comerciale GeoCities care, în mod contrar declarațiilor sale și fără o permisiune prealabilă, a divulgat unor terți, în scopuri publicitare, informații strânse pe site-ul său web ([4]). Reprezentanții FTC au arătat, de asemenea, că strângerea de informații cu caracter personal de la copii, precum și vânzarea și divulgarea acestor informații fără consimțământul părinților, este susceptibilă de a constitui o practică neloială ([5]).

([1]) Prezentul studiu nu discută întregul ansamblu de dispoziții federale privind protecția vieții private în anumite contexte specifice, nici dispozițiile statale și *common law* care s-ar putea aplica. Printre legile care, la nivel federal, reglementează strângerea și utilizarea de informații cu caracter personal în scopuri comerciale, se numără: Cable Communications Policy Act (47 U.S.C., § 551), Driver's Privacy Protection Act (18 U.S.C., § 2721), Electronic Communications Privacy Act (18 U.S.C., § 2701 și urm.), Electronic Funds Transfer Act [15 U.S.C., §§ 1693, 1693 (m)], Fair Credit Reporting Act (15 U.S.C., § 1681 și urm.), Right to Financial Privacy Act (12 U.S.C., § 3401 și urm.), Telephone Consumer Protection Act (47 U.S.C., § 227) și Video Privacy Protection Act (18 U.S.C., § 2710). Numeroase state membre ale federației dispun de o legislație analoagă în aceste domenii. A se vedea, de exemplu: Mass. Gen. Laws, capitolul 167B, § 16 (prin care se interzice instituțiilor financiare să divulge informații financiare cu privire la clienții lor unor terți fără consimțământul clienților sau fără o hotărâre judecătorească în acest sens); NY Pub. Health Law, § 17 (prin care este limitată utilizarea și divulgarea datelor privind sănătatea fizică sau mentală și prin care li se acordă pacienților dreptul de acces la aceste date).

([2]) În cadrul unei astfel de acțiuni în justiție, instanța federală districtuală poate, de asemenea, stabili prin intermediul unui ordin judecătoresc măsuri reparatorii echitabile considerate adecvate pentru punerea în aplicare a hotărârii FTC [15 U.S.C., § 45 (1)].

([3]) Prin „practică frauduloasă" se înțelege o declarație, o omisiune sau o practică susceptibilă de a induce în eroare, într-o măsură semnificativă, consumatorul avizat în mod normal.

([4]) A se vedea www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) A se vedea scrisoarea FTC adresată Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Pe lângă aceasta, Children's Online Privacy Protection Act din 1998 conferă FTC atribuții juridice specifice pentru a reglementa colectarea de informații cu caracter personal de la copii de către operatorii de site-uri web și de servicii on-line (15 U.S.C. §§ 6501-6506). Legea obligă acești operatori să trimită un aviz de informare și să obțină consimțământul verificabil al părinților înainte de a strânge, utiliza sau divulga informații cu caracter personal obținute de la copii [15 U.S.C. § 6502 (b)]. De asemenea, legea dă părinților dreptul de a avea acces la informațiile strânse și de a refuza acordarea permisiunii de a continua utilizarea acestora (Idem).

Într-o scrisoare adresată domnului John Mogg, director general al Comisiei Europene, domnul Pitofsky, președintele FTC, a remarcat că atribuțiile FTC cu privire la protecția vieții private erau limitate în absența unei declarații false (sau în absența oricărei declarații) cu privire la utilizarea ulterioară a informațiilor (A se vedea scrisoarea domnului Pitofsky, președintele FTC, adresată domnului John Mogg la 23 septembrie 1998). Cu toate acestea, întreprinderile care doresc să beneficieze de avantajele „sferei de siguranță" propuse vor trebui să certifice că vor proteja informațiile pe care le strâng în conformitate cu liniile directoare prescrise. În consecință, orice societate comercială care certifică faptul că va garanta confidențialitatea informațiilor și care nu va respecta acest angajament se va face vinovată de declarație falsă și va comite o „practică frauduloasă" în sensul articolului 5.

Competența FTC cuprinde actele și practicile neloiale sau frauduloase „din comerț" și nu acoperă colectarea și utilizarea de informații cu caracter personal în scopuri necomerciale (de exemplu, strângerile de fonduri în scopuri de binefacere) (scrisoarea domnului Pitofsky, p. 3). Cu toate acestea, utilizarea informațiilor cu caracter personal în cadrul oricărei tranzacții comerciale intră în competența FTC. Atunci când un angajator vinde, de exemplu, informații cu caracter personal privind salariații săi unei societăți comerciale de marketing direct, tranzacția intră în domeniul de aplicare al articolului 5.

Derogări prevăzute la articolul 5

Articolul 5 prevede derogări de la competența FTC în materie de acte și practici neloiale sau frauduloase pentru următoarele sectoare de activitate:

— instituțiile financiare, inclusiv băncile, societățile financiare de economii și împrumut și cooperativele de credit;

— societățile de telecomunicații și societățile publice de transport interstatal;

— transportatorii aerieni;

— operatorii din sectorul de ambalare și cei din sectorul zootehnic.

A se vedea 15 U.S.C. § 45 (a) (2). Fiecare derogare și organismele de reglementare care se substituie FTC-ului sunt examinate mai jos.

Instituții financiare ([1])

Prima derogare se referă la „bănci, societăți de economii și împrumut în sensul articolului 18 (f) (3) [15 U.S.C. § 57 (a) (f) (3)]" precum și „cooperativele federale de credit în sensul articolului 18 (f) (4) [15 U.S.C. § 57 (a) (f) (4)]" ([2]). Aceste instituții financiare se supun în schimb dispozițiilor emise de Federal Reserve Board, Office of Thrift Supervision ([3]) și National Credit Union Administration Board [15 U.S.C. § 57 (a) (f)]. Aceste organe de reglementare au obligația de a adopta dispozițiile necesare pentru a preveni practicile neloiale și frauduloase ale acestor instituții financiare ([4]) și de a înființa servicii distincte însărcinate să se ocupe de plângerile consumatorilor [15 U.S.C. § 57 (a) (f) (1)]. În sfârșit, competențele de punere în aplicare decurg din articolul 8 din Federal Deposit Insurance Act (12 U.S.C. § 1818) în cazul băncilor și al societăților de economii și împrumut și din articolele 120 și 206 din Federal Credit Union Act în cazul cooperativelor federale de credit [15 U.S.C. §§ 57 (a) (f) (2)-4)].

Deși societățile de asigurări nu sunt în mod expres incluse pe lista derogărilor din articolul 5, legea McCarran-Ferguson (15 U.S.C. § 1011 *și urm.*) prevede că, în general, reglementarea activităților de asigurare revine fiecărui stat membru al federației în parte ([5]). Pe lângă aceasta, în temeiul articolului 2 (b) din legea McCarran-Ferguson, nici o lege federală

([1]) La 12 noiembrie 1999, președintele Clinton a promulgat, prin semnare, Gramm-Leach-Bliley Act, aceasta urmând a intra în vigoare (Pub. L. 106-102, codificată la 15 U.S.C. § 6801 și urm.). Această lege limitează divulgarea de către instituțiile financiare a informațiilor cu caracter personal despre clienții lor. Legea obligă instituțiile financiare, între altele, să informeze toți clienții despre politicile și practicile lor cu privire la protecția vieții private în cadrul schimbului de informații cu caracter personal cu întreprinderi afiliate sau nu. Legea autorizează FTC, autoritățile bancare federale și alte autorități să adopte dispoziții pentru punerea în aplicare a măsurilor stabilite pentru protecția vieții private. Organismele publice în cauză au emis propuneri de dispoziții în acest scop.

([2]) Prin formularea sa, această derogare nu se aplică sectorului de valori mobiliare. În consecință, brokerii, operatorii cu titluri și ceilalți participanți din sectorul societăților de valori mobiliare intră sub jurisdicția concurentă a Securities and Exchanges Commission și a FTC cu privire la actele și practicile neloiale sau frauduloase.

([3]) Derogarea prevăzută la articolul 5 se referea inițial la Federal Home Loan Bank Board, care a fost desființat de Financial Institutions Reform, Recovery and Enforcement Act din 1989. Funcțiile sale au fost transferate la Office of Thrift Supervision, precum și la Resolution Trust Corporation, Federal Deposit Insurance Corporation și Housing Finance Board.

([4]) Deși exclude instituțiile financiare din domeniul de competență al FTC, articolul 5 prevede că ori de câte ori FTC emite o dispoziție cu privire la actele și practicile neloiale sau frauduloase, organismele de reglementare financiară trebuie să adopte dispoziții similare în termen de 60 de zile [15 U.S.C. § 57 (a) (f) (1)].

([5]) „Activitățile de asigurare precum și persoanele care desfășoară activități în acest domeniu se supun legilor diferitelor state membre ale federației cu privire la reglementarea sau impozitarea acestor activități" [15 U.S.C., § 1012 (a)].

nu poate abroga, modifica sau înlocui reglementarea unui stat membru al federației „decât în cazul în care o astfel de lege se referă în mod expres la activitățile de asigurare" [15 U.S.C. § 1012 (b)]. Cu toate acestea, dispozițiile din legea privind Comisia Federală pentru Comerț se aplică sectorului asigurărilor „în măsura în care această activitate nu este reglementată de către statele membre ale federației" (*Idem*). Mai trebuie menționat că legea McCarran-Ferguson nu conferă competență statelor membre ale federației decât cu privire la „activitățile de asigurare". În consecință, FTC rămâne autoritatea competentă, cu titlu supletiv, pentru actele și practicile neloiale sau frauduloase comise de societățile de asigurări în cadrul activităților care nu intră în domeniul asigurărilor. Acestea pot include, de exemplu, vânzarea de către asigurator de informații cu caracter personal cu privire la clienții săi către comercianții direcți de produse din afara sectorului asigurărilor ([1]).

Transportatorii publici

A doua derogare prevăzută la articolul 5 îi privește pe transportatorii publici „supuși legilor vizând reglementarea comerțului" [15 U.S.C. § 45 (a) (2)]. În acest caz, „legile vizând reglementarea comerțului" corespund subtitlului IV din titlul 49 din United States Code și Communications Act din 1934 (47 U.S.C. § 151 *și urm.*) [15 U.S.C. § 44].

Subtitlul IV din titlul 49 din U.S.C. (transportul interstatal) include transportatorii pe cale ferată, rutieră și navigabilă, brokerii, comisionarii de transport și transportatorii prin conducte (49 U.S.C. § 10101 *și urm.*). Acești transportatori publici sunt supuși reglementărilor emise de Surface Transportation Board, un organism independent din cadrul Departamentului Transporturilor (49 U.S.C. §§ 10501, 13501 și 15301). În toate cazurile, transportatorului i se interzice divulgarea de informații cu privire la natura, destinația și alte aspecte ale încărcăturii sale care ar putea fi utilizate în detrimentul expeditorului (49 U.S.C. §§ 11904, 14908 și 16103). Trebuie observat că aceste dispoziții se referă la informații privind încărcătura expeditorului și nu privesc datele cu caracter personal referitoare la expeditor și care nu au legătură cu mărfurile expediate.

Communications Act prevede că reglementarea „comerțului interstatal și internațional cu comunicații prin cablu și prin radio" revine Federal Communications Commission (FCC) (47 U.S.C. §§ 151 și 152). Pe lângă întreprinderilor de telecomunicații publice, această lege se aplică și altor întreprinderi precum teledifuzorii, radiodifuzorii și furnizorii de servicii prin cablu, care nu sunt transportatori publici și care nu îndeplinesc condițiile cerute pentru a beneficia de derogarea prevăzută la articolul 5 din FTC Act. În consecință, FTC are competența de a investiga aceste societăți comerciale pentru practici neloiale și frauduloase, în timp ce FCC are o competență concurentă care îi permite să exercite atribuții independente în acest domeniu, după cum este descris mai jos.

În temeiul Communications Act, „orice societate de telecomunicații", inclusiv societățile comerciale locale, are datoria de a proteja confidențialitatea informațiilor exclusive cu privire la clienți ([2]) [47 U.S.C. § 222 (a)]. Pe lângă această dispoziție generală privind protecția vieții private, Communications Act a fost modificat de Cable Communications Policy Act din 1984 (denumit în continuare Cable Act) (47 U.S.C. § 521 *și urm.*), astfel încât să prevadă în mod clar că operatorii de servicii prin cablu trebuie să protejeze confidențialitatea „informațiilor identificabile personal" cu privire la abonații serviciilor prin cablu (47 U.S.C. § 551) ([3]). Cable Act limitează colectarea de informații cu caracter personal de către operatorii de servicii prin cablu și îi obligă pe aceștia din urmă să informeze abonații cu privire la natura și la utilizarea ulterioară a informațiilor colectate. Cable Act dă abonaților dreptul de acces la informațiile despre ei și îi obligă pe operatorii de servicii prin cablu să distrugă aceste informații atunci când nu le mai sunt necesare.

Communications Act acordă FCC competență pentru punerea în aplicare – din proprie inițiativă sau ca răspuns la o plângere din exterior – a acestor două dispoziții privind confidențialitatea ([4]) (47 U.S.C. §§ 205, 403; § 208). În cazul în care FCC stabilește că o societate de telecomunicații (inclusiv un operator de servicii prin cablu) a încălcat normele privind protecția vieții private menționate la articolele 222 și 551, acesta poate lua trei măsuri diferite. În primul rând,

---

([1]) FTC și-a exercitat atribuțiile cu privire la societățile de asigurări în contexte diferite. Într-unul din cazuri, FTC a luat măsuri împotriva unei întreprinderi care făcuse publicitate înșelătoare într-un stat membru al federației în care nu era autorizată. Competența FTC a fost confirmată pe baza faptului că nu exista nici o reglementare eficientă la nivelul statelor membre ale federației deoarece întreprinderea în cauză se găsea, practic, în afara domeniului de aplicare a statului în cauză. A se vedea FTC contra Travelers Health Association, 362 U.S. 293 (1960).
În ceea ce privește statele membre ale federației, șaptesprezece dintre acestea au adoptat modelul „Insurance Information and Privacy Protection Act" elaborat de National Association of Insurance Commissioners (NAIC). Această lege cuprinde dispoziții cu privire la informarea asiguraților, utilizarea, divulgarea și accesul la datele strânse. De asemenea, aproape toate statele membre ale federației au adoptat modelul „Unfair Insurance Practices Act" elaborat de NAIC, care vizează în mod expres practicile comerciale neloiale din sectorul asigurărilor.

([2]) Prin „informații de rețea exclusive privind clienții" se înțeleg informațiile care privesc „numărul, configurația tehnică, tipul, destinația și frecvența utilizării serviciilor de telecomunicații" furnizate unui client, precum și informațiile incluse în facturile telefonice [47 U.S.C. § 222 (f) (1)]. Cu toate acestea, nu sunt incluse informațiile privind lista de abonați (Idem).

([3]) Legislația nu definește în mod expres noțiunea de „informații identificabile personal".

([4]) Această competență include dreptul la reparații în cazul nerespectării confidențialității în conformitate cu articolul 222 din Communications Act și, pentru abonații serviciilor prin cablu, în conformitate cu articolul 551 din Cable Act care modifică Communications Act [a se vedea și 47 U.S.C. § 551 (f) (3)] (o acțiune civilă într-o instanță federală districtuală constituie o cale de atac neexclusivă, disponibilă „în completarea oricărei alte căi de atac de care dispune un abonat la serviciile prin cablu").

în urma unei audieri și după ce încălcarea dispozițiilor a fost constatată, FCC poate ordona transportatorului să plătească daune-interese ([1]) (47 U.S.C. § 209). Alternativ, FCC poate emite o ordonanță de încetare împotriva transportatorului, pentru ca acesta să înceteze practica sau omisiunea incriminată [47 U.S.C. § 205 (a)]. În sfârșit, FCC poate, de asemenea, ordona transportatorului contravenient să „se conformeze și să respecte orice reglementare sau practică" pe care ar putea-o prescrie FCC (*Idem*).

Persoanele private care consideră că o societate de telecomunicații sau un operator de servicii prin cablu a încălcat dispozițiile corespondente din Communications Act sau din Cable Act pot fie să depună o plângere la FCC, fie să sesizeze o instanță federal districtuală (47 U.S.C. § 207). Reclamanții care au câștig de cauză într-o acțiune intentată în fața unei instanțe federale împotriva unei societăți de telecomunicații care nu a protejat informațiile exclusive despre clienți în temeiul articolului 222 din Communications Act pot beneficia de despăgubiri pentru prejudiciul efectiv suferit și de rambursarea onorariilor plătite avocaților (47 U.S.C. § 206). Reclamanții care intentează o acțiune în justiție pretinzând nerespectarea confidențialității în temeiul articolului 551 din Cable Act pot beneficia, în plus, de daune-interese cu titlu de sancțiune și de rambursarea, în limite rezonabile, a cheltuielilor de judecată [47 U.S.C. § 551 (f)].

FCC a stabilit modalitățile de punere în aplicare a articolului 222 (a se vedea 47 CFR 64.2001-2009). Aceste norme stabilesc o serie de măsuri de salvgardare în vederea protecției împotriva accesului neautorizat la informațiile din rețea exclusive privind clienții. Aceste norme obligă societățile de telecomunicații:

— să elaboreze și să pună în aplicare sisteme software care să semnaleze situația clientului (aviz/consimțământ) atunci când datele acestuia apar pentru prima dată pe ecran;

— să păstreze o „pistă de control" electronică pentru a ține evidența accesării contului unui client și pentru a stabili când, de către cine și în ce scop sunt consultate datele unui client;

— să își formeze personalul cu privire la utilizarea autorizată a informațiilor din rețea exclusive privind clienții și să adopte procedurile disciplinare care se impun;

— să stabilească un proces de revizuire și supraveghere pentru a garanta respectarea regulilor pe parcursul desfășurării activităților de marketing extern;

— să prezinte anual la FCC o declarație cu privire la măsurile luate pentru a se conforma acestor reguli.

Transportatorii aerieni

Transportatorii aerieni din Statele Unite ale Americii și cei străini care intră sub incidența domeniului de aplicare al Federal Aviation Act din 1958 sunt și ei excluși din domeniul de aplicare al articolului 5 din FTC Act [15 U.S.C. § 45 (a) (2)]. Este vorba de orice persoană care furnizează servicii interstatale sau internaționale de transport de mărfuri sau de pasageri pe cale aeriană sau transporturi poștale pe cale aeriană (49 U.S.C. § 40102). Transportatorii aerieni se supun jurisdicției Departamentului Transporturilor. În această privință, Secretarul pentru Transporturi este autorizat să ia măsuri „pentru a împiedica practicile neloiale, frauduloase, abuzive sau anticoncurențiale din domeniul transporturilor aeriene" [49 U.S.C. § 40101 (a) (9)]. Atunci când interesul public o cere, Secretarul pentru Transporturi poate conduce o anchetă pentru a stabili dacă un transportator aerian din Statele Unite ale Americii sau străin sau un agent care livrează bilete de avion s-a angajat în practici neloiale sau frauduloase (49 U.S.C. § 41712). În urma unei audieri, Secretarul pentru Transporturi poate emite o ordonanță de încetare a practicii ilegale în cauză (*Idem*). Din câte cunoaștem noi, Secretarul pentru Transporturi nu a făcut încă uz de aceste atribuții cu privire la protejarea confidențialității informațiilor cu caracter personal referitoare la clienții companiilor aeriene ([2]).

Există două dispoziții privind protecția confidențialității informațiilor cu caracter personal care se aplică transportatorilor aerieni în contexte specifice. Pe de-o parte, Federal Aviation Act protejează viața privată a candidaților la un post de pilot [49 U.S.C. § 44936 (f)]. Chiar dacă această lege permite transportatorilor aerieni să obțină informații cu privire la antecedentele profesionale ale unui candidat, ea oferă candidatului dreptul de a fi anunțat când sunt solicitate astfel de informații, de a-și da consimțământul pentru această solicitare, de a corecta inexactitățile și de a nu permite divulgarea acestor informații decât celor implicați direct în procesul de recrutare. Pe de altă parte, reglementările Departamentului Transporturilor cer ca informațiile din listele de pasageri colectate în scopuri administrative, în eventualitatea unei catastrofe aeriene, „să fie prelucrate în regim de confidențialitate și comunicate numai Departamentului de Stat al Statelor Unite ale Americii, National Transportation Board (la cererea NTSB) și Departamentului Transporturilor" [14 CFR partea 243, § 243.9 (c)] (astfel cum a fost completat de 63 FR 8258).

([1]) Cu toate acestea, absența unei daune directe suferite de reclamant nu constituie un motiv suficient pentru respingerea unei plângeri [47 U.S.C. § 208 (a)].

([2]) Se pare că în prezent se întreprind eforturi în această ramură de activitate pentru a rezolva problema protecției vieții private. Reprezentanții acestei ramuri au examinat principiile propuse pentru „sfera de siguranță" și eventuala lor aplicare în cazul transportatorilor aerieni. Această examinare a inclus, de asemenea, propunerea de a se adopta o politică privind protecția vieții private valabilă pentru întreaga ramură și în cadrul căreia întreprinderile participante să se supună în mod expres autorității Departamentului Transporturilor.

Operatorii din sectorul de ambalare și cei din sectorul zootehnic

Packers and Stockyards Act (lege privind operatorii din sectorul de ambalare și cei din sectorul zootehnic) din 1921 (7 U.S.C. § 181 *și urm*.) interzice „oricărui operator din sectorul de ambalare de animale vii, carne, produse din carne sau produse animale neprelucrate sau oricărui comerciant de păsări de curte vii de a recurge, în cadrul activităților sale, la practici sau acte neloiale, injust discriminatorii sau frauduloase" [7 U.S.C. § 192 (a); a se vedea și 7 U.S.C. § 213 (a)] (interzicând orice „practici sau acte neloiale, injust discriminatorii sau frauduloase" în legătură cu animalele). Revine Secretarului pentru Agricultură responsabilitatea punerii în aplicare a acestor dispoziții, în timp ce FTC își păstrează competența pentru comerțul cu amănuntul și pentru operațiunile privind industria păsărilor de curte [7 U.S.C. § 227 (b) (2)].

Nu este clar dacă Secretarul pentru Agricultură va interpreta situațiile în care un operator din sectorul de ambalare sau din sectorul zootehnic nu oferă protecție datelor cu caracter personal în conformitate cu politica sa declarată drept practici „frauduloase" în temeiul Packers and Stockyards Act. Cu toate acestea, derogarea de la articolul 5 nu se aplică persoanelor, asociațiilor și societăților comerciale decât „în măsura în care fac obiectul Packers and Stockyards Act". Prin urmare, în cazul în care protecția vieții private nu intră în domeniul de aplicare al Packers și Stockyards Act, derogarea prevăzută la articolul 5 poate să nu se aplice, iar operatorii din sectorul de ambalare și cei din sectorul zootehnic ar urma să intre în competența FTC în această privință.

Competența statelor membre ale federației în materia „practicilor neloiale și frauduloase"

Potrivit unei analize realizate de FTC, „toate cele cincizeci de state, precum și Districtul Columbia, Guam, Puerto Rico și Insulele Virgine au adoptat legi mai mult sau mai puțin similare cu Federal Trade Commission Act pentru a lupta împotriva practicilor neloiale sau frauduloase". [FTC fact sheet, retipărit în „Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation", *59 Tul. L. Rev. 427 (1984)*]. În toate cazurile, un organism public însărcinat cu punerea în aplicare a legislației este abilitat „să desfășoare cercetări prin intermediul citațiilor sau al solicitărilor de anchete civile, să obțină din partea organizațiilor în cauză asigurarea că acestea respectă în mod voluntar legislația, să emită ordonanțe de întrerupere și de încetare a activității și să solicite ordine judecătorești în vederea împiedicării practicilor comerciale neloiale, imorale sau frauduloase (*Idem*). În patruzeci și șase dintre jurisdicțiile menționate anterior, legea permite persoanelor private să intenteze acțiuni în vederea obținerii unei despăgubiri simple, duble sau triple sau chiar a unor despăgubiri cu titlu de sancțiune precum și, în anumite cazuri, rambursarea cheltuielilor și a onorariilor plătite avocaților (*Idem*)."

Deceptive and Unfair Trade Practices Act din statul Florida autorizează, de exemplu, procurorul general să ancheteze și să intenteze acțiuni civile pentru „concurență neloială sau practici comerciale neloiale, imorale sau frauduloase", incluzând publicitatea mincinoasă sau înșelătoare, ofertele înșelătoare de franciză sau de operațiuni comerciale, practicile frauduloase de telemarketing și sistemele piramidale. A se vedea și N.Y. General Business Law § 349 (interzicând actele neloiale și practicile frauduloase în lumea afacerilor).

O anchetă realizată în acest an de către National Association of Attorneys General (NAAG) confirmă aceste rezultate. Fiecare dintre cele patruzeci și trei de state care au răspuns au legi „mini-FTC" sau alte legi care oferă o protecție similară. Potrivit aceleiași anchete, treizeci și nouă de state au indicat că ar avea competența de a examina plângerile depuse de nerezidenți. În ceea ce privește protecția vieții private a consumatorilor, în special, treizeci și șapte din cele de patruzeci și unu de state care au răspuns au arătat că ar răspunde plângerilor care pretind că o societate comercială din jurisdicția lor nu ar respecta politica privind protecția vieții private pe care a declarat-o.

ANEXA IV

Daune-interese pentru nerespectarea protecției vieții private, autorizații legale, fuziuni și absorbții în conformitate cu legislația Statelor Unite ale Americii

Prezentul document răspunde cererii formulate de Comisia Europeană privind clarificarea legislației Statelor Unite ale Americii cu privire la (a) cererile de despăgubiri pentru nerespectarea protecției vieții private, (b) „autorizațiile exprese" prevăzute în legislația Statelor Unite ale Americii pentru utilizarea informațiilor cu caracter personal într-un mod care contravine principiilor „sferei de siguranță" și (c) efectul fuziunilor și absorbțiilor asupra obligațiilor asumate în conformitate cu principiile „sferei de siguranță".

A. **Despăgubiri pentru nerespectarea protecției vieții private**

Nerespectarea principiilor „sferei de siguranță" ar putea da naștere la o serie de reclamații ale persoanelor private, în funcție de circumstanțe. În special, organizațiile care a aderat la „sfera de siguranță" ar putea fi considerate responsabile de falsificare pentru nerespectarea politicilor declarate cu privire la protecția vieții private. De asemenea, legislația prevede și posibilitatea intentării de acțiuni juridice de către persoane private în vederea obținerii de despăgubiri pentru nerespectarea protecției vieții private. Sunt prevăzute numeroase dispoziții la nivel federal și național pentru anchetarea cererilor de despăgubire depuse de către persoane particulare pentru încălcarea protecției vieții private.

Dreptul la despăgubire pentru încălcarea vieții private este bine stabilit în legislația Statelor Unite ale Americii.

Utilizarea informațiilor cu caracter personal într-un mod care contravine principiilor „sferei de siguranță" poate da naștere unei responsabilități legale în temeiul diferitor teorii juridice. De exemplu, atât responsabilul de date care efectuează transferul, cât și persoanele în cauză pot urmări în justiție, pentru falsificare, organizația care a aderat la „sfera de siguranță" care nu își onorează angajamentul de a respecta principiile „sferei de siguranță". În conformitate cu Restatement of the Law, Second, Torts ([1]):

> Oricine se face vinovat de falsificarea unui fapt, unei opinii, unei intenții sau unei legi cu scopul de a determina o altă persoană să acționeze sau să nu acționeze pe baza acestei declarații este responsabil de eventuala daună pecuniară provocată persoanei înșelate care a avut încredere, din motive justificabile, în această declarație falsă.

(Restatement, paragraf 525). O falsificare este „frauduloasă" în cazul în care este făcută cu bună știință sau având convingerea că este falsă (*Idem*, paragraf 526). De regulă, persoana care face o falsificare frauduloasă este potențial responsabilă pentru eventualele daune pecuniare suferite de toate persoanele care au avut încredere în elementul fals prezentat (*Idem*, paragraf 531). Mai mult, o parte care face o falsificare frauduloasă față de o altă parte ar putea fi considerată responsabilă și față de o parte terță în cazul în care cel ce a realizat falsificarea intenționează sau se așteaptă ca falsificarea să fie repetată către o parte terță care să acționeze pe baza ei (*Idem*, paragraf 533).

În cadrul „sferei de siguranță", reprezentarea relevantă este declarația publică prin care organizația atestă că va adera la principiile „sferei de siguranță". Luându-și acest angajament, încălcarea cu bună știință a principiilor ar putea constitui temei pentru intentarea unei acțiuni în justiție pentru înșelăciune de către persoanele care au avut încredere în acel element fals prezentat. Întrucât angajamentul de a respecta aceste principii este universal, persoanele care fac subiectul acelor informații, precum și responsabilul de date din Europa care efectuează transferul informațiilor cu caracter personal către organizația din Statele Unite ale Americii ar putea toți avea temei pentru acțiuni în justiție împotriva organizației din Statele Unite ale Americii pentru înșelăciune ([2]). Pe lângă aceasta, organizația din Statele Unite ale Americii rămâne responsabilă față de aceste persoane pentru „înșelăciune în formă continuă" pe întreaga perioadă în care aceste persoane au încredere în acel element fals prezentat în detrimentul lor (Restatement, paragraf 535).

([1]) Second Restatement of the Law – Torts; American Law Institute (1997).

([2]) Acest lucru ar putea fi valabil, de exemplu, în cazurile în care persoanele au avut încredere în angajamentul asumat de organizația din Statele Unite de a respecta principiile „sferei de siguranță" atunci când și-au dat consimțământul responsabilului de date pentru ca acesta să transfere informațiile cu caracter personal către Statele Unite.

Persoanele care se încred într-o înșelăciune săvârșită cu intenție au dreptul la despăgubiri. În conformitate cu Restatement:

> Destinatarul unei înșelăciuni săvârșite cu intenție are dreptul să-și recupereze sub formă de despăgubiri, prin intermediul unei acțiuni în justiție pentru înșelăciune, pierderea pecuniară pe care autorul înșelăciunii i-a provocat-o.

(Restatement, paragraf 549). Aceste despăgubiri includ, pe lângă prejudiciul efectiv, și câștigurile nerealizate în cadrul unei tranzacții comerciale [*Idem*; a se vedea, de exemplu, *Boling v. Tennessee State Bank*, 890 S.W.2d 32 (1994)] (banca trebuie să plătească persoanelor care au luat împrumuturi despăgubiri în valoare de 14 825 USD pentru divulgarea informațiilor cu caracter personal și a planurilor de afaceri ale acestor persoane către președintele băncii, care se afla într-o situație de conflict de interese).

Întrucât o înșelăciune săvârșită cu intenție presupune cunoașterea efectivă sau cel puțin convingerea că prezentarea este falsă, responsabilitatea poate, de asemenea, exista și pentru înșelăciunile săvârșite din culpă. În conformitate cu Restatement, oricine face o declarație falsă în exercitarea activității sale de afaceri, a profesiei sau a activității pentru care a fost angajat, sau într-o operațiune financiară poate fi considerat responsabil „în cazul în care nu acționează cu prudența sau competența rezonabilă în obținerea sau comunicarea informației” [Restatement, paragraf 552 (1)]. Spre deosebire de înșelăciunile săvârșite cu intenție, despăgubirile în cazul înșelăciunii săvârșite din culpă se limitează la prejudiciul efectiv [*Idem*, paragraf 552 B (1)].

Într-un caz recent, de exemplu, Curtea Superioară din Connecticut a decis că omisiunea unei întreprinderi furnizoare de electricitate de a declara faptul că transmisese informații cu privire la plățile efectuate de clienți către organismele de credit naționale constituie temei pentru o acțiune în justiție pentru înșelăciune (a se vedea *Brouillard v. United Illuminating Co.*, 1999 Conn. Super. LEXIS 1754). În acest caz, reclamantului i s-a refuzat creditul, deoarece pârâtul a comunicat plățile neefectuate în timp de treizeci de zile de la data facturării drept plăți întârziate. Reclamantul a susținut că nu a fost informat cu privire la această politică atunci când a încheiat cu pârâtul un contract de furnizare a energiei electrice la consumatorii casnici. Instanța a decis că „poate exista temeiul unei plângeri pentru falsificare din neglijență bazat pe lipsa declarației pârâtului atunci când acesta avea obligația să o facă”. Cazul de față demonstrează, de asemenea, că faptulou de a acționa cu bună știință sau cu intenția de a înșela nu constituie un element necesar pentru temeiul unei acțiuni în justiție pentru înșelăciune săvârșită din culpă. Astfel, o organizație din Statele Unite ale Americii care din culpă nu divulgă integral modul în care va utiliza informațiile cu caracter personal primite în conformitate cu principiile „sferei de siguranță” ar putea fi considerată ca susceptibilă să răspundă pentru înșelăciune.

În măsura în care încălcarea principiilor „sferei de siguranță” a atras după sine utilizarea abuzivă a informațiilor cu caracter personal, aceasta ar putea constitui temei pentru depunerea de către persoana ce face subiectul acelor informații a unei plângeri pentru delictul de încălcare a vieții private, recunoscut de *common law*. Dreptul american recunoaște de multă vreme motivele care justifică o acțiune în justiție pentru violarea vieții private. Într-o cauză din 1905 ([1]), Curtea Supremă din Georgia a stabilit că dreptul la protecția vieții private este înrădăcinat în principiile dreptului natural și ale *common law*, atunci când a hotărât în favoarea unui cetățean a cărui fotografie a fost utilizată de o societate de asigurări de viață fără consimțământul sau cunoștința acestuia, pentru a ilustra o reclamă comercială. Enunțând teme acum familiare jurisprudenței americane în materie de viață privată, instanța a hotărât că utilizarea fotografiei a fost „cu rea intenție”, „falsă”, și tindea să „ridiculizeze reclamantul în ochii întregii lumi” ([2]). Motivarea sentinței în cauza *Pavesich* a prevalat, cu mici variații, devenind baza dreptului american în acest domeniu. Instanțele federale au susținut în mod constant acțiunile intentate în legătură cu violarea vieții private și cel puțin patruzeci și opt de state acceptă acum pe cale jurisprudențială temeiurile pentru atari acțiuni ([3]). Pe lângă aceasta, cel puțin douăsprezece state dispun de dispoziții constituționale care garantează drepturile cetățenilor lor împotriva actelor de violare a vieții lor private ([4]), dispoziții care în unele cazuri pot fi extinse astfel încât să includă protecția împotriva amestecului unor entități neguvernmentale [a se vedea, de exemplu, *Hill v. NCAA*, 865 P.2d 633 (Ca. 1994); a se vedea și S. Ginder, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 S.D.L. Rev. 1153 (1997)]. („Constituțiile unora dintre state cuprind dispoziții cu privire la protecția vieții private care le depășesc pe cele din Constituția Statelor Unite ale Americii. Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, Carolina de Sud și Washington asigură o protecție mai largă a vieții private.”).

Second Restatement of Torts oferă o imagine autorizată a dreptului din acest domeniu. Reflectând practica juridică comună, Restatement explică faptul că „dreptul la protecția vieții private” înglobează sub această denumire patru posibilități distincte de acțiune în justiție pentru delict (a se vedea Restatement, §652A). În primul rând, o plângere privind „violarea intimității” poate fi depusă împotriva unui pârât care, în mod intenționat, încalcă, fizic sau în alt mod, solitudinea sau intimitatea unei alte persoane sau chestiunile ori preocupările personale ale acesteia ([5]). În al doilea

([1]) Pavesich contra New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

([2]) Idem, 69.

([3]) O consultare electronică a bazei de date Westlaw a găsit 2 703 de plângeri intentate în tribunalele de stat cu privire la „protecția vieții private” începând cu anul 1995. Am transmis deja Comisiei rezultatele acestui studiu.

([4]) A se vedea, de exemplu, constituțiile statelor Alaska, articolul 1 secțiunea 22; Arizona, articolul 2 secțiunea 8; California, articolul 1 secțiunea 1; Florida, articolul 1 secțiunea 23; Hawaii, articolul 1 secțiunea 5; Illinois, articolul 1 secțiunea 6; Louisiana, articolul 1 secțiunea 5; Montana, articolul 2 secțiunea 10; New York, articolul 1 secțiunea 12; Pennsylvania, articolul 1 secțiunea 1; Carolina de Sud, articolul 1 secțiunea 10 și Washington, articolul 1 secțiunea 7.

([5]) Idem, capitolul 28 secțiunea 62 B.

rând, poate fi depusă o plângere pentru „uzurpare" atunci când o persoană folosește numele sau imaginea unei alte persoane în interesul sau spre avantajul său ([1]). În al treilea rând, poate fi intentată o acțiune în instanță pentru „publicarea de fapte private" atunci când situația făcută publică este de natură să cauzeze grave prejudicii unei persoane rezonabile și nu reprezintă o preocupare legitimă pentru publicul larg ([2]). În sfârșit, poate fi intentată o acțiune în instanță pentru „publicitate mincinoasă" atunci când pârâtul, cu bună știință sau din neglijență, pune o altă persoană într-o lumină falsă în fața publicului, susceptibilă de a aduce grave prejudicii unei persoane rezonabile ([3]).

În contextul „sferei de siguranță", „violarea intimității" ar putea îngloba strângerea neautorizată de informații cu caracter personal, iar utilizarea neautorizată a informațiilor cu caracter personal în scopuri comerciale ar putea genera o plângere pentru uzurpare. În mod similar, divulgarea de date cu caracter personal inexacte ar face obiectul unui delict de „publicitate mincinoasă", în cazul în care informațiile sunt de natură să cauzeze grave prejudicii unei persoane rezonabile. În sfârșit, încălcarea vieții private care rezultă din publicarea sau divulgarea de informații cu caracter personal sensibile ar putea constitui temei de acțiune în instanță pentru „publicare de date private" (a se vedea exemple de procese reprezentative mai jos).

Cu privire la despăgubiri, încălcarea vieții private dă părții lezate dreptul la despăgubiri pentru:

(a) prejudiciul cauzat vieții sale private ca urmare a acestei încălcări;

(b) prejudiciul psihologic dovedit a fi suferit, în cazul în care acesta este de natura celor care sunt în mod normal cauzate de o asemenea încălcare;

(c) orice prejudiciu special a cărui cauză legală este încălcarea respectivă.

[Restatement, paragraf 652 (H)]. Dată fiind aplicabilitatea generală a legislației în ceea ce privește delictele civile și multitudinea plângerilor primite cu privire la diferite aspecte legate de protecția vieții private, este posibil ca persoanele ale căror interese sunt lezate ca urmare a violării vieții private ca rezultat al nerespectării principiilor „sferei de siguranță" să beneficieze de despăgubiri financiare.

Într-adevăr, instanțele federale nu mai fac față plângerilor privind încălcarea vieții private în situații analoage. De exemplu, *Ex Parte AmSouth Bancorporation et al.*, 717 So. 2d 357 a implicat o acțiune colectivă în justiție prin care împotriva pârâtului a fost formulată o plângere cu privire la faptul că „a exploatat depunătorii de fonduri fiduciare în bancă, împărtășind informații confidențiale cu privire la depunători și la conturile bancare ale acestora" pentru a permite unui afiliat al băncii să vândă fonduri de plasament și alte investiții. În asemenea cazuri se acordă deseori despăgubiri. În cauza *Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580 (D.C.App. 1985), o curte de apel a anulat decizia unei instanțe inferioare, hotărând că utilizarea fotografiilor reclamantului „înainte" și „după" intervenția de chirurgie plastică, într-o prezentare efectuată într-un mare magazin, a constituit o încălcare a vieții private prin publicarea de fapte cu caracter privat. În cauza *Candebat v. Flanagan*, 487 So.2d 207 (Miss. 1986), societatea de asigurări pârâtă a utilizat în cadrul unei campanii publicitare un accident în care soția reclamantului a fost grav rănită. Reclamantul a intentat proces pentru „încălcarea vieții private". Curtea a hotărât că reclamantul putea obține despăgubiri pentru suferință emoțională și pentru uzurparea identității. Plângerile pentru uzurpare pot fi intentate chiar în cazul în care reclamantul nu este o persoană celebră [a se vedea, de exemplu, *Staruski v. Continental Telephone Co.*, 154 Vt. 568 (1990)] (pârâtul a dobândit avantaje comerciale utilizând numele și fotografia unui angajat într-un anunț publicitar apărut într-un ziar). În cauza *Pulla v. Amoco Oil Co.*, 882 F.Supp. 836 (S.D Iowa 1995), un angajator a violat intimitatea reclamantului angajat al său punând un alt angajat să verifice extrasele cărților de credit ale acestuia pentru a verifica absențele acestuia motivate cu concediu medical. Instanța a decis că pârâtul trebuie să plătească despăgubiri de 2 USD și penalități pentru daune morale de 500 000 USD. Un alt angajator a fost declarat responsabil după ce a publicat în ziarul întreprinderii povestea unui angajat concediat pentru o presupusă falsificare a documentelor de angajare [a se vedea *Zinda v. Louisiana-Pacific Corp.*, 140 Wis.2d 277 (Wis.App. 1987)]. Povestea a constituit o încălcare a vieții private a reclamantului prin publicarea unei probleme private deoarece ziarul a circulat în rândul colegilor de serviciu. În sfârșit, un colegiu care i-a supus pe studenții săi unor teste HIV după ce le-a spus că testul era efectuat doar pentru rubeolă a fost găsit responsabil de violare a intimității [a se vedea *Doe v. High-Tech Institute, Inc.*, 972 P.2d 1060 (Colo. App. 1998)] (pentru celelalte cauze, a se vedea Restatement, paragraf 652 H, anexă).

Statele Unite ale Americii sunt deseori criticate pentru că sunt excesiv de litigioase, însă acest fapt înseamnă în același timp că persoanele pot (și chiar fac lucrul acesta) intenta acțiuni în justiție atunci când cred că au fost nedreptățite. Multe aspecte ale sistemului judiciar american înlesnesc intentarea unei acțiuni în justiție, în mod individual sau

([1]) Idem, capitolul 28 secțiunea 652 C.

([2]) Idem, capitolul 28 secțiunea 652 D.

([3]) Idem, capitolul 28 secțiunea 652 E.

colectiv. Baroul, mai numeros decât în majoritatea celorlalte țări, face ca reprezentarea profesională să fie ușor accesibilă. Avocatul acuzării care reprezintă persoanele private în procesele private își stabilește de obicei onorariile pe o bază aleatorie, ceea ce permite chiar și reclamanților cu o situație financiară precară să obțină despăgubiri. Este vorba de un factor important – de obicei, în Statele Unite ale Americii fiecare parte suportă onorariile avocaților săi și celelalte costuri. Acest sistem este diferit de cel european, unde partea care pierde suportă în mod normal și cheltuielile celeilalte părți. Fără a dezbate meritele relative ale celor două sisteme, trebuie admis faptul că regula americană pare să descurajeze mai puțin procesele intentate de persoane care nu ar fi în măsură să acopere costurile ambelor părți în cazul în care ar pierde procesul.

Persoanele pot intenta un proces chiar dacă revendicările sunt relativ mici. Majoritatea, dacă nu toate jurisdicțiile din Statele Unite ale Americii, dispun de instanțe inferioare care garantează proceduri simplificate, cu cheltuieli mai mici, pentru litigiile aflate sub limitele fixate de lege ([1]). Posibilitatea daunelor morale oferă de asemenea o compensație financiară persoanelor care au suferit într-o mică măsură un prejudiciu direct și care intentează un proces pentru comportament reprehensibil. De asemenea, persoanele care au fost lezate în același mod își pot reuni resursele și reclamațiile pentru a intenta un proces colectiv.

Un bun exemplu cu privire la capacitatea persoanelor de a intenta proces pentru a obține despăgubiri îl constituie litigiul în curs de desfășurare împotriva Amazon.com pentru încălcarea vieții private. Amazon.com, marele comerciant cu amănuntul on-line, este pârât în cadrul unei acțiuni colective, în care aceștia susțin că nu au fost informați și nu și-au dat acordul cu privire la strângerea de informații cu caracter personal despre ei atunci când au utilizat un program software deținut de Amazon și denumit „Alexa." În această cauză, reclamanții au invocat încălcarea Computer Fraud and Abuse Act sub forma accesului ilegal la comunicările lor stocate precum și a Electronic Communications Privacy Act pentru interceptarea ilegală a comunicărilor lor electronice și telefonice. De asemenea, au invocat și încălcarea vieții private în temeiul *common law*. Această acțiune decurge dintr-o plângere depusă de un expert în probleme de siguranță a internetului în decembrie. Cererea de despăgubire se ridică la suma de 1 000 USD pentru fiecare persoană, plus onorariile avocaților și profitul obținut ca urmare a încălcării legislației. Dat fiind faptul că numărul membrilor grupului de reclamanți ar putea să se ridice la câteva milioane, despăgubirile ar putea totaliza miliarde de dolari. FTC anchetează, de asemenea, plângerile.

Legislația federală și statală privind viața privată oferă deseori motive private de acțiuni în instanță în materie de prejudiciu financiar.

Pe lângă faptul că ea dă naștere răspunderii civile delictuale, încălcarea principiilor „sferei de siguranță" poate, de asemenea, contraveni uneia sau alteia dintre sutele de legi federale și statale cu privire la protecția vieții private. Multe din aceste legi, care privesc prelucrarea informațiilor cu caracter personal atât de organisme guvernamentale, cât și de sectorul privat, fac posibilă intentarea de procese în vederea obținerii de despăgubiri atunci când indivizii sunt victime ale încălcării legilor. De exemplu:

Electronic Communications Privacy Act din 1986. Această lege (ECPA) interzice interceptarea neautorizată a convorbirilor pe telefoane celulare și a transmisiilor de la calculator la calculator. Încălcarea acestor dispoziții poate avea ca rezultat o răspundere civilă de cel puțin 100 USD pentru fiecare zi în care sunt încălcate dispozițiile. Protecția pe care o oferă ECPA include și accesul neautorizat sau divulgarea comunicațiilor electronice înregistrate. Contravenienții sunt responsabili de prejudiciile provocate sau de pierderea profiturilor suferite în urma încălcării dispozițiilor din acest act.

Telecommunications Act din 1996. În conformitate cu alineatul (702), informațiile privind abonații telefonici [Customer proprietary network informatiom (CPNI)] nu pot fi utilizate în alt scop decât acela de a furniza servicii de telecomunicație. Abonații acestor servicii pot fie să depună o plângere la Federal Communications Commission, fie să intenteze un proces la instanța federală districtuală pentru a obține despăgubiri și recuperarea onorariilor avocaților.

Consumer Credit Reporting Reform Act din 1996. Legea din 1996 a modificat Fair Credit Reporting Act din 1970 (FCRA) pentru a cere îmbunătățirea informației și a dreptului de acces al persoanelor la credite. De asemenea, Reform Act a impus noi restricții revânzătorilor de informații privind creditele de consum. Consumatorii pot obține despăgubiri și recuperarea onorariilor avocaților pentru încălcarea acestor dispoziții.

([1]) Am transmis deja Comisiei informații cu privire la acțiunile din instanțele inferioare.

Legile statale protejează, de asemenea, viața privată într-o serie largă de situații. Printre domeniile în care statele au luat măsuri sunt extrasele bancare, abonamentele la operatorii de servicii de televiziune prin cablu, informațiile privind creditele, documentele de angajare, arhivele administrative, informațiile genetice și dosarele medicale, informațiile cu privire la asigurări, dosarele școlare, comunicațiile electronice și închirierea de casete video ([1]).

B. **Autorizări legale exprese**

Principiile „sferei de siguranță" conțin o excepție atunci când legile, reglementările sau jurisprudența instituie „obligații contradictorii sau autorizări exprese, cu condiția ca la data acestor autorizări, o organizație să poată demonstra că nerespectarea principiilor este limitată în măsura necesară satisfacerii intereselor legitime principale stabilite de această autorizație". În mod evident, în cazurile în care legislația Statelor Unite ale Americii impune o obligație conflictuală, organizațiile din Statele Unite ale Americii care fac parte sau nu din „sfera de siguranță" trebuie să se conformeze acestei legislații. În ceea ce privește autorizațiile exprese, deși principiile „sferei de siguranță" sunt destinate să restrângă diferențele dintre sistemul din Statele Unite ale Americii și cel european cu privire la protecția vieții private, trebuie să respectăm prerogativele legislative ale legislatorilor pe care i-am ales. Excepția limitată de la respectarea strictă a principiilor „sferei de siguranță" încearcă să stabilească un echilibru pentru a ține seama de interesele legitime ale fiecărei părți.

Excepția se limitează la cazurile în care există o autorizație expresă. În consecință, ca situație limită, legislația, reglementarea sau decizia judecătorească pertinentă trebuie să autorizeze în mod afirmativ o anumită conduită a organizațiilor care aderă la „sfera de siguranță" ([2]). Cu alte cuvinte, această excepție nu se va aplica atunci când legea nu dispune. Pe lângă aceasta, excepția nu se va aplica decât în cazul în care autorizația expresă vine în conflict cu respectarea principiilor „sferei de siguranță". Chiar și în aceste condiții, excepția „este limitată în măsura necesară satisfacerii intereselor legitime principale stabilite de această autorizație". De exemplu, în cazul în care legea autorizează în mod simplu o societate comercială să furnizeze informații cu caracter personal organismelor guvernamentale, excepția nu se aplică. Pe de altă parte, atunci când legea autorizează în mod expres societatea comercială să furnizeze informații cu caracter personal organismelor guvernamentale fără acordul persoanei, aceasta ar constitui o „autorizație expresă" de a acționa într-un mod care contravine principiilor „sferei de siguranță". De altfel, excepțiile specifice de la cerințele privind notificarea și consimțământul s-ar încadra în domeniul de aplicare al excepției (echivalând cu o autorizație specifică de divulgare a informației fără notificare și consimțământ). De exemplu, o lege care îi autorizează pe medici să furnizeze dosarele medicale cu privire la pacienții lor autorităților sanitare fără acordul prealabil al acestor pacienți ar putea permite o excepție de la principiul notificării și principul opțiunii. Această autorizație nu ar permite unui doctor să furnizeze aceleași dosare medicale organizațiilor de protecție a sănătății sau laboratoarelor de cercetare farmaceutică, acesta nefiind unul din scopurile autorizate de lege și prin urmare nefăcând parte din domeniul de aplicare a excepției ([3]). Autorizația în cauză poate fi o autorizație „autonomă" de a face anumite lucruri cu informațiile cu caracter personal, dar, după cum ilustrează exemplele de mai jos, este mai probabil ca ea să fie o excepție de la o lege mai vastă care interzice colectarea, utilizarea sau divulgarea informațiilor cu caracter personal.

Telecommunications Act din 1996

În majoritatea cazurilor, utilizările autorizate fie sunt conforme cu cerințele directivei și cu principiile, fie sunt autorizate de una sau alta dintre excepțiile permise. De exemplu, alineatul (702) din Telecommunications Act (codificat în 47 U.S.C. § 222) impune operatorilor de telecomunicații obligația de a respecta confidențialitatea informațiilor cu caracter personal pe care le obțin pe parcursul perioadei în care furnizează servicii clienților. Această dispoziție permite operatorilor de telecomunicații:

(1) să utilizeze informațiile despre clienți pentru a furniza servicii de telecomunicații și în special pentru a publica registrele de abonați;

(2) să ofere informații despre clienți unor terți la cererea în scris a clienților și

(3) să ofere informații despre clienți în formă agregată.

([1]) O consultare electronică recentă a bazei de date Westlaw a găsit 994 de cauze de despăgubiri și încălcarea vieții private judecate la nivelul statelor membre ale federației.

([2]) Ca element de clarificare, autoritatea juridică pertinentă nu va trebui să facă referire în mod specific la principiile „sferei de siguranță".

([3]) În mod similar, medicul din acest exemplu nu s-ar putea bizui pe o autorizare legală pentru a nu lua în considerare opțiunea pe care o oferă FAQ 12 indivizilor de a refuza marketing-ul direct. Câmpul de aplicare al oricărei excepții pentru „autorizările exprese" este în mod necesar limitat la câmpul de aplicare al autorizației în conformitate cu legea în materie.

[A se vedea 47 U.S.C. § 222 (c) (1)-(3).] De asemenea, legea permite operatorilor de telecomunicații o excepție în utilizarea informațiilor despre clienți:

(1) pentru punerea în funcțiune, prestarea, facturarea și încasarea pentru serviciile lor;

(2) pentru protecția împotriva comportamentelor frauduloase, abuzive sau ilegale și

(3) pentru furnizarea serviciilor de vânzare de bunuri prin telefon, de asistență sau administrative în timpul unui apel inițiat de client [1].

[*Idem*, § 222 (d) (1)-(3).] În cele din urmă, operatorii de telecomunicații au obligația de a furniza editorilor de cărți de telefon informații privind lista abonaților lor, care pot include doar numele, adresele, numerele de telefon și domeniul de activitate în cazul clienților comerciali [*idem*, § 222e)].

Excepția privind „autorizările exprese" s-ar putea aplica atunci când operatorii de telecomunicații utilizează CPNI pentru a preveni frauda sau orice alt comportament ilegal. Chiar și în acest caz, asemenea acțiuni ar putea fi considerate „de interes public" și autorizate de principii din acest motiv.

Reglementări propuse de Departamentul Sănătății și Serviciilor Umane

Department of Health and Human Services (HHS) a propus reglementări cu privire la standardele privind confidențialitatea informațiilor medicale identificabile individual [a se vedea 64 Fed. Reg. 59.918 (2 noiembrie 1999) (urmează să fie codificat la 45 C.F.R. punctele 160-164)]. Aceste norme ar consta în punerea în aplicare a dispozițiilor cu privire la confidențialitatea din Health Insurance Portability and Accountability Act din 1996, Pub. L. 104-191. Normele propuse ar interzice în mod normal organismelor aflate în domeniul de aplicare (planuri sanitare, centre de documentare sanitară și prestatori de servicii de îngrijire sanitară care transmit informații medicale în format electronic) să utilizeze sau să divulge informații medicale fără autorizarea persoanelor private (a se vedea propunerea 45 C.F.R. paragraf 164.506). Normele propuse nu ar autoriza divulgarea informațiilor medicale protejate decât pentru două motive: (1) pentru a permite persoanelor să consulte și să copieze informații medicale despre ele însele (*idem*, paragraf 164.514) și (2) pentru a pune în aplicare normele (*idem*, paragraf 164.522).

Normele propuse ar permite utilizarea sau divulgarea informațiilor medicale protejate, fără o autorizație expresă dată de persoană, într-un număr limitat de circumstanțe. Acestea includ, de exemplu, supravegherea sistemului de sănătate, punerea în aplicare a legislației și urgențele (*idem,* paragraf 164.510). Normele propuse stabilesc în detaliu limitele acestor utilizări și divulgări. Mai mult, utilizările și divulgările autorizate de informații medicale protejate ar fi limitate la minimul necesar de informații (*idem,* paragraf 164.506).

Utilizările expres autorizate de reglementările propuse sunt în general conforme cu principiile „sferei de siguranță" sau, în caz contrar, sunt permise de o altă excepție. De exemplu, punerea în aplicare a legislației și administrarea judiciară sunt permise, precum și cercetarea medicală. Alte utilizări, precum supravegherea sistemului de sănătate, funcția sănătății publice și sistemele de informare sanitară naționale, sunt de interes public. Divulgările în vederea prelucrării contribuțiilor și scutirilor sanitare sunt necesare pentru garantarea asistenței sanitare. Utilizările în caz de urgență pentru consultarea unei rude apropiate cu privire la un tratament în cazul în care consimțământul pacientului „nu poate fi obținut în mod practic sau rezonabil" sau pentru stabilirea identității sau a cauzei decesului defunctului, protejează interesele vitale ale persoanei în cauză și ale altor persoane. Utilizările pentru gestionarea personalului militar activ și a altor categorii speciale de persoane facilitează îndeplinirea corectă a misiunii militare sau a altor situații critice similare; în orice caz, asemenea utilizări au un impact limitat, poate chiar nul, asupra consumatorilor în general.

Este autorizată doar utilizarea informațiilor cu caracter personal de către structurile sanitare în vederea întocmirii listelor de pacienți. În cazul în care o asemenea utilizare nu poate fi caracterizată ca fiind de interes „vital", listele de pacienți sunt în beneficiul pacienților, precum și al prietenilor și rudelor acestora. De asemenea, domeniul de aplicare

[1] Sfera de aplicare a acestei excepții este extrem de limitată. Conform dispozițiilor, operatorul de telecomunicații poate utiliza CPNI numai în timpul unei convorbiri inițiate de client. Mai mult, am fost informați de FCC că operatorul de telecomunicații nu poate utiliza CPNI pentru comercializarea serviciilor din afara cadrului cererii clientului. În sfârșit, întrucât clientul trebuie să aprobe utilizarea CPNI în acest scop, această dispoziție nu constituie în realitate o „excepție".

al acestei utilizări autorizate este limitat. În consecință, recurgerea la excepția de la principii pentru utilizările „în mod expres autorizate" de lege în acest scop prezintă un risc minim pentru viața privată a pacienților.

Fair Credit Reporting Act

Comisia Europeană și-a exprimat îngrijorarea cu privire la faptul că excepția „autorizărilor exprese" ar „obliga la stabilirea în mod efectiv a caracterului adecvat" al Fair Credit Reporting Act (FCRA). Nu este cazul. În absența constatării specifice a caracterului adecvat al FCRA, organizațiile din Statele Unite ale Americii care altminteri s-ar bizui pe această constatare trebuie să promită că aderă în toate privințele la principiile „sferei de siguranță". Aceasta înseamnă că atunci când cerințele FCRA depășesc nivelul de protecție oferit de principii, organizațiile din Statele Unite ale Americii trebuie să respecte doar FCRA. Pe de altă parte, atunci când FCRA se poate dovedi insuficient, organizațiile trebuie să pună practicile lor de informare în conformitate cu principiile. Excepția nu ar trebui să modifice această evaluare de bază. Prin natura dispozițiilor sale, excepția se aplică numai atunci când legea relevantă autorizează expres o conduită care contravine principiilor „sferei de siguranță". Excepția nu s-ar aplica în situațiile în care cerințele FCRA nu îndeplinesc principiile „sferei de siguranță" ([1]).

Cu alte cuvinte, prin „excepție" nu înțelegem că ceea ce nu este obligatoriu ar fi „autorizat în mod expres". Pe de altă parte, excepția se aplică numai atunci când ceea ce este autorizat în mod expres de legislația americană vine în contradicție cu dispozițiile din principiile „sferei de siguranță". Legea pertinentă trebuie să răspundă acestor două elemente înainte de a autoriza nerespectarea principiilor.

Paragraful 604 din FCRA autorizează, de exemplu, în mod expres publicarea de către agențiile de informare cu privire la consumatori a rapoartelor de consumatori în diferite situații enumerate (FCRA, paragraf 604). Prin aceasta, paragraful 604 autorizează agențiile de informare cu privire la credite să acționeze în contradicție cu principiile „sferei de siguranță", ceea ce ar avea ca efect obligativitatea agențiilor de informare cu privire la credite de a apela la excepție (exceptând, desigur, cazurile în care se aplică o altă excepție). Agențiile de informare cu privire la credite trebuie să se supună hotărârilor judecătorești și citațiilor emise de marele juriu, iar utilizarea dosarelor de credit de către organele autorizate, organismele sociale și organismele de susținere a copilului are o finalitate publică [*idem*, § 604 (a) (1), (3) (D) și (4)]. În consecință, agenția de informare cu privire la credite nu ar trebui să recurgă la excepția „autorizării exprese" în acest scop. Atunci când acționează în conformitate cu instrucțiunile scrise ale consumatorului, agenția de informare cu privire la consumatori respectă integral principiile „sferei de siguranță" [*idem*, § 604 (a) (2). În același mod, dosare referitoare la consum pot fi obținute în scopuri de angajare numai pe baza autorizației scrise din partea consumatorului [*idem*, §§ 604 (a) (3) (B) și (b) (2) (A) (ii)] iar pentru operațiuni de credit sau de asigurări care nu sunt angajate de consumator numai în cazul în care acesta nu și-a exprimat dezacordul cu privire la aceste solicitări [*id*em, § 604 (c) (1) (B)]. De asemenea, FCRA interzice agențiilor de informare cu privire la credite să furnizeze informații medicale în scopul angajării fără consimțământul consumatorului [*idem*, § 604 (g)]. Aceste utilizări sunt conforme principiilor notificării și opțiunii. Celelalte scopuri autorizate de paragraful 604 privesc operațiile care îl implică pe consumator și din acest motiv ar fi permise de principii [*idem*, § 604 (a) (3) (A) și (F)].

Ultima utilizare „autorizată" de paragraful 604 se referă la piețele de credit secundare [*idem*, § 604 (a) (3) (E)]. Nu există un conflict între utilizarea dosarelor consum în acest scop și principiile „sferei de siguranță" ca atare. Este adevărat că FCRA nu impune agențiilor de informare cu privire la credite, de exemplu, să notifice consumatorii și să le solicite consimțământul atunci când publică rapoarte în acest scop. Cu toate acestea, reamintim că absența unei cerințe nu înseamnă „autorizare expresă" de a acționa într-o manieră contrară celei care a fost stabilită. În mod similar, paragraful 608 autorizează furnizarea de către agențiile de informare cu privire la credite a anumitor informații cu caracter personal organismelor guvernamentale. Această „autorizare" nu ar justifica faptul că o agenție de informare cu privire la credite își ignoră angajamentele de a adera la principiile „sferei de siguranță". Acest fapt contrastează cu celelalte exemple ale noastre în care excepțiile de la principiile notificării afirmative și posibilității opțiunii sunt invocate pentru a autoriza în mod expres utilizarea de date cu caracter personal fără notificare și opțiune.

Concluzie

Din analiza, oricât de limitată ar fi, a acestor acte legislative se desprind câteva linii distincte:

— „Autorizația expresă" permite în general utilizarea sau divulgarea informațiilor cu caracter personal fără acordul prealabil al persoanei în cauză; astfel, excepția s-ar limita la principiile notificării și opțiunii;

([1]) Prezenta analiză nu trebuie înțeleasă ca o recunoaștere a faptului că FCRA nu oferă un nivel „adecvat" de protecție. Orice evaluare a FCRA trebuie să ia în considerare protecția oferită de lege în ansamblul său și nu să se concentreze exclusiv asupra excepțiilor, cum se întâmplă în cazul de față.

— în majoritatea cazurilor, excepțiile autorizate de lege sunt formulate în manieră restrictivă pentru a se aplica în situații concrete pentru scopuri bine stabilite. De altfel, legea interzice utilizarea sau divulgarea neautorizate a informațiilor cu caracter personal care nu se încadrează în aceste limite;

— în majoritatea cazurilor, reflectând caracterul lor legislativ, utilizarea sau divulgarea autorizată servește unui interes public;

— în aproape toate cazurile, utilizările autorizate sunt fie pe deplin conforme cu principiile „sferei de siguranță", fie respectă cerințele pentru una dintre excepțiile autorizate.

În concluzie, excepția privind „autorizările exprese" din lege va fi, prin natura ei, destul de limitată în domeniul său de aplicare.

C. **Fuziuni și absorbții**

Grupul de lucru prevăzut la articolul 29 și-a exprimat îngrijorarea cu privire la situațiile în care o organizație din cadrul „sferei de siguranță" este absorbită sau fuzionează cu o întreprindere care nu și-a luat angajamentul de a respecta principiile „sferei de siguranță". Se pare că grupul de lucru a presupus că firma supraviețuitoare nu ar avea obligația de a aplica principiile „sferei de siguranță" la informațiile cu caracter personal deținute de firma care este absorbită, însă lucrurile nu stau neapărat așa în legislația Statelor Unite ale Americii. Regula generală în Statele Unite ale Americii în ceea ce privește fuziunile și absorbțiile este aceea că o societate comercială care achiziționează capitalul unei alte societăți comerciale își asumă în general obligațiile și responsabilitățile societății comerciale achiziționate [a se vedea 15 *Fletcher Cyclopedia of the Law of Private Corporations* § 7117 (1990); a se vedea, de asemenea, *Model Bus. Corp. Act* § 11.06 (3) (1979)] („societății comerciale supraviețuitoare îi revin toate responsabilitățile fiecărei societăți comerciale care participă la fuziune"). Cu alte cuvinte, întreprinderea supraviețuitoare în urma unei fuziuni sau absorbții a unei organizații aderente la „sfera de siguranță" prin această metodă este obligată să respecte angajamentele acesteia din urmă în ceea ce privește „sfera de siguranță".

Pe lângă aceasta, chiar dacă fuziunea sau absorbția a fost efectuată prin achiziția de active, responsabilitățile întreprinderii achiziționate ar putea deveni obligatorii pentru societatea comercială care a achiziționat-o în anumite circumstanțe (15 *Fletcher*, § 7122). Chiar și atunci când responsabilitățile nu au supraviețuit fuziunii, trebuie remarcat că ele nu ar supraviețui unei fuziuni în care datele au fost transferate din Europa în conformitate cu un contract – singura alternativă viabilă în afara „sferei de siguranță" pentru transferurile de date în Statele Unite ale Americii. Pe lângă aceasta, documentele „sferei de siguranță" așa cum sunt ele revizuite, prevăd că orice organizație din cadrul „sferei de siguranță" trebuie să informeze Departamentul Comerțului în legătură cu orice achiziție și să permită datelor să continue să fie transferate organizației succesoare numai în cazul în care organizația succesoare aderă la „sfera de siguranță" (a se vedea FAQ 6). Într-adevăr, Statele Unite ale Americii au revizuit în prezent cadrul „sferei de siguranță" pentru a cere organizațiilor din Statele Unite ale Americii care se găsesc în această situație să șteargă informațiile pe care le-au primit în temeiul „sferei de siguranță" în cazul în care angajamentele lor în ceea ce privește „sfera de siguranță" nu sunt menținute sau în cazul în care nu sunt puse în practică măsuri adecvate de salvgardare.

ANEXA V

14 iulie 2000

John Mogg
Director, DG XV
Comisia Europeană
Birou C 107-6/72
Rue de la Loi/Wetstraat 200
B – 1049 Bruxelles

Stimate domnule Mogg,

Înțeleg că în urma scrisorii pe care v-am adresat-o la 29 martie 2000 au apărut o serie de întrebări. Pentru a clarifica atribuțiile Comisiei Federale pentru Comerț (FTC) în anumite domenii, vă trimit prezenta scrisoare care, pentru a facilita schimburile noastre viitoare, completează și recapitulează conținutul corespondenței noastre de până acum.

În cadrul vizitelor efectuate la birourile noastre, precum și în corespondența dumneavoastră anterioară, ați ridicat mai multe întrebări privind autoritatea Comisiei Federale pentru Comerț (FTC) a Statelor Unite ale Americii cu privire la protecția vieții private pe internet. Am considerat că ar fi util să rezum răspunsurile mele precedente astfel încât să vă furnizez informații suplimentare cu privire la competența FTC în ceea ce privește problemele legate de protecția vieții private a consumatorului pe care le-ați menționat în ultima dumneavoastră scrisoare. Mai precis, doriți să știți: (1) dacă FTC dispune de competență în ceea ce privește transferurile de date legate de angajări în cazul în care acestea sunt efectuate în contradicție cu principiile „sferei de siguranță" din Statele Unite ale Americii; (2) dacă FTC dispune de competență în ceea ce privește programele „seal" cu scop nelucrativ de protecție a vieții private; (3) dacă Federal Trade Commission Act se aplică atât datelor on-line cât și datelor off-line și (4) ce se întâmplă atunci când atribuțiile FTC se suprapun peste cele ale altor organe însărcinate cu aplicarea legii.

Aplicarea FTC Act în cazul protecției vieții private

Competența legală a Comisiei Federale pentru Comerț în acest domeniu este definită la articolul 5 din Federal Trade Commission Act („FTC Act"), care interzice actele sau practicile neloiale sau frauduloase din comerț sau care afectează comerțul [1]. Prin „practică frauduloasă" se înțelege o prezentare, omisiune sau practică susceptibilă de a induce cu adevărat consumatorii în eroare. O practică este considerată neloială în cazul în care cauzează sau este susceptibilă să cauzeze un prejudiciu grav consumatorilor, care nu poate fi evitat și care nu este compensat prin avantaje pentru consumatori sau concurență [2].

Anumite metode de strângere a datelor sunt susceptibile de a încălca FTC Act. De exemplu, în cazul în care un site de internet afirmă în mod fals că respectă o politică privind protecția vieții private sau o serie de principii de autoreglementare, articolul 5 din FTC Act oferă o bază juridică ce permite atacarea acestei prezentări eronate ca fiind frauduloasă. Într-adevăr, aplicarea cu succes a legii ne-a permis să stabilim acest principiu [3]. Pe lângă aceasta, FTC consideră că poate contesta practicile care aduc atingere grav protecției vieții private atunci când acestea privesc copii sau utilizarea de informații foarte sensibile precum registrele financiare [4] sau dosarele medicale. Comisia Federală pentru Comerț va continua să vegheze la aplicarea legii bazându-se pe acțiunile noastre de supraveghere și investigare, precum și pe trimiterile pe care le primim de la organizațiile de autoreglementare și altele, inclusiv statele membre ale Uniunii Europene.

---

(1) 15 U.S.C. § 45. Fair Credit Reporting Act s-ar aplica și în cazul colectării și vânzării datelor internet care corespund definițiilor legale ale noțiunilor de „raport privind consumatorii" și „agenție de studiu al consumului".

(2) 15 U.S.C. § 45 (n).

(3) A se vedea GeoCities, dosar nr. C-3849 (sentință definitivă din 12 februarie 1999) (www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., dosar nr. C-3891 (sentință definitivă din 12 august 1999) (www.ftc.gov/opa/1999/9905/younginvestor.htm). A se vedea, de asemenea, Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. partea 312 (www.ftc.gov/opa/1999/9910/childfinal.htm). Regulamentul COPPA, care a intrat în vigoare luna trecută, prevede că operatorii de site-uri internet care se adresează copiilor sub 13 ani sau care strâng cu bună știință informații cu caracter personal de la copii sub 13 ani trebuie să aplice principiile codului deontologic al informației enunțate în regulament.

(4) A se vedea *FTC v. Touch Tone, Inc.*, cauza civilă nr. 99-WM-783 (D.Co.) (înregistrată la 21 aprilie 1999) (www.ftc.gov/opa/1999/9904/touchtone.htm). Avizul personalului din 17 iulie 1997, emis ca răspuns la o petiție depusă de Center for Media Education (www.ftc.gov/os/1997/9707/cenmed.htm).

Contribuția la autoreglementare

FTC va acorda prioritate cazurilor de încălcare a principiilor de autoreglementare primite din partea organizațiilor precum BBBOnline și TRUSTe (1). Această abordare ar fi în conformitate cu relațiile pe care le avem de vreme îndelungată cu National Advertising Review Board (NARB) din cadrul Better Business Bureau, care transmite FTC plângerile cu privire la publicitate. National Advertising Division (NAD) din cadrul NARB soluționează plângerile cu privire la publicitate la nivel național pe calea arbitrajului. Atunci când o parte refuză să se conformeze deciziei NAD, cauza este transmisă către FTC. Personalul FTC analizează, cu titlu prioritar, publicitatea contestată pentru a stabili dacă aceasta contravine FTC Act și deseori reușește cu succes să oprească practica incriminată sau să convingă partea interesată să respecte procesul NARB.

În mod similar, FTC acordă prioritate cazurilor de nerespectare a principiilor „sferei de siguranță" prezentate de statele membre ale Uniunii Europene. Ca și în situația cererilor primite din partea organizațiilor de autoreglementare din Statele Unite ale Americii, colaboratorii noștri vor lua în considerare orice informații prin care se poate stabili dacă acea practică constituie o încălcare a articolului 5 din legea FTC Act. Acest angajament este exprimat și în principiile „sferei de siguranță" (întrebare frecventă referitoare la punerea în aplicare a deciziilor – FAQ 11).

GeoCities: Primul caz de nerespectare a protecției vieții private pe internet tratat de FTC

Primul caz de nerespectare a protecției vieții private pe internet, GeoCities, a fost tratat de Comisia Federală pentru Comerț în temeiul articolului 5(5) (2). În această cauză, FTC a declarat că GeoCities a prezentat într-o manieră falsă, atât adulților cât și copiilor, modalitatea în care utiliza datele lor cu caracter personal. În conformitate cu plângerea Comisiei Federale pentru Comerț, GeoCities a declarat că anumite date cu caracter personal pe care le-a obținut pe site-ul său nu erau destinate decât utilizării în scopuri interne sau pentru a trimite consumatorilor oferte promoționale, pentru a le furniza produse sau servicii care răspundeau cererilor acestora și că datele suplimentare „opționale" nu ar fi divulgate fără acordul consumatorului. În realitate, aceste informații au fost divulgate unor terți care le-au utilizat pentru a trimite membrilor solicitări, altele decât cele la care aceștia și-au dat acordul. De asemenea, plângerea acuza societatea comercială GeoCities de recurgere la practici frauduloase cu privire la obținerea de informații de la copii. GeoCities a fost, de asemenea, acuzată că recurge la practici frauduloase în ceea ce privește strângerea de informații de la copii. Societatea comercială GeoCities a declarat că gestionează pe site-ul său de internet pagini rezervate copiilor și că informațiile obținute aici sunt păstrate de societatea comercială. În realitate, aceste pagini de pe site erau gestionate de terți care colectau și păstrau informațiile.

Hotărârea prin care a fost soluționat litigiul interzice societății comerciale GeoCities să prezinte în mod deformat scopurile în care colectează sau utilizează informațiile cu caracter personal de la sau despre consumatori, inclusiv copii. În conformitate cu ordinul, societatea comercială trebuie să afișeze pe site-ul său un anunț clar și inteligibil cu privire la protecția vieții private în care să indice consumatorilor ce informații sunt colectate și în ce scop, cui vor fi acestea divulgate și cum pot consumatorii accesa și șterge aceste date. Pentru a asigura un control parental, GeoCities trebuie să obțină acordul părinților înainte de a colecta informații cu caracter personal de la copii sub 12 ani. GeoCities are obligația de a-și informa membrii și de a le oferi posibilitatea de a șterge informațiile care îi privesc din bazele de date ale GeoCities și ale terților. Hotărârea de soluționare a litigiului prevede în mod expres că GeoCities trebuie să informeze părinții copiilor sub 12 ani și să șteargă informațiile legate de aceștia în cazul în care unul dintre părinți nu și-a dat acordul pentru păstrarea și utilizarea acestor date. În sfârșit, GeoCities trebuie să solicite terților cărora le-a divulgat informații ștergerea acestor informații (3).

ReverseAuction.com

Această agenție a formulat de curând o acțiune privind pretinsa încălcare a vieții private de către o altă societate comercială care operează pe internet. În ianuarie 2000, Comisia a declarat admisibilă plângerea depusă împotriva ReverseAuction.com și a aprobat încheierea unei înțelegeri cu aceasta. S-a pretins că acest site de licitații on-line a obținut date de identificare cu caracter personal ale consumatorilor de la un site concurent (eBay.com), iar apoi a trimis prin poșta electronică mesaje înșelătoare și nesolicitate consumatorilor interesați de activitățile lor (4). În plângerea

(1) Într-adevăr, FTC a depus recent plângere la o curte federală împotriva TRUSTe, Toysmart.com, cerând să fie luate măsuri de constrângere pentru a împiedica vânzarea de informații nominale (în ceea ce privește clienții) pe care această societate le strângea pe site-ul său internet încălcând propriile sale principii de protecție a vieții private. FTC a fost informat direct de TRUSTe de această infracțiune. *FTC v. Toysmart.com, LLC*, cauza civilă nr. 00-11341-RGS (D.Ma.), înregistrată la 11 iulie 2000 (www.ftc.gov/os/2000/07/toysmart.htm).

(2) GeoCities, dosar nr. C-3849 (sentința definitivă din 12 februarie 1999) (www.ftc.gov/os/1999/9902/9823015d%26o.htm).

(3) Ulterior, FTC a soluționat o altă cauză privind colectarea pe internet de date cu caracter personal de la copii. Liberty Financial Companies Inc. administra site-ul Internet Young Investor, care se adresa copiilor și adolescenților și era axat pe probleme financiare și de investiții. FTC a subliniat că site-ul declara în mod fals că informațiile cu caracter personal obținute de la copii în cadrul unei anchete vor fi păstrate anonime și că participanții vor primi un buletin informativ electronic precum și premii. În realitate, datele cu caracter personal cu privire la copii și la situația financiară a familiilor lor au fost păstrate în manieră identificabilă și nu au fost trimise nici buletine și nici premii. Acordul de consimțământ interzice asemenea prezentări eronate pe viitor și obligă Liberty Financial să includă pe site-urile sale pentru copii o notă privind protecția vieții private și să obțină consimțământul verificabil al părinților înainte de a colecta date cu caracter personal de la copii. *Liberty Financial Cos.*, cauza nr. C-3891 (sentința definitivă din 12 august 1999) (www.ftc.gov/opa/1999/9905/younginvestor.htm).

(4) A se vedea *ReverseAuction.com, Inc.*, cauza civilă nr. 000032 (D.D.C.) (înregistrată la 6 ianuarie 2000) (comunicatul de presă și actele de procedură pot fi consultate la următoarea adresă: www.ftc.gov/opa/2000/01/reverse4.htm).

noastră am arătat că ReverseAuction a încălcat articolul 5 din FTC Act prin obținerea de date de identificare cu caracter personal care includeau adresele de poștă electronică și codurile personale de identificare ale utilizatorilor site-ului eBay, precum și prin trimiterea către aceștia de mesaje electronice frauduloase.

După cum se arată în plângere, înainte de a obține aceste informații, ReverseAuction s-a înregistrat ca utilizator al eBay și a acceptat să respecte acordul privind utilizatorii și politica de protecție a vieții private. Acordul și politica protejează viața privată a consumatorilor, interzicând utilizatorilor eBay să colecteze și să utilizeze date de identificare cu caracter personal în scopuri neautorizate, cum ar fi trimiterea de mesaje electronice comerciale nesolicitate. În consecință, plângerea noastră a susținut în primul rând că ReverseAuction a mințit că va respecta acordul privind utilizatorii și politica de protecție a vieții private ale eBay, ceea ce constituie o practică frauduloasă în temeiul articolului 5. Alternativ, plângerea a susținut că utilizarea acestor date de către ReverseAuction pentru a trimite mesaje electronice comerciale nesolicitate, în contradicție cu acordul privind utilizatorii și politica de protecție a vieții private a constituit o practică comercială neloială în temeiul articolului 5.

În al doilea rând, plângerea a susținut că mesajele electronice trimise consumatorilor conțineau o informație înșelătoare în subiectul mesajului, fiecare destinatar fiind informat că respectivul său cod de identificare pentru eBay „va expira în curând". În sfârșit, plângerea a susținut că mesajele electronice lăsau să se înțeleagă, în mod fals, că eBay a furnizat în mod direct sau indirect societății comerciale ReverseAuction date de identificare cu caracter personal cu privire la utilizatorii eBay sau că a participat la difuzarea mesajelor e-mail nesolicitate.

Înțelegerea de soluționare a litigiului obținută de FTC interzice societății comerciale ReverseAuction să comită asemenea infracțiuni pe viitor. De asemenea, obligă societatea comercială ReverseAuction să notifice consumatorii care, ca urmare a primirii mesajelor prin poștă electronică trimise de ReverseAuction, s-au înscris sau se vor înscrie la ReverseAuction. Notificarea îi informează pe consumatori că respectivele lor coduri personale de identificare pentru eBay nu urmează să expire și că eBay nu a cunoscut și nu a autorizat difuzarea de către ReverseAuction a mesajelor electronice nesolicitate. Notificarea oferă, de asemenea, acestor consumatori posibilitatea de a anula înscrierea la ReverseAuction și de a șterge informațiile cu caracter personal din baza de date a societății comerciale ReverseAuction. Pe lângă aceasta, hotărârea obligă ReverseAuction să șteargă informațiile cu caracter personal ale membrilor eBay care au primit mesajele electronice ale societății comerciale ReverseAuction dar nu s-au abonat la aceasta și interzice utilizarea sau divulgarea acestor date. În sfârșit, în conformitate cu deciziile anterioare obținute de FTC în ceea ce privește protecția vieții private, hotărârea cere ca ReverseAuction să-și publice principiile privind protecția vieții private pe site-ul său internet și cuprinde dispoziții exhaustive cu privire la înregistrarea datelor pentru a permite FTC să supravegheze punerea în aplicare a acestor principii.

Cauza ReverseAuction demonstrează că FTC este hotărâtă să ia măsuri de executare pentru a consolida codurile de auto-reglementare aplicate de întreprinderi în ceea ce privește protecția vieții private a consumatorilor pe internet. Hotărârea dată în acest caz a permis încetarea unor practici contrare unui acord privind protecția vieții private și care puteau diminua încrederea consumatorilor în măsurile de protecție adoptate de societățile comerciale de vânzări on-line. Întrucât această cauză privea informații cu caracter personal deturnate de o întreprindere, atunci când acestea erau protejate de principii stabilite de o altă întreprindere, cauza ar putea avea relevanță și în cadrul problemelor legate de protecția vieții private pe care le ridică transferul de date între întreprinderi din țări diferite.

Chiar dacă Comisia Federală pentru Comerț a luat acțiuni coercitive în cazurile GeoCities, Liberty Financial Cos. și ReverseAuction, competența acestui organism este mai limitată în anumite domenii ale protecției vieții private pe internet. După cum am menționat mai sus, informațiile cu caracter personal colectate și utilizate fără consimțământul persoanelor în cauză nu sunt supuse prevederilor legii privind FTC, decât în cazul în care acestea se înscriu în contextul practicilor comerciale neloiale sau frauduloase. În consecință legea privind FTC nu se aplică practicilor unui website care colectează informații cu caracter personal de la consumatori fără a ascunde scopul pentru care sunt strânse aceste informații sau fără a utiliza/divulga aceste date în scopuri susceptibil de a produce prejudicii grave consumatorilor. De asemenea, FTC nu este în măsură să ceară în mod sistematic entităților care strâng informații pe internet să adere la un mecanism de protecție a vieții private sau să subscrie la unul dintre aceste mecanisme [1]. După cum s-a precizat mai sus, o întreprindere care nu își respectă angajamentele privind protecția vieții private este susceptibilă de a comite un act fraudulos.

---

[1] Din acest motiv, Comisia Federală pentru Comerț a declarat, în cadrul unei audieri în fața Congresului, că introducerea de texte legislative suplimentare ar fi fără îndoială necesară pentru a obliga site-urile de internet cu caracter comercial din Statele Unite să adopte practici precise cu privire la informarea obiectivă a consumatorilor (a se vedea „Consumer Privacy on the World Wide Web," mărturie prezentată Subcomitetului pentru telecomunicații, comerț și protecția consumatorului din cadrul Comitetului pentru Comerț al Camerei Reprezentanților din Statele Unite la 21 iulie 1998; acest document poate fi consultat la următoarea adresă: www.ftc.gov/os/9807/privac98.htm). FTC nu a solicitat încă elaborarea unei astfel de legislații pentru ca întreprinderile care optează pentru coduri de autoreglementare să poată demonstra că bunele practici privind informarea pe website-uri sunt larg difuzate. În raportul privind protecția vieții private pe internet prezentat Congresului în iunie 1998 („Privacy Online: A Report to Congress"), (raportul poate fi consultat la următoarea adresă: www.ftc.gov/reports/privacy3/toc.htm), FTC a recomandat adoptarea de texte legislative care să oblige website-urile comerciale să obțină consimțământul părinților înainte de a colecta informații cu caracter personal de la copii sub 13 ani (a se vedea nota de subsol 3 de mai sus). Anul trecut, FTC a constatat, în raportul său intitulat „Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress" (iulie 1999, raportul poate fi consultat la următoarea adresă: www.ftc.gov/os/1999/9907/index.htm#13), că progresele realizate cu privire la autoreglementare sunt satisfăcătoare și, în consecință, a decis să nu recomande elaborarea de texte legislative la acea dată. În mai 2000 Comisia a prezentat un al treilea raport Congresului:
„Privacy Online: Fair Information Practices in the Electronic Marketplace" (www.ftc.gov/os/2000/05/index.htm#22). Acest document analizează ancheta recent efectuată de FTC în ceea ce privește site-urile internet comerciale și respectarea de către acestea a practicilor echitabile în ceea ce privește informarea. Conține, de asemenea, o recomandare (votată de majoritatea membrilor FTC) care invită Congresul să adopte o legislație care să stabilească un nivel de bază de protecție a vieții private pentru site-urile internet comerciale care se adresează consumatorilor.

Pe lângă aceasta, domeniul de competență al FTC nu include actele și practicile frauduloase sau neloiale decât în cazul în care acestea sunt de natură „comercială". Informațiile strânse de către entitățile comerciale care promovează produse sau servicii, inclusiv informații strânse și utilizate în scopuri comerciale, intră probabil în domeniul de competență al FTC. Pe de altă parte, multe persoane particulare și entități strâng informații pe internet fără a urmări un scop comercial și astfel nu intră în domeniul de competență al FTC. Un exemplu îl reprezintă „forumurile de discuții" gestionate de entități necomerciale, în special de organisme de caritate.

În sfârșit, domeniul de competență fundamental al FTC în ceea ce privește practici comerciale este supus unui număr de excluderi legale totale sau parțiale, ceea ce limitează capacitatea FTC de a oferi un răspuns exhaustiv problemelor legate de protecția vieții private pe internet. Aceste excluderi privesc un număr mare de întreprinderi care au recurs la un volum mare de informații cu privire la consumatori, precum băncile, societățile de asigurare și companiile aeriene. După cum bine știți, alte agenții federale sau ale statelor membre ale federației au competență în ceea ce privește aceste entități, în special agențiile federale responsabile cu problemele bancare și Departamentul Transporturilor.

În cauzele în care dispune de competență, FTC înregistrează plângerile primite din partea consumatorilor (prin poștă electronică, telefon și, mai nou, pe website-ul său ([1]) la Consumer Response Center („CRC"). CRC înregistrează toate plângerile din partea consumatorilor, inclusiv de la cei care locuiesc în statele membre ale Uniunii Europene. Legea privind FTC permite Comisiei Federale pentru Comerț să obțină hotărâri reparatorii pentru orice încălcare a legii respective, precum și despăgubiri pentru consumatorii prejudiciați. În caz de plângere, facem eforturi pentru a verifica dacă întreprinderea în cauză s-a angajat, în mod repetat, în practici abuzive, întrucât noi nu ne ocupăm de litigii individuale în domeniul consumului. În trecut, Comisia Federală pentru Comerț a obținut despăgubiri pentru cetățeni ai Statelor Unite ale Americii și ai altor țări ([2]). FTC va continua, după caz, să obțină despăgubiri pentru cetățenii altor țări care au suferit prejudicii în urma unei practici frauduloase care ține de competența sa.

Date privind angajarea

În ultima dumneavoastră scrisoare ați solicitat clarificări suplimentare cu privire la atribuțiile FTC în domeniul datelor privind angajarea. Mai întâi, ați întrebat dacă FTC poate lua măsuri în temeiul articolului 5 împotriva unei întreprinderi care declară că pune în practică principiile „sferei de siguranță", dar care transferă sau utilizează date privind angajarea într-o manieră care contravine acestor principii. Dorim să vă asigurăm că am analizat atent dispozițiile legislative care definesc mandatul FTC, precum și documentele conexe și jurisprudența și am ajuns la concluzia că FTC dispune de aceeași competență pentru datele cu privire la angajare ca și pentru toate celelalte date care intră în domeniul de aplicare al articolului 5 din FTC Act ([3]). Adică putem lua măsuri în cazul datelor privind angajarea în cazul în care o cauză referitoare la protecția vieții private răspunde criteriilor care ne cer luarea de măsuri (practici neloiale și frauduloase).

De asemenea, dorim să eliminăm orice îndoieli cu privire la capacitatea FTC de a lua măsuri legate de protecția vieții private numai în situațiile în care o întreprindere a adus prejudicii consumatorilor particulari. În realitate, după cum arată acțiunile întreprinse de FTC în cazul ReverseAuction ([4]), FTC ia măsuri de punere în aplicare în cauzele privind protecția vieții private atunci când, în cadrul transferurilor de date între întreprinderi, una dintre întreprinderile în cauză comite o infracțiune față de cealaltă societate comercială, conducând la un eventual prejudiciu suferit atât de consumatori cât și de întreprinderi. Credem că aceasta este situația în care este cel mai probabil să se pună problema datelor privind angajarea, întrucât acest tip de date privind cetățenii europeni sunt transferate de către întreprinderi europene către întreprinderi din Statele Unite ale Americii care și-au luat angajamentul de a respecta principiile „sferei de siguranță".

Trebuie totuși să semnalăm că, în anumite circumstanțe, marja de manevră a FTC este limitată, în special atunci când o cauză este deja discutată într-un litigiu tradițional de drept al muncii (cel mai probabil o reclamație sau o solicitare de arbitraj ori o plângere depusă la National Labor Relations Board pentru practici frauduloase în domeniul dreptului muncii). Aceasta ar fi cazul, de exemplu, dacă un angajator și-a luat un angajament privind utilizarea datelor cu caracter

([1]) A se vedea http://www.ftc.gov/ftc/complaint.htm pentru a consulta formularul pentru depunerea plângerilor pe site-ul Comisiei Federale pentru Comerț.

([2]) De exemplu, într-o cauză recentă privind un sistem piramidal pe internet, FTC a obținut rambursări pentru 15 622 de consumatori în valoare totală de aproximativ 5,5 milioane USD. Consumatorii erau rezidenți din Statele Unite și din alte 70 de țări (a se vedea www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm).

([3]) Trebuie notată o excepție (semnalată în mod expres în dispozițiile legislative ce definesc mandatul FTC): competențele pe care legea privind FTC le conferă acestei Comisii în domeniul practicilor „comerciale" coexistă cu atribuțiile constituționale ale Congresului în conformitate cu Clauza privind comerțul [*United States v. American Building Maintenance Industries*, 422 US 271, 277 n. 6 (1975)]. Competența FTC înglobează, așadar, practicile aplicate în materie de angajare de către întreprinderi și ramuri ale comerțului internațional.

([4]) A se vedea „Online Auction Site Settles FTC Privacy Charges", comunicat de presă al FTC (6 ianuarie 2000), disponibil la următoarea adresă: http://www.ftc.gov/opa/2000/01/reverse4.htm.

personal în cadrul unui acord colectiv iar un angajat sau un sindicat susține că acest angajator a încălcat acordul menționat anterior. FTC nu ar interveni, probabil, într-o asemenea procedură (1).

Competența în cazul programelor de tip „seal"

În al doilea rând, doreați să aflați dacă FTC dispune de competență în cazul programelor de tip „seal" care administrează mecanisme de soluționare a litigiilor în Statele Unite ale Americii atunci când aceste sisteme abuzează de rolul lor în aplicarea principiilor „sferei de siguranță" și în tratarea plângerilor individuale, chiar dacă tehnic aceste sisteme sunt organisme cu scop nelucrativ. Pentru a stabili dacă FTC dispune de competență cu privire la o entitate care se declară drept entitate fără scop lucrativ, analizăm îndeaproape dacă această entitate, presupunând că nu urmărește să obțină profit pentru ea însăși, favorizează obținerea de profit de către membrii săi. Comisia a stabilit cu succes că are competență în acest domeniu și, la 24 mai 1999, Curtea Supremă a Statelor Unite ale Americii a confirmat în unanimitate că în competența FTC intră și asociațiile private cu scop nelucrativ reunind grupuri locale de medici stomatologi într-un proces antitrust (*California Dental Association v. Federal Trade Commission*). Curtea a afirmat:

> „Legea privind FTC trebuie să includă nu doar entitățile care urmăresc să obțină profit în nume propriu (15 U.S.C. § 44), ci și entitățile care urmăresc să obțină profit pentru membrii lor. [……] Ar fi într-adevăr greu de crezut că Congresul a dorit adoptarea unei noțiuni atât de limitate de organizații de ajutor, având în vedere că o asemenea restricție ar permite unor organizații să evite competența FTC în cazuri în care legea FTC cere intervenția acesteia."

Pe scurt, pentru a stabili dacă are competență asupra unei anumite entități cu scop nelucrativ care administrează un program de tip „seal", FTC trebuie să verifice în ce măsură o asemenea entitate permite membrilor săi să obțină profituri. În cazul în care entitatea menționată anterior gestionează programul de tip „seal" astfel încât membrii săi să obțină profituri, probabil că FTC își declară competența. De altfel, FTC ar dispune probabil de competență în cazul sistemelor frauduloase care se prezintă ca fiind entități cu scop nelucrativ.

Protecția datelor „off-line" cu caracter personal

În alt treilea rând, ați atras atenția asupra faptului că până acum corespondența noastră s-a axat pe protecția vieții private în cadrul activităților on-line. Chiar dacă acest domeniu este una dintre preocupările majore ale FTC, având în vedere că reprezintă unul dintre elementele principale ale dezvoltării comerțului electronic, legea privind FTC datează încă din 1914 și se aplică, de asemenea, activităților off-line. În consecință, suntem abilitați să urmărim în justiție întreprinderile care se angajează în practici neloiale sau frauduloase cu privire la protecția vieții private (2). De fapt, într-un proces intentat de Comisie anul trecut, *FTC v. TouchTone Information Inc.* (3), un „comerciant de informații" a fost acuzat de obținerea și vânzarea ilegală de date confidențiale privind situația financiară a anumitor consumatori. FTC a susținut că TouchTone a obținut aceste informații sub pretexte false, folosind tehnici de investigație utilizate la origine de anchetatori privați pentru a obține informații cu caracter personal, de obicei la telefon. În această cauză, înregistrată la 21 aprilie 1999 la un tribunal federal din Colorado, procurorul solicită un ordin și rambursarea tuturor profiturilor obținute în mod ilegal.

Suprapunere de competențe

În sfârșit, ne întrebați cu privire la suprapunerea de competențe dintre FTC și celelalte agenții în cauză. Am stabilit o serie de relații strânse cu numeroase alte agenții, inclusiv agenții federale de supraveghere a activităților bancare și

(1) Problema de a ști dacă o practică este contrară dreptului muncii sau unui acord colectiv reprezintă o problemă tehnică rezervată de obicei tribunalelor specializate, în special instanțele de arbitraj și National Labor Relations Board (NLRB).

(2) După cum cunoașteți, Fair Credit Reporting Act conferă FTC atribuția de a proteja confidențialitatea datelor cu caracter personal cu caracter financiar în cadrul domeniului de aplicare al legii, iar FTC adoptă recent o decizie cu privire la această problemă („In the Matter of Trans Union", dosar nr. 9255, 1 martie 2000, comunicat de presă și aviz disponibile la următoarea adresă: www.ftc.gov/os/2000/03/index.htm#1).

(3) „Acțiunea civilă 99-WM-783 (D.Colo.)" disponibilă la următoarea adresă: http://www.ftc.gov/opa/1999/9904/touchtone.htm (în așteptarea unei hotărâri cu privire la un acord provizoriu).

procurorii generali ai statelor membre ale federației. În cazul în care competențele noastre se suprapun, deseori ne coordonăm anchetele în vederea utilizării optime a resurselor. De asemenea, prezentăm adesea probleme spre investigare agențiilor federale sau naționale.

Sper că această trecere în revistă vă va fi de ajutor și rămân la dispoziția dumneavoastră pentru orice informații suplimentare.

Al dumneavoastră,

Robert Pitofsky

ANEXA VI

John Mogg
Director, DG XV
Comisia Europeană
Birou C 107-6/72
Rue de la Loi/Wetstraat 200
B – 1049 Bruxelles

Stimate domnule Director General Mogg,

Vă trimit prezenta scrisoare ca urmare a cererii Departamentului Comerţului al Statelor Unite ale Americii de a explica rolul Departamentului Transporturilor în protecţia vieţii private a consumatorilor cu privire la informaţiile pe care aceştia le furnizează companiilor aeriene.

Departamentul Transporturilor încurajează autoreglementarea ca fiind modul cel mai puţin constrângător şi cel mai eficient de a asigura protecţia confidenţialităţii informaţiilor pe care consumatorii le furnizează companiilor aeriene. În consecinţă, Departamentul Transporturilor sprijină instituirea unei „sfere de siguranţă" care să permită companiilor aeriene să se conformeze dispoziţiilor din directiva Uniunii Europene cu privire la protecţia datelor cu caracter personal transferate în afara Uniunii Europene. Departamentul recunoaşte, cu toate acestea, că aceste măsuri nu pot fi eficiente decât în cazul în care companiile aeriene îşi respectă angajamentul de a respecta principiile privind protecţia vieţii private prevăzute de „sfera de siguranţă". În acest sens, autoreglementarea ar trebui să fie însoţită de aplicarea legilor. Prin urmare, Departamentul face apel la autoritatea sa de supraveghere a protecţiei consumatorilor şi va garanta respectarea de către companiile aeriene a angajamentului luat faţă de public cu privire la protecţia vieţii private. Va da curs plângerilor cu privire la nerespectarea prezumată a angajamentelor pe care le primim din partea organizaţiilor de autoreglementare şi altele, inclusiv din statele membre ale Uniunii Europene.

Departamentul este abilitat să ia măsuri de punere în aplicare în acest domeniu în temeiul titlului 49 articolul 41712 din U.S.C., care interzice unui transportator „orice practică neloială sau frauduloasă sau orice act de concurenţă neloială" pentru vânzarea serviciilor de transport aerian, care aduce sau este susceptibilă de a aduce prejudicii consumatorului. Articolul 41712 este formulată după modelul articolului 5 din Federal Trade Commission Act (15 U.S.C. 45). Cu toate acestea, transportatorii aerieni sunt scutiţi de dispoziţiile articolului 5 de către Comisia Federală pentru Comerţ în temeiul titlului 15 articolul 45 (a) (2) din U.S.C.

Biroul meu analizează cazuri şi intentează acţiuni în justiţie în anumite cazuri în temeiul titlului 49 articolul 41712 din U.S.C. (a se vedea, de exemplu, următoarele ordonanţe ale Departamentului Transporturilor: 99-11-5, 9 noiembrie 1999; 99-8-23, 26 august 1999; 99-6-1, 1 iunie 1999; 98-6-24, 22 iunie 1998; 98-6-21, 19 iunie 1998; 98-5-31, 22 mai 1998 şi 97-12-23, 18 decembrie 1997). Instrumentăm astfel de cauze pe baza propriilor noastre investigaţii, precum şi pe baza plângerilor oficiale sau neoficiale primite din partea persoanelor particulare, a agenţiilor de turism, a companiilor aeriene şi a organismelor guvernamentale din Statele Unite ale Americii sau din străinătate.

Aş dori să vă atrag atenţia asupra faptului că nerespectarea de către un transportator a caracterului privat al informaţiilor comunicate de pasageri nu ar constitui o încălcare *a priori* a articolului 41712. Cu toate acestea, odată ce un transportator şi-a luat în mod formal şi public angajamentul de a respecta principiile „sferei de siguranţă" care garantează respectarea caracterului privat al informaţiilor pe care i le-a furnizat consumatorul, Departamentul poate să recurgă la atribuţiile care îi sunt conferite de articolul 41712 pentru a asigura respectarea acestor principii. În consecinţă, atunci când un pasager furnizează informaţii unui transportator care şi-a luat angajamentul să respecte principiile „sferei de siguranţă", orice nerespectare a acestui angajament ar fi susceptibilă să aducă prejudiciu consumatorului şi ar constitui o încălcare a articolului 41712. Biroul meu acordă prioritate examinării acestor cazuri şi trimiterii în instanţă în caz de încălcare. De asemenea, informăm Departamentul Comerţului cu privire la rezultatul acestor acţiuni.

Nerespectarea dispoziţiilor articolului 41712 pot avea ca rezultat emiterea de ordonanţe de întrerupere şi încetare a activităţii şi de sancţiuni de drept civil pentru încălcarea acestor ordonanţe. Deşi nu avem competenţa să acordăm daune-interese sau o despăgubire pecuniară reclamantului, suntem în schimb abilitaţi să sancţionăm regulamentele care rezultă în urma anchetelor şi cazurile examinate de Departament care prevăd acordarea de plăţi în natură consumatorilor cu titlu de despăgubire sau pentru a compensa penalizările plătibile în alte moduri. Am procedat astfel în trecut şi continuăm şi vom continua să procedăm la fel în cadrul „sferei de siguranţă" atunci când circumstanţele o justifică. Încălcările repetate ale articolului 41712 de către o companie aeriană din Statele Unite ale Americii ar pune, de asemenea, la îndoială bunăvoinţa companiei aeriene de a îşi respecta angajamentul. În situaţii extreme, s-ar putea considera că acea companie nu mai este aptă de exploatare şi, în consecinţă, riscă să-şi piardă licenţa de exploatare.

[A se vedea ordonanțele Departamentului Transportului 93-6-34, 23 iunie 1993 și 93-6-11, 9 iunie 1993. Deși această cauză nu a avut legătură cu articolul 41712, ea a avut ca rezultat revocarea licenței de exploatare a unui transportator pentru încălcarea totală a dispozițiilor legii federale privind transporturile aeriene (Federal Aviation Act), ale unui acord bilateral și a regulamentului interior al Departamentului.]

Sper că aceste informații vă vor fi utile. Vă stau la dispoziție pentru orice informații suplimentare.

Al dumneavoastră,

Samuel Podberesky

Consilier general adjunct „Aviation Enforcement and Proceeding”

ANEXA VII

Având în vedere articolul 1 alineatul (2) litera (b), organele administrative din Statele Unite ale Americii abilitate să instrumenteze plângerile și să obțină măsuri împotriva practicilor neloiale sau frauduloase, precum și despăgubiri pentru prejudiciul suferit de persoanele în cauză, indiferent de țara de rezidență sau de cetățenie, în caz de încălcare a principiilor puse în aplicare în conformitate cu FAQ, sunt următoarele:

1. Comisia Federală pentru Comerț;

2. Departamentul Transporturilor.

Competența Comisiei Federale pentru Comerț se întemeiază pe articolul 5 din Federal Trade Commission Act. În temeiul articolului 5, Comisia Federală pentru Comerț nu dispune de competență cu privire la bănci, societăți de economii și împrumuturi și cooperative de credit, societăți de telecomunicații și societăți de transport public interstatal, transportatori aerieni, ambalatori și operatori din sectorul zootehnic. Chiar dacă societățile de asigurări nu sunt incluse în mod expres pe lista excepțiilor de la articolul 5, legea McCarran-Ferguson ([1]) lasă reglementarea acestei ramuri de activitate fiecărui stat membru al federației în parte. Cu toate acestea, dispozițiile din Federal Trade Commission Act se aplică sectorului asigurărilor în măsura în care această activitate nu este reglementată de legea statului membru al federației respectiv. Comisia Federală pentru Comerț are competență reziduală privind practicile neloiale sau frauduloase comise de societățile de asigurări în cadrul activităților altele decât cele din sectorul asigurărilor.

Departamentul Transporturilor al Statelor Unite ale Americii acționează pe baza atribuțiilor care îi sunt conferite în temeiul titlului 49 din United States Code, articolul 41712. Departamentul Transporturilor al Statelor Unite ale Americii instrumentează cazurile bazate pe propriile sale anchete, precum și pe baza plângerilor oficiale sau neoficiale primite din partea persoanelor particulare, a agențiilor de turism, companiilor aeriene și agențiilor guvernamentale din Statele Unite ale Americii și din străinătate.

([1]) 15 U.S.C. § 1011 și urm.