GRUPUL DE LUCRU PRIVIND PROTECȚIA DATELOR, CONSTITUIT ÎN TEMEIUL ARTICOLULUI 29

00350/09/RO
WP 159

Avizul 1/2009 referitor la propunerile de modificare a Directivei 2002/58/CE privind confidențialitatea și comunicațiile electronice (Directiva privind confidențialitatea în mediul electronic)

Adoptat la 10 februarie 2009

Acest grup de lucru a fost înființat în conformitate cu articolul 29 din Directiva 95/46/CE. Este un organism european consultativ independent în materie de protecția datelor şi confidențialitate. Atribuțiile acestui grup sunt descrise în articolul 30 din Directiva 95/46/CE şi în articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcția C (Justiție civilă, drepturi şi cetățenie) a Comisiei Europene, Direcția Generală Justiție, Libertate şi Securitate, B-1049 Bruxelles, Belgia, Biroul nr. LX-46 01/06.

Site web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

CUPRINS

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR FIZICE ÎN PRIVINȚA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995[1],

având în vedere articolul 29, articolul 30 alineatul (1) litera (a) și articolul 30 alineatul (3) din această directivă, precum și articolul 15 alineatul (3) din Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002,

având în vedere articolul 255 din Tratatul de instituire a Comunității Europene, precum și Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei,

având în vedere regulamentul de procedură al Grupului,

ADOPTĂ PREZENTUL DOCUMENT:

1. CONTEXT

La 13 noiembrie 2007, Comisia a adoptat o propunere de directivă („propunerea") de modificare a Directivei 2002/58/CE (Directiva privind confidențialitatea în mediul electronic) privind prelucrarea datelor cu caracter personal și protejarea confidențialității în sectorul comunicațiilor publice și a Directivei 2002/21/CE (directiva-cadru).

În cadrul primei lecturi, la 24 septembrie 2008, Parlamentul European a adoptat amendamente la propunere („amendamentele Parlamentului"), la care au fost făcute observații, la 6 noiembrie 2008, de către Comisia Europeană, în COM(2008)723 final („observațiile Comisiei").

Ulterior, la 27 noiembrie 2008, Consiliul Uniunii Europene a ajuns la un acord politic („acordul Consiliului").

Grupul de lucru constituit în temeiul articolului 29 dorește să prezinte unele observații cu privire la amendamentele Parlamentului, la observațiile Comisiei și la acordul Consiliului.

Grupul de lucru amintește că a adoptat deja două avize privind propunerile de modificare a cadrului de reglementare al Uniunii Europene pentru rețelele și serviciile de comunicații electronice (Avizul 8/2006 adoptat la 26 septembrie 2006[2] și Avizul 2/2008 adoptat la 15 mai 2008[3]).

Grupul de lucru, apreciind faptul că unele din recomandările sale anterioare au fost luate în considerare, dorește să sublinieze unele preocupări majore legate de problemele ridicate după prima lectură la Parlament și la Consiliu; grupul de lucru nu repetă toate punctele de vedere afirmate în avizele anterioare, care rămân valabile.

---

1 JO L281, 23.11.1995, p. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

3 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_ro.pdf

2. NOTIFICAREA PRIVIND VIOLAREA DATELOR CU CARACTER PERSONAL

2.1. Observații

Grupul de lucru sprijină pe deplin propunerea de consolidare a articolului 4 din Directiva privind confidențialitatea în mediul electronic, solicitând furnizorilor de servicii de comunicații accesibile publicului să notifice cazurile de încălcare a securității. Notificarea cazurilor de încălcare poate deveni un instrument important la îndemâna autorităților pentru protecția datelor de a spori atenția și eficiența atunci când pun în aplicare obligația furnizorilor de servicii de a lua măsurile de securitate corespunzătoare.

În general, grupul de lucru recomandă următoarea abordare a chestiunii privind notificărilor referitoare la violarea datelor cu caracter personal:

- autoritatea națională de reglementare competentă este informată ori de câte ori există riscul producerii unor efecte negative[4] asupra vieții private a persoanelor și datelor cu caracter personal;

- este esențial ca utilizatorii afectați să fie informați imediat de către furnizorii de servicii în cazul în care încălcarea securității ar putea avea efecte negative[5] asupra vieții private a persoanelor și a datelor cu caracter personal, fără a fi exclusă posibilitatea ca autoritatea națională de reglementare competentă să dezvăluie în mod public informațiile cu privire la cazul de încălcare și să oblige furnizorul de servicii să facă același lucru;

- fiecare furnizor de servicii trebuie să păstreze o evidență[6] a tuturor cazurilor de violare a datelor cu caracter personal.

De asemenea, grupul de lucru constată că cele trei propuneri (a Parlamentului, a Comisiei și a Consiliului) adoptă abordări substanțial diferite ale chestiunii referitoare la încălcarea securității și violarea datelor cu caracter personal, în special în ceea ce privește:

- domeniul de aplicare a obligației (care, în amendamentele Parlamentului, este extins la serviciile societății informaționale, iar în cazul Comisiei și Consiliului este limitat la serviciile de comunicații electronice accesibile publicului); grupul de lucru sprijină ferm extinderea domeniului de aplicare a obligației la serviciile societății informaționale;

- entitatea care trebuie să ia decizia de a notific persoanele (conform Parlamentului și Comisiei, aceasta este autoritatea competentă, iar conform Consiliului, entitatea respectivă este furnizorul de servicii);

---

[4] Riscul producerii unor efecte negative trebuie să fie evaluat luându-se în considerare elemente precum cantitatea de date afectate de încălcare, natura acestora, impactul încălcării asupra unei persoane, de exemplu furtul de identitate, pierderile financiare, pierderea oportunităților de afaceri sau de angajare sau o combinație a acestora sau alte situații similare. Criteriile calitative și cantitative de evaluare a impactului efectelor negative trebuie să fie definite cu exactitate în timpul procedurii de comitologie, avându-se în vedere faptul că este important ca autoritățile să nu fie asaltate cu cazuri minore și ca persoana să nu fie alarmată în mod inutil.

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

[6] Formatul acestor evidențe ar trebui standardizat pentru a se asigura că înregistrările pot fi auditate de către autoritatea națională de reglementare competentă.

- tipurile de încălcări care trebuie notificate (în propunerea Parlamentului şi în observaţiile Comisiei, toate tipurile de încălcare, iar în acordul Consiliului, numai cazurile grave de încălcare);

- precum şi persoanele care pot fi notificate (pentru Parlament şi Comisie, abonaţi sau persoane fizice, iar pentru Consiliu, numai abonaţi).

Domeniul de aplicare al notificării: serviciile societăţii informaţionale

Grupul de lucru susţine cu fermitate amendamentele 187/rev şi 184 din amendamentele Parlamentului. **O extindere a notificărilor cu privire la violarea datelor cu caracter personal pentru a cuprinde serviciile societăţii informaţionale este necesară, având în vedere rolul din ce în ce mai mare al acestor servicii în viaţa de zi cu zi a cetăţenilor europeni** şi cantitatea din ce în ce mai mare de date cu caracter personal prelucrate de aceste servicii. Tranzacţiile online, care includ accesul la serviciile bancare electronice (e-banking), fişele medicale din sectorul privat şi cumpărăturile online sunt doar câteva exemple de servicii care pot face obiectul violării datelor cu caracter personal, care constituie riscuri majore pentru un număr mare de cetăţeni ai Uniunii Europene. Limitarea domeniului de aplicare al acestor obligaţii la serviciile de comunicaţii electronice accesibile publicului ar afecta doar un număr foarte limitat de părţi interesate, reducând astfel în mod semnificativ impactul notificărilor cu privire la violarea datelor cu caracter personal, fiind astfel un mijloc de protejare a persoanelor împotriva riscurilor precum furtul de identitate, pierderile financiare, pierderea oportunităţilor de afaceri sau de angajare şi prejudiciul fizic.

Prin urmare, Grupul de lucru regretă profund că această propunere nu a fost susţinută de către Comisie şi de către Consiliu şi aminteşte că unele dispoziţii ale directivei privind confidenţialitatea în mediul electronic sunt aplicate deja pe un plan mai larg decât domeniul strict de aplicare al serviciilor de comunicaţii electronice[7].

Responsabilitate şi criterii de notificare

Furnizorii de servicii în cauză trebuie să fie responsabili pentru evaluarea riscurilor create prin violarea datelor cu caracter personal; aceştia sunt cei mai în măsură să decidă fără întârziere dacă persoanele afectate ar trebui notificate, în baza normelor de evaluare stabilite de către autorităţi. **Fără a aduce atingere obligaţiei lor de a notifica autorităţile naţionale de reglementare competente cu privire la toate cazurile de încălcare ori de câte ori există riscul unor efecte negative, furnizorii de servicii ar trebui să stabilească dacă este necesară notificarea abonaţilor sau a persoanelor fizice. Pentru a asigura comunicarea unor informaţii exacte şi relevante publicului, autorităţile naţionale de reglementare competente pot decide să dezvăluie în mod public cazurile de încălcare, ori de câte ori acest lucru este considerat necesar şi pot obliga furnizorul de servicii să facă acelaşi lucru.**

---

[7] Anumite dispoziţii ale directivei privind confidenţialitatea în mediul electronic, cum ar fi articolul 5 alineatul (3) (fişiere cookies şi spyware) şi articolul 13 (comunicaţii nesolicitate) reprezintă deja dispoziţii generale care sunt aplicabile nu numai serviciilor de comunicaţii electronice.
Această posibilă extindere în afara domeniului strict de aplicare al serviciilor de comunicaţii electronice accesibile publicului este avută în vedere şi în alte situaţii, deoarece Comisia a propus extinderea domeniului de aplicare al articolului 5 alineatul (3) pentru a acoperi cazurile în care sunt furnizate fişiere cookies şi spyware pe suporturi tip CD-ROM sau USB, care nu constituie servicii de comunicaţii electronice accesibile publicului.

Având în vedere că notificarea se efectuează de către furnizorul de servicii, **este esențial ca directiva să ofere protecție pentru a garanta că aceste cazuri de încălcare nu sunt ascunse**, că evaluarea încălcării a fost corect efectuată și că persoanele au fost notificate ori de câte ori a fost necesar.

Autoritățile vor fi notificate cu privire la un număr mai mare de cazuri, astfel încât acestea să fie în măsură să exercite controlul privind procesul de notificare a persoanelor de către furnizorul de servicii. Formatul notificării ar trebui să fie armonizat la nivelul Uniunii Europene și ar trebui să includă criterii obiective și clare, utilizate la evaluarea impactului efectelor negative produse de cazurile de încălcare. În plus, autoritatea națională de reglementare competentă trebuie să verifice dacă evaluarea încălcării a fost corect efectuată de către furnizorul de servicii și dacă au fost luate măsurile corespunzătoare în urma încălcării datelor cu caracter personal. În cele din urmă, **pentru a se preveni ascunderea cazurilor de încălcare, este esențial ca directiva să atribuie autorității naționale competente de reglementare competența de a impune sancțiuni financiare punitive (penalități)[8] în cazul în care furnizorul de servicii nu raportează sau raportează incorect, persoanelor și/sau autoritățile naționale de reglementare, cazurile de violare a datelor cu caracter personal. .**

<u>Tipurile de încălcare care trebuie raportate persoanelor fizice: noțiunea de efecte negative</u>

Grupul de lucru salută introducerea unei noi definiții a „încălcării datelor cu caracter personal" în articolul 2[9], propusă în Observațiile Comisiei[10] .

Cu toate acestea, Grupul de lucru observă că cele trei propuneri folosesc formulări diferite pentru a descrie situațiile în care ar trebui raportate persoanelor vizate, cazurile de încălcare privind datele cu caracter personal. Prin urmare, **Grupul de lucru recomandă ca încălcarea securității ar trebui raportată persoanelor vizate atunci când cazul de încălcare poate produce efecte negative asupra vieții private a persoanelor și a protecției datelor cu caracter personal.** În acest sens, acordul Consiliului oferă exemple utile în considerentul 29.

<u>Persoanele care pot fi notificate</u>

Grupul de lucru salută trimiterile la „abonați sau persoane fizice", la „utilizatori prejudiciați" și la „autoritatea națională competentă" incluse în considerentul 29 din amendamentele Parlamentului[11]. Acordul Consiliului limitează notificările la „abonați" și, prin urmare, unele violări ale datelor cu caracter personal, descrise în Avizul 2/2008, nu vor fi raportate persoanelor afectate.

2.2. Exceptarea de la notificare

Grupul de lucru confirmă faptul că notificările cu privire la violarea datelor cu caracter personal ar trebui să cuprindă informații cu privire la împrejurările în care s-a produs cazul de încălcare, inclusiv dacă datele cu caracter personal au fost protejate prin criptare; aceste informații sunt esențiale pentru autoritatea națională de reglementare competentă, în cazul

---

8 Grupul de lucru reține că aceste dispoziții au fost propuse de către Parlament, Comisie și Consiliu într-un nou articol 15a alineatul (1).

9 A se vedea observațiile Comisiei privind amendamentele 187/rev și 184 din amendamentele Parlamentului

10 Totuși, această noțiune de „violare a datelor cu caracter personal" este generală și nu ar trebui să fie limitată la datele prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului; noțiunea ar trebui să acopere, de asemenea, cel puțin serviciile societății informaționale.

11 A se vedea amendamentul 183

unei încălcări, pentru ca aceasta să poată stabili măsurile adecvate care trebuie luate, dacă este cazul, în ceea ce privește furnizorul de servicii.

Totuși, **Grupul de lucru are obiecțiuni cu privire la introducerea unor excepțări de la notificare[12], atunci când furnizorii de servicii pun în aplicare „măsuri tehnice de protecție corespunzătoare, iar aceste măsuri vizează datele afectate de încălcarea securității". Această dispoziție ar reduce în mod semnificativ calitatea și utilitatea informațiilor furnizate persoanelor afectate.** Numai utilizatorii afectați pot fi în măsură să ia măsurile adecvate pentru limitarea riscurilor cu care se confruntă, dacă sunt corect informați. Prin urmare, **Grupul de lucru subliniază importanța formatului notificării și a evaluării riscului pentru a stabili dacă persoanele ar trebui informate sau nu, indiferent de măsurile tehnice luate efectiv pentru protejarea datelor acestora.**

3. DATE DE TRANSFER

3.1. Prelucrarea datelor de transfer în scopul protejării securității

Într-un nou articol 6 alineatul (6) litera (a), Parlamentul, Consiliul și Comisia propun introducerea unei noi excepții în directiva privind confidențialitatea în mediul electronic, prin care este permisă prelucrarea datelor de transfer în scopul protejării securității.

Grupul de lucru cunoaște faptul că „furnizorii de servicii de securitate" aplică soluții de securitate[13] (cum ar fi program anti-virus și anti-spam, firewall sau sisteme de detectare a intruziunii) care pot necesita prelucrarea datelor de transfer în scopul securizării datelor personale ale utilizatorilor și al protejării serviciului propriu-zis. Totuși, Grupul de lucru este preocupat de faptul că textul actual ar putea acorda legitimitate desfășurării la scară largă a verificării în profunzime a pachetului de servicii[14], atât în rețea, cât și în echipamentul utilizatorului, cum ar fi dispozitivele ADSL, în timp ce cadrul legal existent descrie deja cazurile în care datele de transfer pot fi prelucrate în scopul protejării securității.

Într-adevăr, temeiul juridic care permite prelucrarea datelor de transfer de către serviciile de comunicații electronice accesibile publicului și prelucrarea datelor personale de către operatorii de date este stabilit prin dispozițiile articolului 6 din directiva privind confidențialitatea în mediul electronic, precum și de articolele 7 și 17 din directiva privind protecția datelor. Articolul 7 litera (f) din directiva privind protecția datelor arată în ce măsură datele personale pot fi prelucrate în interesul legitim al operatorului ; la prelucrarea datelor trebuie să se țină seama de interesul persoanelor vizate în ceea ce privește drepturile și libertățile fundamentate. De asemenea, articolul 17 din directiva privind protecția datelor stabilește obligația caoperatorii de date să pună în aplicare *„măsuri de protecție tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii accidentale, modificării, dezvăluirii sau accesului neautorizat ... precum și împotriva oricărei alte forme de prelucrare ilegală"*. Măsurile adoptate trebuie, de asemenea, să fie proporționale cu riscurile reprezentate de prelucrare și de natura datelor care trebuie protejate.

---

[12] A se vedea considerentul 29 din amendamentele Parlamentului (amendamentul 122) și considerentele 29 și 32 din acordul Consiliului.

[13] Fie în echipamentul terminal al utilizatorului, fie în rețea.

[14] Verificarea în profunzime a pachetului de servicii permite reperarea și urmărirea în mod foarte invaziv a comportamentului utilizatorului.

Grupul de lucru subliniază, de asemenea, că domeniul de aplicare al amendamentului 180 din amendamentele Parlamentului este clarificat în observațiile Comisiei. **Grupul de lucru ia notă de faptul că textul propus de către Comisie stabilește fără echivoc faptul că prelucrarea datelor de transfer intră sub incidența domeniului de aplicare al directivei privind protecția datelor.** Prin urmare, furnizorii de servicii de securitate trebuie să notifice autoritățile naționale pentru protecția datelor ori de câte ori este necesar și să asigure că persoanele își pot exercita drepturile.

În cele din urmă, Grupul de lucru amintește că prelucrarea datelor de transfer în scopul protejării securității se efectuează deja în statele membre în care au fost adoptate măsuri specifice în conformitate cu articolul 15 alineatul (1) din directiva privind confidențialitatea în mediul electronic care permite statelor membre să adopte măsuri legislative de renunțare la principiul anonimatului sau la ștergerea datelor de transfer[15], atunci când acestea nu mai sunt necesare în scopul transmiterii comunicării, pentru a se preveni utilizarea neautorizată a sistemului de comunicații electronice.

Din motivele invocate mai sus, **propunerea referitoare la introducerea unui nou articol 6, respectiv (6a), nu este necesară.**

4. ADRESE IP

Parlamentul și Comisia propun introducerea unui nou considerent (27a) cu privire la adresele IP [16].

Grupul de lucru salută textul propus în observațiile Comisiei care face referire în mod specific la activitatea sa. Totuși, Grupul de lucru nu sprijină propunerea de a se face o referire explicită la acest aspect într-o directivă.

În acest sens, **Grupul de lucru reconfirmă avizul anterior[17] conform căruia, în cazul în care furnizorul de servicii** „*nu este în măsură să decidă cu certitudine absolută dacă datele corespund unor utilizatori care nu pot fi identificați, acesta trebuie să trateze toate informațiile ca fiind date cu caracter personal, pentru a fi în siguranță"*.

În majoritatea cazurilor, adresele IP se referă la persoane care pot fi identificate. Posibilitatea identificării înseamnă posibilitatea ca persoanele să poată fi identificate prin furnizorul de acces sau prin alte mijloace, cu ajutorul unor elemente suplimentare de identificare, cum ar fi „fișierele cookies", ori în interacțiunile cu serviciile de internet cu care persoana vizată este identificată în mod explicit sau implicit.

Considerentul 26 din directiva privind protecția datelor specifică în mod clar că pentru a se stabili dacă o persoană este identificabilă, *„este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată"*.

Definiția datelor cu caracter personal din directiva privind protecția datelor se referă la date „legate de" o persoană, iar adresele IP sunt utilizate în mod frecvent pentru a se face deosebirea între utilizatorii cărora trebuie să li se aplice un tratament diferit, de exemplu în scopul publicității pentru un public țintă sau pentru crearea de profiluri.

---

15 Stabilite la articolul 6 alineatul (1).

16 Amendamentul 185 al Parlamentului.

17 Avizul 4/2007 privind conceptul de date cu caracter personal și Avizul privind aspectele de protecție a datelor în ceea ce privește motoarele de căutare.

Cu toate că este pregătit să asiste Comisia în activitatea privind adresele IP sugerată de Parlament[18], Grupul de lucru este de acord cu Comisia în privința faptului că o directivă întemeiată pe fond nu reprezintă cea mai adecvată modalitate de abordare a acestei probleme și că obligația de raportare în ceea ce privește „scopurile care nu au fost prevăzute de această directivă" nu este potrivită.

5. INFORMAREA AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR

În cadrul primei lecturi, Parlamentul a adoptat amendamentul 136 la articolul 15 din Directiva privind confidențialitatea în mediul electronic, care ulterior a fost modificat în observațiile Comisiei. Această propunere ar crea obligația ca toți furnizorii de servicii și rețele de telecomunicații și toți furnizorii de servicii în domeniul societății informaționale să raporteze autorității competente pentru protecția datelor orice solicitare „primită în conformitate cu alineatul (1)"[19], precum și obligația autorității respective de a examina fiecare solicitare și de a informa, la rândul său, autoritățile judiciare competente în cazul în care consideră că sunt încălcate dispozițiile relevante ale legislației naționale."

Propunerea privind introducerea raportării este utilă, întrucât sporește transparența și controlul exercitat de autoritățile de reglementare. Însă, deși această dispoziție ar consolida puternic capacitățile de supraveghere și punere în aplicare ale autorităților pentru protecția datelor, contribuind astfel la mai buna aplicare a accesului legal la informații, ar crea, de asemenea, o povară administrativă, atât pentru societățile implicate, cât și pentru autoritățile pentru protecția datelor. În acest sens, Grupul de lucru este preocupat de necesitatea monitorizării solicitărilor tot mai numeroase provenind de la autoritățile judiciare[20] și de noua responsabilitate creată pentru autoritățile pentru protecția datelor, de a controla fiecare anchetă judiciară în parte, ceea ce necesită o creștere considerabilă a resurselor financiare și de personal ale autorităților respective.

Prin urmare, **Grupul de lucru consideră ca această raportare ar putea avea loc numai odată pe an. Raportarea ar putea include detalii cu privire la procedurile interne folosite pentru a răspunde solicitărilor de acces la datele personale ale utilizatorilor, la numărul de solicitări primite, la argumentele juridice invocate și la problemele întâmpinate, dacă este cazul.** De asemenea, este esențial ca această obligație de raportare să fie armonizată și detaliată la nivelul Uniunii Europene.

6. COMUNICAȚII NESOLICITATE

Amendamentul 131 al Parlamentului clarifică faptul că MMS și tehnologiile similare sunt acoperite de noțiunea de „poștă electronică" menționată în articolul 2 alineatul (h).

În primul rând, Grupul de lucru observă că, în directiva privind confidențialitatea în mediul electronic, considerentul 40 clarifică deja faptul că mesajele SMS sunt incluse în noțiunea de mesaj electronic (e-mail)[21].

În al doilea rând, este necesară adaptarea articolului 13 alineatul (1) în ceea ce privește tehnologiile emergente, cu respectarea principiului stabilit în considerentul 4[22]. Textul actual

---

[18] În amendamentele 139 și 186/rev.

[19] Care descrie obligațiile de reținere a datelor impuse în mod oficial prin directiva privind păstrarea datelor (2006/24/CE).

[20] Mulți operatori de telecomunicații primesc mai multe sute de cereri pe zi.

[21] Definită la articolul 2 litera (h) din directiva privind confidențialitatea în mediul electronic.

[22] Conform căruia directiva privind confidențialitatea în mediul electronic trebuie „adaptată la dezvoltarea pieței și tehnologiilor în domeniul serviciilor de comunicații electronice, astfel încât să asigure un nivel

al articolului 13 alineatul (1) pornește de la premisa că persoana este deja conectată la rețeaua prin care este transmisă comunicația (de exemplu, un apel sau un mesaj electronic). Acest text nu face referire la cazurile în care o solicitare ar îndemna un utilizator să se conecteze la o rețea care servește exclusiv reclamelor de publicitate. Acesta ar putea fi în mod tipic cazul în aplicațiile de marketing Bluetooth.

Prin urmare, Grupul de lucru salută clarificările din observațiile Comisiei asupra domeniului de aplicare al articolului 13, care privește în principal utilizarea cuvântului „comunicație" și noul considerent referitor la „tehnologii similare". Acest lucru asigură necesitatea consimțământului prealabil în aplicațiile de marketing Bluetooth, ținând astfel seama de observațiile Grupului de lucru prezentate în Avizul 2/2008 cu privire la „necesitatea protejării utilizatorilor mijloacelor de comunicație fără cablu pe distanțe scurte (short-range wireless media) împotriva comunicațiilor nesolicitate, în conformitate cu articolul 13". O referire explicită la Bluetooth ar putea fi, de asemenea, inclusă în considerentul 40.

În al treilea rând, Grupul de lucru amintește observația sa din Avizul 2/2008 cu privire la utilizarea termenului „abonat" în articolul 13 și ia notă cu satisfacție de formularea propusă în acordul Consiliului.

În cele din urmă, propunerea Consiliului de modificare a articolului 13 alineatul (2) prin adăugarea frazei „în momentul colectării datelor de contact" este, de asemenea, foarte utilă, întrucât oferă informații fără echivoc cu privire la momentul în care utilizatorii pot obiecta cu privire la utilizarea datelor lor de contact electronic în scopuri de marketing direct.

7. SETĂRILE BROWSERELOR

Grupul de lucru se opune cu fermitate amendamentului 128 adoptat de Parlament, susținând că setările implicite („default") ale browserelor ar constitui un mijloc de a obține consimțământul prealabil. Cu toate că acest amendament a fost inclus în observațiile Comisiei și în acordul Consiliului, Grupul de lucru dorește să prezinte anumite observații în legătură cu acest amendament.

Pe lângă problema formală de creare a unui limbaj specific acestei tehnologii în cadrul directivei, Grupul de lucru este preocupat de erodarea noțiunii de consimțământ, rezultatul fiind lipsa de transparență.

Majoritatea browserelor utilizează setări implicite **(„default")** , care nu permit utilizatorilor să fie informați cu privire la orice tentativă de stocare sau acces la echipamentele lor terminale. Prin urmare, setările implicite **(„default")** ale browserelor ar trebui să „respecte" confidențialitatea, dar nu pot constitui un mijloc de a se obține în mod gratuit, specific și informat consimțământul utilizatorilor, astfel cum se prevede la articolul 2 litera (h) din directiva privind protecția datelor.

În ceea ce privește fișierele cookies, Grupul de lucru consideră că un operator de fișiere cookies ar trebui să își informeze utilizatorii prin declarația sa de confidențialitate, și nu se poate baza pe setările implicite(„default") ale browserelor. De asemenea, formularea aleasă nu se limitează la problema actuală pe care o reprezintă fișierele cookies, ci implică orice alte noi tehnologii care ar putea fi folosite pentru urmărirea comportamentului utilizatorilor care folosesc browserul.

---

egal de protecție a datelor personale și confidențialității utilizatorilor de servicii de comunicații electronice publice, indiferent de tehnologiile folosite".

8. ACȚIUNI ÎN JUSTIȚIE ALE PERSOANELOR FIZICE ȘI JURIDICE

Grupul de lucru sprijină propunerea Parlamentului[23] de a introduce în articolul 13 alineatul (6) posibilitatea „oricărei persoane fizice sau juridice de a intenta acțiuni în instanță în cazul în care persoana în cauză a fost prejudiciată în urma încălcării prevederilor legale naționale adoptate în conformitate cu directiva privind confidențialitatea în mediul electronic”.

În mod cert, această dispoziție va consolida drepturile utilizatorului și va contribui la dezvoltarea unor practici de securitate mai bune în rândul actorilor din acest sector de activitate.

9. ALTE ASPECTE

În cele din urmă, Grupul de lucru ia notă cu satisfacție de următoarele:

- legislatorul intenționează să pedepsească practicile de *phishing*[24];
- Comisia și Consiliul[25] au ținut seama de solicitarea Grupului de lucru de a fi consultat în timpul procedurii de comitologie prevăzută la articolul 4 alineatul (4); a fost luată în considerare de către Comisie și de către Consiliu;
- Grupul de lucru a fost inclus în procesul de consultare menționat la articolul 15a alineatul (4);
- Grupul de lucru va fi consultat la pregătirea raportului cu privire la aplicarea directivei revizuite privind confidențialitatea în mediul electronic[26];
- Comisia, Consiliul și Parlamentul doresc să clarifice dacă directiva privind confidențialitatea în mediul electronic se aplică în cazul tehnologiilor emergente, cum ar fi RFID[27] sau NFC, care se bazează pe dispozitive de identificare fără contact, care utilizează fecvențe radio.

10. CONCLUZIE

Grupul de lucru constituit în temeiul articolului 29 invită legislatorii europeni să ia în considerare, în primul rând, printre celelalte aspecte subliniate în prezentul aviz, extinderea domeniului de aplicare al obligației de notificare cu privire la violarea datelor cu caracter personal pentru a include serviciile societății informaționale, dat fiind impactul esențial asupra protecției datelor cu caracter personal ale tuturor cetățenilor Uniunii Europene.

Adoptat la Bruxelles la 10/02/2009

Pentru Grupul de lucru
Președinte
Alex TÜRK

---

23 În amendamentul 133.
24 Ase vedea amendamentul 132 al Parlamentului.
25 În observațiile privind amendamentul 127 al Parlamentului.
26 A se vedea amendamentele 139 și 186/rev ale Parlamentului.
27 În articolul 3 și în considerentul 28.