GRUPUL DE LUCRU ARTICOLUL 29 PRIVIND PROTECȚIA DATELOR

01189/09/RO
WP 163

Avizul 5/2009 privind socializarea în rețea online

Adoptat la 12 iunie 2009

Prezentul grup de lucru a fost înființat în temeiul articolului 29 din Directiva 95/46/CE. Acesta reprezintă un organism european consultativ independent privind protecția datelor şi a vieții private. Misiunile acestuia sunt descrise în articolul 30 din Directiva 95/46/CE şi în articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de către Direcția D (Drepturi fundamentale şi cetățenie) a Comisiei Europene, Direcția Generală Justiție, Libertate şi Securitate, B-1049 Bruxelles, Belgia, Birou nr. LX-46 01/02.

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

Cuprins

Rezumat

Prezentul aviz se concentrează asupra modului în care funcționarea site-urilor de socializare în rețea poate respecta dispozițiile cuprinse în legislația UE privind protecția datelor. Obiectivul său principal este de a oferi îndrumări furnizorilor de servicii de socializare în rețea (SSR) privind măsurile care trebuie aplicate pentru a garanta respectarea legislației UE.

În aviz se semnalează că furnizorii SSR și, în numeroase cazuri, furnizorii terți de aplicații sunt operatori de date cu anumite obligații față de utilizatorii SSR. Avizul subliniază că un număr mare de utilizatori acționează într-un sector personal, intrând în contact cu alte persoane în decursul acțiunilor de abordare a problemelor de natură personală, familială sau domestică. În acest tip de cazuri, avizul precizează că se aplică „excepția activităților domestice", și nu reglementările referitoare la operatorii de date. Avizul menționează, de asemenea, condițiile în care activitățile unui utilizator SSR nu sunt acoperite de „excepția activităților domestice". Diseminarea și utilizarea informațiilor disponibile pe SSR în alte scopuri secundare, fără o intenție definită, reprezintă principalul motiv de îngrijorare al grupului de lucru „Articolul 29". Configurațiile implicite care favorizează un nivel ridicat de securitate și protecția vieții private sunt promovate în cadrul avizului ca reprezentând punctul ideal de plecare în ceea ce privește toate serviciile oferite. Accesarea informațiilor privind profilul utilizatorului se evidențiază ca unul dintre motivele principale de îngrijorare. Se abordează, de asemenea, teme precum prelucrarea datelor și a imaginilor sensibile, inserarea de anunțuri publicitare și de marketing direct la nivelul SSR, precum și aspecte referitoare la păstrarea datelor.

Principalele recomandări fac referire în special la obligațiile furnizorilor SSR de a respecta Directiva privind protecția datelor și de a susține și consolida drepturile utilizatorilor. Obligația furnizorilor SSR de a informa utilizatorii cu privire la identitatea lor și de a evidenția diferitele scopuri pentru care prelucrează datele cu caracter personal prezintă o importanță covârșitoare. Furnizorii SSR trebuie să acorde o atenție deosebită prelucrării datelor cu caracter personal ale minorilor. În aviz se recomandă să se permită utilizatorilor să încarce imagini sau informații despre alte persoane fizice doar dacă au acordul persoanelor în cauză și, în plus, se menționează că SSR au, de asemenea, datoria de a informa utilizatorii cu privire la drepturile celorlalți la viață privată.

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR FIZICE ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

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

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

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

având în vedere Regulamentul său de procedură,

ADOPTĂ PREZENTUL DOCUMENT:

1. Introducere

Dezvoltarea comunităților web și a serviciilor găzduite, precum serviciile de socializare în rețea („SSR") reprezintă un fenomen relativ recent, caracterizat prin creșterea exponențială constantă a numărului de utilizatori ai acestor site-uri.

Informațiile cu caracter personal pe care un utilizator le publică online, alături de datele care descriu acțiunile sale și interacțiunile cu alte persoane pot crea un profil cuprinzător, care să cuprindă pasiunile și activitățile persoanei respective. Datele cu caracter personal publicate pe site-urile de socializare în rețea pot fi utilizate de părțile terțe în scopuri multiple, inclusiv în scopuri comerciale și pot crea riscuri majore, precum furtul de identitate, pierderi financiare, pierderea unor oportunități comerciale sau de angajare și daune fizice.

Grupul internațional de lucru din Berlin pentru protecția datelor din domeniul telecomunicațiilor a adoptat *Memorandumul de la Roma*[2] în luna martie a anului 2008. Memorandumul analizează riscurile rețelelor de socializare asupra vieții private și asupra securității și oferă îndrumări autorităților de reglementare, furnizorilor și utilizatorilor. Rezoluția privind viața privată în cadrul serviciilor de socializare în rețea,[3] adoptată recent, abordează, de asemenea, provocările SSR. Grupul de lucru ia totodată în considerare documentul de poziție publicat de Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) în octombrie 2007, „*Aspecte privind securitatea și recomandări în privința rețelelor de socializare online*"[4], adresat autorităților de reglementare și furnizorilor de rețele de socializare.

---

1 Jurnalul Oficial L281, 23.11.1995, p. 31, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Adoptat la cea de-a 30-a Conferință internațională privind protecția datelor și comisarii pentru protecția vieții private din Strasbourg, 17.10.2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

2. Definiția „serviciului de socializare în rețea (SSR)” și modelul comercial

În linii mari, SSR pot fi definite ca platforme de comunicare online care oferă persoanelor fizice posibilitatea de a se alătura unei rețele sau de a crea rețele de utilizatori care împărtășesc aceleași opinii. Din punct de vedere juridic, rețelele de socializare reprezintă servicii ale societății informaționale, conform definiției prevăzute la articolul 1 alineatul (2) al Directivei 98/34/CE astfel cum a fost modificată prin Directiva 98/48/CE. SSR prezintă anumite caracteristici comune:

- utilizatorii sunt invitați să furnizeze date cu caracter personal cu scopul de a crea o descriere personală sau un „profil”.

- SSR oferă, de asemenea, instrumente care să permită utilizatorilor să publice propriile materiale (conținut generat de utilizator, cum ar fi o fotografie, o intrare din jurnal, muzică, videoclipuri sau link-uri către alte site-uri[5]);

- „socializarea în rețea” este facilitată de utilizarea unor instrumente care prezintă pentru fiecare utilizator o listă de contacte cu care utilizatorii pot interacționa.

O mare parte din profiturile obținute de SSR sunt generate prin inserarea de anunțuri publicitare în cadrul configurației paginilor web și accesarea acestora de către utilizatori. Utilizatorii care publică în cadrul profilului un număr mare de informații privind pasiunile lor, constituie o țintă comercială directă pentru părțile care fac publicitate și care doresc să trimită anunțuri selective în baza acelor informații.

Prin urmare, este important ca SSR să funcționeze într-un mod prin care să respecte drepturile și libertățile utilizatorilor care au încredere legitimă în faptul că datele personale pe care le divulgă vor fi prelucrate în conformitate cu legislația europeană și națională privind protecția datelor și a vieții private.

3. Punerea în aplicare a Directivei privind protecția datelor

Prevederile Directivei privind protecția datelor se aplică furnizorilor SSR în majoritatea cazurilor, chiar dacă sediul central al acestora nu se află în SEE. Grupul de lucru „Articolul 29” face referire la avizul său anterior privind motoarele de căutare în care se oferă orientări suplimentare în privința problemelor referitoare la instalarea și utilizarea echipamentelor, acestea fiind decisive pentru aplicarea Directivei privind protecția datelor și a normelor care derivă din prelucrarea adreselor IP și utilizarea „cookie-urilor”.[6]

3.1 Ce părți sunt considerate operatori de date?

Furnizorii SSR

Furnizorii SSR sunt operatori de date în temeiul Directivei privind protecția datelor. Aceștia pun la dispoziție metodele de prelucrare a datelor utilizatorilor și furnizează toate serviciile „de bază” referitoare la gestiunea utilizatorilor (de exemplu înregistrarea și ștergerea conturilor de utilizator). De asemenea, furnizorii SSR determină modul în care se pot utiliza datele utilizatorilor în scop publicitar și în scop de marketing – inclusiv în ceea ce privește anunțurile publicitare ale părților terțe.

---

[5] În cazurile în care SSR oferă servicii de comunicare electronică, se vor aplica, de asemenea, prevederile Directivei privind protejarea confidențialitatea în sectorul comunicațiilor publice2002/58.

.

[6] WP148, „Avizul 1/2008 privind aspectele de protecție a datelor legate de motoarele de căutare”.

Furnizorii de aplicații

Furnizorii de aplicații pot fi totodată operatori de date, în situația în care creează aplicații care rulează alături de cele SSR și dacă utilizatorii decid să utilizeze o astfel de aplicație.

Utilizatorii

În majoritatea cazurilor, utilizatorii sunt considerați a fi subiecții datelor. Directiva nu impune obligațiile unui operator de date unei persoane fizice care prelucrează datele personale *„în cursul unei activități exclusiv personale sau domestice"* – așa-numita „excepție a activităților domestice". În anumite situații, există posibilitatea ca activitățile unui utilizator SSR să nu fie acoperite de excepția activităților domestice și să se considere că utilizatorul a preluat unele dintre obligațiile unui operator de date. Unele dintre aceste situații sunt prezentate în continuare:

3.1.1. Obiectul și natura

Există o tendință din ce în ce mai pronunțată a SSR de a „*trece de la «Web 2.0 pentru divertisment» la Web 2.0 pentru productivitate și servicii*”[7], ceea ce presupune posibilitatea de extindere a activităților unor utilizatori SSR dincolo de activitățile exclusiv personale sau domestice, de exemplu în cazul în care SSR este utilizat drept o platformă de colaborare pentru o asociație sau o societate. Dacă utilizatorul SSR acționează în numele unei societăți sau asociații, sau dacă utilizează SSR în special ca o platformă de promovare a obiectivelor comerciale, politice sau caritabile, excepția nu se aplică. În acest caz, utilizatorul își asumă întreaga răspundere a unui operator de date care divulgă date personale unui alt operator de date (SSR) și părților terțe (alți utilizatori SSR sau alți eventuali operatori de date care au acces la aceste date). În aceste situații, utilizatorul trebuie să aibă acordul persoanelor în cauză sau să invoce un alt temei legitim prevăzut de Directiva privind protecția datelor.

În general, accesul la datele (date de profil, publicări, relatări…) cu care a contribuit un utilizator este limitat la contactele selectate de acesta. În anumite situații, însă, lista de contacte terțe ale utilizatorilor se poate amplifica, fără ca utilizatorul în cauză să cunoască unele contacte. Un număr ridicat de contacte poate fi un indiciu că excepția activităților domestice nu se aplică și că utilizatorul poate fi considerat operator de date.

3.1.2. Accesarea informațiilor din profil

SSR trebuie să asigure existența unor configurații implicite gratuite care favorizează protecția vieții private și limitează accesul contactelor selectate de utilizator.

Dacă accesul la informațiile din profil se extinde dincolo de contactele selectate de utilizator, ca în cazul conferirii dreptului de acces la un profil tuturor membrilor SSR[8] sau când datele sunt indexabile de motoarele de căutare, accesul nu se limitează la domeniul personal sau domestic. În mod similar, dacă un utilizator ia o decizie informată de a extinde accesul la profilul său prin acceptarea mai multor persoane în afara „prietenilor” selectați, acesta va trebui să își asume responsabilitățile unui operator de date. În mod efectiv, se va aplica același regim juridic ca în cazul în care o persoană utilizează alte platforme tehnologice pentru a publica date personale pe web[9]. În câteva state membre, lipsa restricțiilor de accesare (care determină caracterul public) presupune că Directiva privind protecția datelor se aplică în cazul utilizatorului de servicii internet care dobândește responsabilități de operator[10].

Trebuie să se rețină că și în cazul în care nu se aplică excepția activităților domestice, utilizatorul SSR poate beneficia de alte excepții, precum excepția pentru scopuri jurnalistice, artistice sau literare. În aceste cazuri, trebuie să se obțină un echilibru între libertatea de expresie și dreptul la viață privată.

3.1.3 Prelucrarea datelor părților terțe de către utilizatori

---

7 „Internetul în viitor: Europa trebuie să joace un rol esențial” discursul doamnei Reding, comisarul european pentru societatea informațională și media, în cadrul reuniunii Inițiativa privind viitorul internetului, organizată de Consiliul de la Lisabona, Bruxelles, 2 februarie 2009

8 sau dacă se poate argumenta că nu s-a realizat o selecție reală a contactelor acceptate, adică utilizatorul acceptă „contactele” fără a ține cont de legătura pe care o are cu acestea

9 Ca în cazul platformelor de publicare care nu sunt SSR, sau al programelor informatice cu gazdă proprie.

10 Decizia Satamedia a CEJ dispune contrariul în alineatul 44: „Rezultă că această a doua excepție trebuie interpretată în sensul că vizează numai activitățile care se includ în cadrul vieții private sau familiale a particularilor (a se vedea Hotărârea Lindqvist, citată anterior, punctul 47). În mod evident, această situație nu se regăsește în cazul activităților exercitate de Markkinapörssi și de Satamedia, al căror obiect este aducerea datelor colectate la cunoștința unui număr nedeterminat de persoane.”

Aplicarea excepției activităților domestice este, totodată, limitată de necesitatea de a garanta drepturile părților terțe, în special în ceea ce privește datele sensibile. În plus, trebuie să se precizeze că și în cazul în care se aplică excepția activităților domestice, un utilizator poate fi considerat răspunzător conform dispozițiilor generale ale legislațiilor naționale civile sau penale în cauză (de exemplu, calomniere, răspundere delictuală pentru încălcarea dreptului la personalitate, răspundere penală).

3.2 Securitate și configurațiile implicite privind viața privată

Prelucrarea în condiții de siguranță a informațiilor reprezintă un element esențial de încredere în SSR. Operatorii trebuie să aplice măsurile tehnice și organizatorice adecvate, „atât în momentul proiectării sistemului de prelucrare, cât și în cel al prelucrării în sine" în scopul menținerii securității și prevenirii oricărei prelucrări neautorizate, luând în considerare riscurile reprezentate de prelucrarea datelor și de natura acestora[11].

Un element important al configurațiilor privind viața privată este accesarea datelor cu caracter personal publicate într-un profil. Dacă nu există restricții privind accesul la astfel de date, părțile terțe pot avea acces la detalii intime referitoare la utilizatori, fie în calitate de membru al SSR, fie prin intermediul unui motor de căutare. Cu toate acestea, numai un număr restrâns de utilizatori modifică configurațiile implicite când subscriu la acest tip de serviciu. Prin urmare, SSR ar trebui să stabilească configurațiile implicite care favorizează protecția vieții private și care permit utilizatorilor să accepte în mod liber și specific orice accesare a conținutului profilului lor care depășește limitele listei de contacte selectate, cu scopul de a reduce riscul prelucrării ilegale de către părțile terțe. Profilurile cu accesare limitată nu trebuie să poată fi descoperite de motoarele interne de căutare, nici prin funcția de a găsi utilizatori în funcție de anumiți parametri, precum vârsta sau locația. Există posibilitatea ca deciziile de a extinde accesul să nu fie implicite[12], spre exemplu în cazul unei excluderi voluntare („opt-out") realizate de un operator al SSR.

3.3 Informațiile care vor furnizate de către SSR

Furnizorii SSR au obligația de a informa utilizatorii cu privire la identitatea lor și de a evidenția scopurile diferite pentru care prelucrează datele cu caracter personal în conformitate cu prevederile articolului 10 din Directiva privind protecția datelor inclusiv, dar fără a se limita la:

- utilizarea datelor în scop de marketing direct;
- posibila partajare a datelor cu anumite categorii de părți terțe;
- o prezentare generală a profilurilor: crearea acestora și principalele surse de informații folosite;
- utilizarea datelor sensibile.

Grupul de lucru recomandă:

- furnizorilor SSR să transmită utilizatorilor avertismente adecvate cu privire la riscurile la adresa vieții private a lor și a altora în momentul încărcării informațiilor în SSR;

---

[11] Articolul 17 și considerentul 46 din Directiva privind protecția datelor.

[12] Raportul și orientările privind protecția vieții private în cadrul serviciilor de socializare în rețea („Memorandumul de la Roma") indicată riscuri precum „Noțiunea înșelătoare de comunitate", p2, „Riscul de a furniza mai multe informații personale decât credeți", p3. O societate de securitate informatică avertizează un SSR important cu privire la accesul prestabilit al membrilor din aceeași zonă geografică:
http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html

- să se reamintească utilizatorilor SSR că încărcarea informațiilor despre alte persoane poate încălca dreptul acestora la viață privată și dreptul de protecție a datelor;

- SSR să își informeze utilizatorii că, dacă doresc să încarce imagini sau informații despre alte persoane, ar trebui să aibă acordul persoanei în cauză[13].

3.4 Date sensibile

Datele care indică originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice, apartenența la un sindicat sau datele privind starea de sănătate sau viața sexuală sunt considerate a fi sensibile. Datele sensibile cu caracter personal pot fi publicate pe internet doar cu acordul explicit al persoanei vizate de aceste date sau dacă acestea au fost făcute publice chiar de subiectul datelor.[14]

În anumite state membre ale UE, imaginile cu persoanele vizate sunt considerate o categorie specială deoarece pot fi utilizate pentru a distinge între originea rasială/etnică sau pot fi utilizate pentru a deduce convingerile religioase sau informații despre starea de sănătate. În general, grupul de lucru nu consideră imaginile de pe internet drept date sensibile[15], decât dacă acestea sunt utilizate în mod evident pentru a divulga date sensibile despre persoane.

În calitate de operatori de date, SSR nu poate prelucra orice tip de date sensibile despre membrii SSR fără a avea acordul explicit al acestora[16]. Dacă un SSR include în formularul pentru crearea profilului adresat utilizatorilor întrebări cu privire la date sensibile, SSR trebuie să menționeze clar că răspunsul la acele întrebări este complet opțional.

3.5 Prelucrarea datelor despre persoanele fără statut de membru

Numeroase SSR permit utilizatorilor să ofere informații despre alte persoane, spre exemplu prin asocierea unui nume cu o imagine, oferind un calificativ unei persoane, enumerând „persoanele pe care le-am cunoscut/pe care aș vrea să le cunosc" la evenimente. Acest tip de marcaj permite identificarea persoanelor care nu au statut de membru. Cu toate acestea, prelucrarea acestor date despre persoanele fără statut de membru de către SSR poate fi realizată doar dacă se îndeplinește unul dintre criteriile prevăzute la articolul 7 din Directiva privind protecția datelor.

În plus, crearea profilurilor persoanelor fără statut de membru, realizate în prealabil prin acumularea datelor care sunt furnizate în mod independent de utilizatorii SSR, inclusiv a datelor deduse din agendele de adrese online, nu are un temei juridic.[17]

Chiar dacă SSR a avut posibilitatea de a contacta persoana în cauză fără statut de utilizator pentru a îl/o informa cu privire la existența unor date cu caracter personal despre el/ea, o eventuală invitație trimisă prin poșta electronică de a se alătura SSR pentru a accesa aceste

---

[13] Această notificare poate fi facilitată prin introducerea unor instrumente de gestionare a marcajelor în cadrul site-urilor web de socializare în rețea, de exemplu prin permiterea accesării unor domenii dintr-un profil personal pentru a indica existența numelui unui utilizator în imaginile sau videoclipurile marcate pentru care se așteaptă acordul, sau prin stabilirea unor date de expirare a marcajelor care nu au primit acordul persoanei marcate.

[14] Statele membre pot stabili excepții de la această regulă; a se vedea articolul 8 alineatul (2) litera (a) cea de-a doua teză și articolul 8 alineatul (4) din Directiva privind protecția datelor.

[15] Publicarea imaginilor pe internet ridică semne din ce în ce mai numeroase de îngrijorare cu privire la protejarea vieții private, ca urmare a dezvoltării tehnologiilor de recunoaștere a fețelor.

[16] Acordul trebuie fie liber, informat și specific.

[17] Considerentul 38 din Directiva privind protecția datelor prevede: *„întrucât, dacă prelucrarea datelor este corectă, persoanele vizate ar trebui să aibă posibilitatea de a afla despre existența prelucrărilor și să beneficieze, atunci când datele sunt colectate de la acestea, de o informare precisă și completă, ținând seama de circumstanțele colectării.*" Pentru anumite SSR, se pare că publicarea profilurilor persoanelor care nu au statut de membru a devenit o metodă importantă de a-și lansa „serviciile".

date ar încălca interdicția prevăzută la articolul 13 alineatul (4) din Directiva privind confidențialitatea în mediul electronic privind trimiterea mesajelor electronice nesolicitate în scopul marketingului direct.

3.6 Accesul părților terțe

3.6.1 Acces prin intermediul SSR

În plus față de serviciile de bază SSR, majoritatea SSR oferă utilizatorilor aplicații suplimentare furnizate de dezvoltatori terți care prelucrează, de asemenea, datele cu caracter personal.

SSR trebuie să dispună de posibilitatea de a se asigura că aplicațiile părților terțe respectă prevederile Directivei privind protecția datelor și ale Directivei privind confidențialitatea în mediul electronic. Aceasta presupune, în special, că utilizatorii primesc informații clare și specifice din partea SSR cu privire la prelucrarea datelor lor personale și că au acces doar la datele personale necesare. Prin urmare, SSR trebuie să ofere dezvoltatorilor terți acces stratificat astfel încât aceștia să poată alege un mod de accesare mai limitat la nivel intern. SSR trebuie, în plus, să se asigure că utilizatorii pot raporta cu ușurință orice îngrijorare pe care o au în privința aplicațiilor.

3.6.2 Accesul părților terțe, mijlocit de utilizatori

SSR permite uneori utilizatorilor să își acceseze și să își actualizeze datele folosind alte aplicații. Spre exemplu, utilizatorii ar putea să:

- citească și să publice mesaje în rețea prin intermediul telefonului mobil;
- sincronizeze datele de contact ale prietenilor din SSR cu agenda lor de adrese, de pe un calculator personal;
- își actualizeze starea sau locația în SSR în mod automat prin intermediul unui alt site web.

SSR publică modul în care acest program informatic poate fi scris sub forma unei „Interfețe de programare a aplicațiilor” („API”). Acesta oferă oricărei părți terțe posibilitatea de a scrie un program informatic pentru a îndeplini aceste sarcini și de a permite utilizatorilor să aleagă liber unul dintre mai mulți furnizori terți[18]. Dacă un SSR pune la dispoziție un API care permite accesul la datele contactelor, acesta trebuie:

- să garanteze un nivel de detaliere care să permită utilizatorului să selecteze un nivel de accesare pentru partea terță care să fie suficient în vederea realizării unei anumite sarcini.

La accesarea datelor personale prin intermediul API al unei părți terțe în numele unui utilizator, serviciile părții terțe trebuie:

- să prelucreze și să păstreze datele pentru o perioadă care să nu depășească timpul necesar pentru realizarea unei anumite sarcini;
- să nu efectueze operații asupra datelor importate aferente contactelor utilizatorului cu excepția utilizării acestora de către utilizatorul care le-a introdus.

[18] Deși „API” este un termen tehnic generic, în acest context API se referă la accesul în numele utilizatorului, adică utilizatorii trebuie să introducă prerogativele de conectare astfel încât acesta să poată acționa în numele lor.

3.7 Temeiuri juridice pentru marketingul direct

Marketingul direct reprezintă o componentă fundamentală a modelului de afaceri al SSR; serviciul poate folosi diferite modele de marketing direct. Cu toate acestea, marketingul care folosește datele personale ale utilizatorilor trebuie să se realizeze în conformitate cu prevederile relevante cuprinse atât în Directiva privind protecția datelor, cât și în Directiva privind confidențialitatea în mediul electronic[19].

Marketingul contextual este personalizat în funcție de conținutul vizualizat sau accesat de utilizator[20].

Marketingul pe segmente constă în trimiterea de anunțuri publicitare unor grupuri țintă de utilizatori[21]; un utilizator este încadrat într-un grup în funcție de informațiile pe care le-a furnizat direct către SSR[22].

În cele din urmă, *marketingul comportamental* selectează anunțurile publicitare ca urmare a observării și analizării activității utilizatorului de-a lungul timpului. Aceste tehnici pot face obiectul diferitelor dispoziții legale, în funcție de temeiurile juridice aplicabile și de caracteristicile tehnicii folosite. Grupul de lucru recomandă să nu se utilizeze datele sensibile în modelele de publicitate bazate pe comportament până nu se vor întruni toate dispozițiile legale.

Indiferent de modelul utilizat sau de combinația de modele utilizată, anunțurile publicitare pot fi trimise direct prin SSR (furnizorul SSR are în acest caz un rol de intermediar) sau prin intermediul unei părți terțe care face publicitate. În primul caz, datele personale ale utilizatorilor nu trebuie să fie divulgate părților terțe. În cel de-al doilea caz, însă, există posibilitatea ca partea terță care face publicitate să proceseze datele personale referitoare la utilizatori dacă, spre exemplu, aceasta prelucrează adresa IP a utilizatorului și un cookie care a fost stocat în calculatorul utilizatorului.

3.8 Păstrarea datelor

SSR nu intră sub incidența definiției serviciilor de comunicații electronice prevăzută la articolul 2 litera (c) din Directiva-cadru (2002/21/CE). Furnizorii SSR pot oferi servicii suplimentare care intră sub incidența unui serviciu de comunicații electronice cum ar fi un serviciu public de poștă electronică. Un astfel de serviciu va face obiectul dispozițiilor Directivei privind confidențialitatea în mediul electronic și Directivei privind păstrarea datelor.

Anumite SSR permit utilizatorilor lor să trimită invitații părților terțe. Interdicția de a utiliza poșta electronică în scopul marketingului direct nu se aplică în cazul comunicărilor personale. Pentru a putea respecta excepția la comunicările personale, un SSR trebuie să întrunească următoarele criterii:

- nu se va oferi niciun stimulent expeditorului sau destinatarului;
- furnizorul nu va selecta destinatarii mesajelor;[23]

---

19 Grupul de lucru intenționează să abordeze diferitele aspecte ale publicității online într-un document separat în viitorul apropiat.

20 De exemplu, dacă pagina afișată cuprinde cuvântul „Paris”, anunțul publicitar ar putea face referire la un restaurant din acest oraș.

21 Fiecare grup este definit printr-un set de criterii.

22 De exemplu, când s-a înregistrat în serviciu.

23 De exemplu, obiceiul unor SSR de a trimite invitații fără discriminare întregii agende de adrese a unui utilizator nu este permis.

- identitatea utilizatorului expeditor trebuie să fie menționată clar;
- utilizatorul expeditor trebuie să cunoască întregul conținut al mesajului care va fi trimis în numele său.

De asemenea, anumite SSR păstrează datele de identificare ale utilizatorilor care au fost eliminați din serviciu, pentru a se asigura că aceștia nu se vor înregistra din nou. În acest caz, utilizatorii în cauză trebuie să fie informați că se efectuează această prelucrare a datelor. În plus, singurele informații care pot fi păstrate sunt informațiile de identificare, și nu motivele pe care s-a bazat eliminarea utilizatorilor în cauză. Aceste informații nu trebuie păstrate mai mult de un an.

Datele personale comunicate de către un utilizator în momentul înregistrării într-un SSR trebuie să fie șterse imediat ce utilizatorul sau furnizorul SSR decid să șteargă contul respectiv[24]. De asemenea, informațiile șterse de un utilizator la actualizarea contului său nu trebuie păstrate. Înainte de a întreprinde aceste acțiuni, SSR va informa utilizatorii cu privire la aceste perioade de păstrare a informațiilor, folosind mijloacele pe care le are la dispoziție. Din motive de siguranță și legale, în anumite situații se poate admite păstrarea datelor actualizate sau șterse și a conturilor pentru o perioadă definită de timp cu scopul de a contribui la evitarea acțiunilor premeditate care pot avea drept rezultat furtul de identitate și alte infracțiuni sau delicte.

Dacă un utilizator nu folosește serviciul pentru o perioadă definită de timp, profilul trebuie dezactivat, ceea ce presupune că nu va mai putea fi vizualizat de alți utilizatori sau de vizitatori, urmând ca după o altă perioadă de timp datele din contul abandonat să fie șterse. Înainte de efectua aceste operații, SSR trebuie să notifice utilizatorii folosind orice tip de mijloace disponibile.

3.9 Drepturile utilizatorilor

SSR trebuie să respecte drepturile persoanelor vizate de prelucrarea datelor conform prevederilor din articolele 12 și 14 din Directiva privind protecția datelor.

Drepturile de accesare și rectificare ale utilizatorilor nu sunt limitate la utilizatorii serviciului, fiind garantate oricărei persoane fizice ale cărei date personale sunt prelucrate[25]. Membrii și persoanele fără statut de membru din cadrul SSR trebuie să dispună de o modalitate de a-și exercita dreptul de accesare, corectare și ștergere a datelor. Prima pagină a site-urilor SSR trebuie să facă referire clară la existența unui „birou de gestionare a reclamațiilor", înființat de furnizorul SSR, care să fie responsabil pentru problemele referitoare la protecția datelor și a vieții private și pentru reclamațiile primite atât din partea membrilor, cât și din partea persoanelor fără statut de membru.

Articolul 6 alineatul (1) litera (c) din Directiva privind protecția datelor prevede că datele trebuie să fie *„adecvate, pertinente și neexcesive în ceea ce privește scopurile în care sunt colectate și/sau prelucrate ulterior"*. În acest context, se observă că poate exista necesitatea ca SSR să înregistreze anumite informații pentru identificarea membrilor, fără a fi nevoie să publice pe internet numele reale ale membrilor. Prin urmare, SSR trebuie să analizeze cu atenție dacă poate justifica obligația impusă membrilor de a acționa folosind numele real în locul unui pseudonim. Există argumente puternice în favoarea posibilității de a prezenta

[24] Conform articolului 6 alineatul 1 litera (e) din Directiva privind protecția datelor, datele trebuie „*păstrate într-o formă care permite identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar în vederea atingerii scopurilor pentru care au fost colectate sau pentru care vor fi prelucrate ulterior."*

[25] Spre exemplu, cazul în care adresa electronică a persoanei în cauză a fost utilizată de serviciul SSR pentru a-i trimite o invitație.

utilizatorilor o alternativă în acest sens, această situație făcând obiectul cerințelor legale în cel puțin un stat membru. Argumentele sunt deosebit de puternice, în special în cazul SSR cu un număr mare de membri.

Articolul 17 din Directiva privind protecția datelor prevede că operatorul trebuie să aplice măsurile tehnice și organizatorice de protecție adecvate pentru protejarea datelor cu caracter personal. Aceste măsuri de protecție includ în special verificarea accesărilor și mecanismele de autentificare care pot fi puse în aplicare dacă se utilizează pseudonimele.

4. Copiii și minorii

Serviciile SSR sunt utilizate într-un procent mare de copii/minori. Avizul WP147 al grupului de lucru[26] s-a axat pe aplicarea principiilor privind protecția datelor în mediul școlar și educațional. În aviz s-a subliniat nevoia de a lua în considerare interesul copilului, prevăzut, de asemenea, în Convenția ONU privind drepturile copilului. Grupul de lucru dorește să accentueze, de asemenea, importanța acestui principiu în contextul SSR.

La nivel mondial, autoritățile din domeniul protecției datelor au întreprins inițiative interesante[27] care se concentrează în special pe sensibilizarea publicului în privința SSR și a eventualelor riscuri. Grupul de lucru încurajează continuarea cercetărilor pe tema abordării dificultăților întâmpinate la verificarea vârstei și a consimțământului informat cu scopul de a răspunde mai eficient acestor provocări.

Bazându-se pe considerațiile anterioare, grupul de lucru consideră că soluția potrivită pentru a ataca problema protecției datelor copiilor în contextul SSR ar fi o strategie multidimensională. Aceasta s-ar baza pe:

- inițiativele de sensibilizare a publicului, care sunt esențiale în vederea asigurării unei implicări active a copiilor (prin intermediul școlilor, prin includerea unor informații de bază privind protecția datelor în programele școlare, prin crearea unor instrumente educaționale ad-hoc și colaborarea organismelor naționale competente);

- prelucrarea corectă și legală a datelor privind minorii, precum neincluderea în formularele de înscriere a întrebărilor privind informațiile sensibile, lipsa prospectării în special în ceea ce privește minorii, obținerea acordului prealabil al părinților anterior înscrierii și niveluri adecvate de separare logică a comunităților de copii de cele de adulți;

- punerea în aplicare a tehnologiilor de protecție a vieții private (Privacy Enhancing Technologies - PET) – de exemplu, configurațiile implicite care favorizează protecția vieții private, ferestre de tip pop-up de avertizare în cadrul etapelor corespunzătoare, programe informatice de verificare a vârstei);

- auto-reglementarea din partea furnizorilor, cu scopul de a încuraja adoptarea unor coduri de conduită completate prin măsuri eficiente de punere în aplicare a acestora, care să prezinte, de asemenea, caracteristici disciplinare;

- dacă este necesar, măsuri legislative ad-hoc care să descurajeze practicile necinstite și/sau înșelătoare din contextul SSR.

---

26 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf

27 Spre exemplu, inițiativa portugheză „Dadus" http://dadus.cnpd.pt/, cartela daneză de identificare în programele de conversație Chat Check Badge, http://www.fdim.dk/

5. Sinteză a obligațiilor/drepturilor

Aplicabilitatea directivelor CE

1. Directiva privind protecția datelor se aplică în general în cazul prelucrării datelor cu caracter personal de către SSR, chiar și atunci când sediul principal al acestora nu se află în SEE.

2. Furnizorii SSR sunt considerați operatori de date în temeiul Directivei privind protecția datelor.

3. Furnizorii de aplicații pot fi considerați operatori de date în temeiul Directivei privind protecția datelor.

4. Utilizatorii sunt considerați persoanele vizate, în contextul prelucrării datelor acestora de către SSR.

5. Prelucrarea datelor cu caracter personal de către utilizatori este acoperită în majoritatea cazurilor de excepția activităților domestice. Există situații în care activitățile întreprinse de un utilizator nu sunt acoperite de această excepție.

6. SSR nu fac obiectul definiției serviciilor de comunicații electronice, Directiva privind păstrarea datelor neaplicându-se, prin urmare, în cazul SSR.

Obligațiile SSR

7. SSR ar trebui să informeze utilizatorii cu privire la identitatea lor și să prezinte informații cuprinzătoare și clare privind scopurile și metodele diferite pe care intenționează să le aplice în prelucrarea datelor cu caracter personal.

8. SSR ar trebui să asigure existența unor configurații implicite care favorizează protecția vieții private.

9. SSR ar trebui să furnizeze utilizatorilor informații și avertismente adecvate cu privire la riscurile la care poate fi suspusă viața privată în momentul încărcării datelor pe SSR.

11. Utilizatorii trebuie să fie informați de către SSR că imaginile și informațiile privind alte persoane ar trebui încărcate doar cu acordul persoanei în cauză.

12. Ca o cerință minimă, pagina de bază a SSR trebuie să cuprindă un link către o funcție de depunere a reclamațiilor privind protecția datelor, care să fie adresată atât membrilor, cât și persoanelor fără statut de membru.

13. Activitatea de marketing trebuie să respecte normele stabilite prin Directiva privind protecția datelor și Directiva privind confidențialitatea în mediul electronic.

14. SSR trebuie să stabilească perioade maxime pentru păstrarea datelor privind utilizatorii inactivi. Conturile abandonate trebuie să fie șterse.

15. În ceea ce privește minorii, SSR ar trebui să ia măsurile adecvate pentru a limita riscurile.

Drepturile utilizatorilor

16. Atât membrii, cât și persoanele fără statut de membru din cadrul SSR beneficiază de drepturile persoanelor vizate, în cazul în care acestea sunt aplicabile, conform prevederilor articolelor 10 – 14 din Directiva privind protecția datelor.

17. Atât membrii, cât și nemembrii trebuie să aibă acces la o procedură facilă de înaintare a reclamațiilor, creată de SSR.

18. În general, ar trebui să se permită utilizatorilor să folosească un pseudonim.

Adoptat la Bruxelles, 12 iunie 2009

Pentru grupul de lucru
Președintele
Alex TÜRK