ApTI– Asociația pentru Tehnologie şi Internet
info@apti.ro
www.apti.ro

1 noiembrie 2011

Observații la Proiectul de ordonanță de urgență privind modificarea şi completarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice

Cu privire la proiectul de **ordonanță de urgență privind modificarea şi completarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice,** publicat de către Ministerul Comunicațiilor şi Societății Informaționale pe site-ul său în data de 7 octombrie 2011, vă rugăm să primiți comentariile de mai jos ale Asociației pentru Tehnologie şi Internet (ApTI), ca reprezentant al societății civile interesat de dezvoltarea unui Internet sigur şi deschis.

Proiectul de ordonanță de urgență îşi propune să transpună modificările aduse Directivei 2002/58/CE prin Directiva 2009/136/CE. Însă modul în care se realizează această transpunere prezintă o serie de neajunsuri, fie prin nepreluarea corectă a prevederilor europene, fie prin simpla preluare a traducerii acestora în limba română, fără să se încerce să se dea o formă şi un înțeles care să permită o implementarea nu doar clară şi predictibilă, dar şi eficientă din punct de vedere al scopului urmărit, acela al asigurării protecției datelor cu caracter personal şi vieții private ale utilizatorilor serviciilor de comunicații electronice.

Subliniem faptul că **în conformitate cu art. 11 alin.(3) din Legea 52/2003 modificată prin Legea 242/2010, MCSI este obligat "să justifice în scris nepreluarea recomandărilor formulate şi înaintate în scris de cetățeni şi asociațiile legal constituite ale acestora."**

În acest context, atragem atenția asupra următoarele probleme, în ordinea importanței lor:

1. Mesaje comerciale nesolicitate

Articolul 12 al Legii nr.506/2004 (care transpune art.13 al Directivei 2002/58/CE) interzice efectuarea de comunicări comerciale prin utilizarea unor sisteme automate de apelare şi comunicare care nu necesită intervenția unui operator uman, prin fax ori prin poştă electronică sau prin orice altă metodă care foloseşte serviciile de comunicații electronice destinate publicului, cu excepția cazului în care abonatul sau utilizatorul vizat şi-au exprimat în prealabil consimțământul expres pentru a primi asemenea comunicări.

Prin modificările aduse Directivei 2002/58/CE, Uniunea Europeană încearcă să promoveze noi măsuri de contracarare a fenomenului mesajelor comerciale nesolicitate transmise prin intermediul serviciilor de comunicații electronice, prin introducerea posibilității ca şi entitățile private care sunt afectate direct sau indirect de această problemă (ISP-işti, furnizori de servicii de găzduire, etc) să poată iniția proceduri legale directe împotriva celor care încalcă prevederile legale referitoare la transmiterea de mesaje comerciale. Astfel, considerentul (68) al Directivei 2009/136/CE arată că:

„Furnizorii de servicii de comunicaţii electronice fac investiţii substanţiale pentru a combate comunicaţiile comerciale nesolicitate („spam"). Aceştia sunt avantajaţi în comparaţie cu utilizatorii finali întrucât posedă cunoştinţele şi resursele necesare detectării şi identificării spammerilor. Furnizorii de servicii de poştă electronică şi furnizorii de alte servicii ar trebui, prin urmare, să aibă posibilitatea de a iniţia acţiuni legale împotriva spammerilor şi de a proteja în acest fel interesele clienţilor ca parte a propriilor interese legitime de afaceri."

Ca urmare, noul alin.(6) al art.13 al Directivei 2002/58/CE conţine următoarele prevederi:

"(6) Fără a se aduce atingere niciunei măsuri corective administrative pentru care ar putea fi adoptate dispoziţii, inter alia, în temeiul articolului 15a alineatul (2), statele membre se asigură că orice persoană fizică sau juridică afectată în mod negativ de încălcările dispoziţiilor naţionale adoptate în temeiul prezentului articol si care are în consecinţă un interes legitim de a pune capăt sau de a interzice astfel de încălcări, inclusiv un furnizor de servicii de comunicaţii electronice care îsi protejează interesele sale legitime comerciale, poate iniţia proceduri legale împotriva unor astfel de încălcări în faţa instanţelor judecătoresti. Statele membre pot, de asemenea, să prevadă dispoziţii specifice privind penalităţile aplicabile furnizorilor de servicii de comunicaţii electronice care, prin neglijenţă, contribuie la încălcarea dispoziţiilor naţionale adoptate în temeiul prezentului articol."

Observăm că, în proiectul de ordonanţă de urgenţă supus consultării publice, textul acestui alineat este preluat ca atare în noul alin.(5) al art.12, fără să se încerce o transpunere a prevederilor europene într-o normă clară şi utilă, care să contribuie într-adevăr la atingerea scopului urmărit. Considerăm că noul text, aşa cum apare în proiect, este lipsit de valoare practică şi nu ajută la soluţionarea problemelor existente, cu atât mai mult cu cât, chiar şi în absenţa sa, orice persoană lezată are dreptul de a iniţia proceduri legale împotriva oricărei alte persoane care i-a creat un prejudiciu.

În acest context, considerăm că este necesară revizuirea alin.(5) al art.12, aşa cum acesta este propus prin proiectul de ordonanţă de urgenţă, astfel încât transpunerea prevederilor din Directivă să se facă într-o manieră care să permită, din punct de vedere practic, atingerea scopului urmărit. Ca punct de plecare în iniţierea unor discuţii în aces sens, propunem următorul text:

„ Art.12[1]

(1) Orice persoană fizică sau juridică afectată în mod negativ de comunicările comerciale nesolicitate poate să iniţieze o acţiune în instanţă pentru încetarea şi interzicerea încălcării prevederilor art.12, ca şi obţinerea de despăgubiri.

(2) În cazul în care acţiunea este iniţiată de un furnizor de servicii de comunicaţii electronice, un furnizor de servicii ale societăţii informaţionale sau o asociaţie pentru protecţia consumatorilor sau pentru apărarea dreptului la viaţă privată, încălcarea prevederilor art.12 este prezumata a afectaa a interesele legitime, comerciale sau asociative, ale iniţiatorului acţiunii.

(3) În cazul în care acţiunea este iniţiată de o asociaţie pentru protectia consumatorilor sau apărarea dreptului la viaţă privată, se pot cere despăgubiri pentru mai mulţi utilizatorii de servicii de comunicaţii electronice ale căror drepturi au fost încălcate prin nerespectarea prevedrilor art.12.

(4) Sarcina probei pentru consimțământul prevazut la alin.(1) al art.12 revine furnizorului de servicii care transmite comunicările comerciale.

(5) Furnizorii de servicii de comunicații electronice au obligația de a adopta un set de măsuri de securitate care să contribuie la împiedicarea transmiterii de mesaje comerciale nesolicitate către utilizatori. Aceste măsuri sunt aplicate de către furnizori la solicitarea utilizatorilor de servicii de comunicații electronice, transmisă sub forma unor plângeri referitoare la primirea de mesaje comerciale nesolicitate. Aceste măsuri de securitate pot fi adoptate sub forma unor coduri de conduită realizate de către asociații profesionale şi/sau în ANSPDCP.

(6) Nerespectarea prevederilor art (5) reprezintă contravenție….."

2. Notificarea pentru încălcarea securității datelor cu caracter personal

a) Conform art.3 al Legii nr.506/2004, propus spre amendarea prin proiectul de ordonanță de urgență în vederea alinierii la prevederile noului art.4 al Directivei nr.2002/58/CE, furnizorii de servicii de comunicații electronice au obligația de a lua măsuri tehnice şi organizatorice adecvate în vederea garantării securității prelucrării datelor cu caracter personal. Conform noului alin.(4) propus spre a fi introdus, ANSPDCP *poate audita aceste măsuri.*

Întrucât măsurile vizate includ şi politici privind securitatea datelor, iar ANSPDCP nu dispune de capacitatea tehnică necesară pentru a realiza un audit de securitate, considerăm că este necesară revizuirea prevederii în sensul impunerii obligației efectuării unui audit de securitate de către specialişti în domeniu, urmând ca acest audit să fie ulterior supus atenției ANSPDCP.

În susținerea acestei propuneri, menționăm faptul că o procedură similară privind auditarea este prevăzută la art.49 în proiectul de ordonanță de urgență privind comunicațiile electronice:

„Art.49. – (1) În vederea aplicării prevederilor prezentului capitol, ANCOM poate solicita furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului:

a) să furnizeze toate informațiile necesare evaluării securității şi integrității rețelelor şi serviciilor, inclusiv politicile interne de securitate aplicabile;

b) **să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent sau de o altă autoritate competentă şi să transmită ANCOM rezultatele auditului.**"

Astfel, propunem modificarea alin.(4) după cum urmează:

„(4) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare ANSPDCP, **poate solicita furnizorilor de servicii de comunicații electronice destinate publicului şi furnizorilor de rețele publice de comunicații electronice să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent şi să transmită ANSPDCP rezultatele auditului**."

În ceea ce priveşte a doua teză a alin.(4) referitoare la stabilirea, de către ANSPDCP, a nivelului de securitate, propunem revizuirea textului, având în vedere prevederile alin.(1a) al

art.4 din Directiva nr.2002/58/CE (potrivit cărora autoritățile emit „recomandări cu privire la cele mai bune practici privind nivelul de securitate care trebuie atins de aceste măsuri”):

„(4[1]) **ANSPDC poate emite recomandări privind nivelul de securitate care trebuie atins prin implementarea măsurilor prevăzute la alin.(1).”**

b) Observăm că proiectul de ordonanță de urgență privind comunicațiile electronice conține prevederi referitoare la obligația furnizorilor de rețele publice de comunicații electronice şi de servicii de comunicații electronice destinate publicului de a asigura securitatea rețelelor şi serviciilor furnizate, de a notifica autoritatea de reglementare în legătură cu orice încălcare a securității care are impact asupra furnizării de rețele sau servicii şi de a se supune, la solicitarea ANCOM, unui audit de securitate, urmând să transmită rezultatele acestui audit către ANCOM.

„Art.46. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile tehnice şi organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor şi serviciilor.
(2) Măsurile luate potrivit alin. (1) trebuie să asigure un nivel de securitate corespunzător riscului identificat şi să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor şi rețelelor interconectate, având în vedere cele mai noi tehnologii.
(3) Furnizorii de rețele publice de comunicații electronice au obligația de a lua măsurile necesare pentru a garanta integritatea rețelelor şi pentru a asigura continuitatea furnizării serviciilor prin intermediul acestor rețele.
(4) Acolo unde este cazul, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului colaborează pentru implementarea măsurilor prevăzute de prezentul articol.

Art.47. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor.
[...]
Art.49. – (1) În vederea aplicării prevederilor prezentului capitol, ANCOM poate solicita furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului:
a) să furnizeze toate informațiile necesare evaluării securității şi integrității rețelelor şi serviciilor, inclusiv politicile interne de securitate aplicabile;
b) să se supună, pe cheltuiala proprie, unui audit de securitate realizat de un organism independent sau de o altă autoritate competentă şi să transmită ANCOM rezultatele auditului.
[...]”

Noile prevederi propuse spre a fi incluse în art.3 al Legii nr.506/2004 abordează problema securității prelucrării datelor cu caracter personal, fiind instituite obligații referitoare la: implementarea, de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului, de măsuri tehnice şi organizatorice necesare pentru a garanta această securitate; notificarea ANSPDCP în cazul unei încălcări a securității datelor cu caracter personal; auditarea, de către ANSPDCP, a măsurilor de securitate implementate.

În acest context, având în vedere că aceste prevederi incluse în cele două proiecte de ordonanță de urgență vizează măsurile de securitate care trebuie implementate de către

furnizori în vederea garantării securității şi integrității rețelelor şi serviciilor furnizate, precum şi a prelucrării datelor cu caracter personal, iar obligațiile impuse în ambele cazuri vizează acțiuni similare care trebuie întreprinse de către furnizori, propunem analizarea oportunității corelării acestor prevederi şi includerii lor într-un singur act normativ. O încălcare a securității „care are un impact semnificativ asupra furnizării de rețele şi servicii" poate reprezenta şi o încălcare a securității datelor cu caracter personal, astfel că măsurile luate de către furnizori pentru a garanta securitatea rețelelor şi serviciilor vor fi implementate în corelare cu cele necesare pentru garantarea securitătii datelor personale. O reglementare unitară referitoare la măsurile de securitate care trebuie implementate, la obligațiile furnizorilor referitoare la notificarea utilizatorilor şi a autorităților competente (ANCOM şi ANSPDCP) în legătură cu încălcarea securității, precum şi la realizarea auditului de securitate ar asigura o mai mare claritate în ceea ce priveşte responsabilitățile furnizorilor, iar acest lucru ar fi benefic atât pentru furnizori, cât şi pentru utilizatori şi pentru autoritățile competente.

3. Modulele de tip cookie şi accesul la informația stocată

Observăm transpunerea corectă, în proiectul de ordonanță de urgență, a prevederilor noului alin.(3) al art. 5 din Directiva 2002/58/CE referitoare la delimitarea clară a condițiilor în care este permisă stocarea de informații sau obținerea accesului la informația stocată în echipamentul terminal al unui abonat sau utilizator de servicii de comunicații electronice (aşa-numitele cookies): informarea exactă a utilizatorului în legătură cu existența aplicațiilor de tip cookies care permit stocarea de informații, cu scopul în care furnizorul prelucrează informațiile stocate şi cu posibilitatea ca utilizatorul să poată şterge informațiile stocate sau să refuze accesul terților la aceste informații.

Observăm, de asemenea, faptul că s-a încercat şi includerea, ca prevedere legală în legislația națională, a considerentului 66 din Directiva 2009/136/CE:

"În cazul în care acest lucru este posibil din punct de vedere tehnic şi eficient, în conformitate cu dispozițiile aplicabile din Directiva 95/46/CE, acordul utilizatorului privind procesarea se poate exprima prin folosirea setărilor adecvate ale unui browser sau ale unei alte aplicații. Asigurarea respectării acestor cerințe ar trebui eficientizată prin acordarea unor puteri extinse autorităților naționale competente."

Atragem însă atenția asupra faptului că textul noului alin.(**5¹**) al art.4 al Legii nr.506/2004, propus prin proiectul de OUG, nu preia corect şi în totalitate sensul considerentului mai sus menționat:

- nu există nicio mențiune referitoare la faptul că exprimarea acordului utilizatorului se poate exprima prin folosirea setărilor unui browser sau unei alte aplicații, ci doar în cazurile în care acest lucru **este posibil din punct de vedere tehnic şi eficient.** Acest lucru ar trebui sa fie stabilit in mod uniform la nivel european, dar este posibil ca sa depinda si de la tara la tara;
- nu există nicio prevedere în textul proiectului de OUG care să asigure **puteri extinse autorității competente** în vederea asigurării respectării cerinței privind posibilitatea tehnică şi eficiența soluției de exprimare a acordului prin folosirea setărilor unui browser. Acest lucru este extrem de important în acest caz.
- prevederea referitoare la „enumerarea furnizorilor cărora abonatul sau utilizatorul le interzice stocarea de informații sau accesul la informația stocată" ca metodă de obținere a acordului utilizatorilor nu doar că nu se regăseşte în textul Directivei, dar este şi extrem de vag şi reflectă principiul de „opt-out" (informațiile sunt stocate

implicit, dar utilizatorul este informat despre acest lucru şi poate solicita dezactivarea aplicațiilor respective) care este deja reglementat prin Legea nr.677/2001, şi nu pe cel de „opt-in” (este necesar acordul prealabil al utilizatorului înainte de stocarea de informații sau de dobândire a accesului la informațiile stocate), fiind, astfel, o transpunere eronată a cerințelor Directivei referitoare la obținerea acordului utilizatorilor. Dacă această măsură de enumerare a furnizorilor cărora le-a fost dat acordul privind stocarea de informații sau accesarea informației stocate ar fi prevazută doar ca element opțional, fara vreo legatură directă cu obligația prevăzută la alin.(5) al art.5, atunci ea ar putea să reprezinte un element util.

De asemenea Grupul de Lucru Articolul 29 are o interepretare[1] destul de detaliată a considerentului (66), care precizează că prevederile acestui considerent „nu constituie o excepție de la articolul 5 alineatul (3), ci mai degrabă reamintește faptul că, în acest mediu tehnologic, consimțământul poate fi dat în diferite moduri, în cazul în care acest lucru este posibil din punct de vedere tehnic, este eficient şi în conformitate cu celelalte cerințe aplicabile pentru valabilitatea consimțământului. În acest context, este relevant să se determine condițiile în care setările browserelor îndeplinesc cerințele Directivei 95/46/CE şi, astfel, constituie un consimțământ valabil *în conformitate cu Directiva 95/46.”*[2]

Observăm faptul că noul alin.(**5¹**) încearcă să creeze un echilibru între interesele legitime ale industriei de publicitate online (care consideră[3] că obligația de a obține acordul la fiecare aplicație de tip cookie ar fi nu doar cvasi-imposibilă şi inutilă, ci şi greu de implementat doar într-un anumit teritoriu - Uniunea Europeană având în vedere caracterul global al Internetului) şi interesele, şi ele legitime, ale utilizatorilor de servicii de comunicații electronice de a le fi respectat dreptul la viață privată. Semnalăm însă că soluția propusă este lipsită de claritate în ceea ce privește modalitatea de implementare a „mecanismelor” propuse pentru asigurarea respectării principiului acordului prealabil al utilizatorilor şi solicităm inițierea unor discuții între autoritățile relevante, sectorul privat şi societatea civilă în vederea identificării unor soluții care să garanteze atât respectarea prevederilor reglementărilor europene, cât şi

---

[1] Grupul de lucru pentru protecția datelor instituit în temeiul articolului 29 – Avizul nr.2/2010 privind publicitatea comportamentală online, adoptat la 22 iunie 2010. Disponibil la http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_ro.pdf

[2] Pentru ca browserele sau orice altă aplicație să poată garanta un consimțământ valabil, trebuie să se respecte următoarele cerințe:

- browserele sau alte aplicații configurate implicit să respingă modulele cookie de la terți şi care presupun ca persoana vizată să se implice într-o acțiune pozitivă de acceptare atât a introducerii, cât şi a continuării transmiterii informațiilor conținute în modulul cookie prin site-uri Internet specifice pot transmite un consimțământ valabil şi efectiv. În schimb, dacă setările browserului au fost preconfigurate să accepte toate modulele cookie, acest consimțământ nu ar respecta dispozițiile articolului 5 alineatul (3) în măsura în care, în general, acest consimțământ nu poate constitui o expresie reală a dorințelor persoanei vizate. Acest consimțământ nu ar fi nici specific şi nici prealabil (prelucrării informațiilor). Deşi o persoană vizată poate, într-adevăr, să decidă să păstreze setările pentru acceptarea tuturor modulelor cookie de la terți, nu ar fi realist ca furnizorii de rețele de publicitate să presupună că majoritatea persoanelor vizate care au browserele „setate” să accepte module cookie, au optat efectiv pentru aceasta.
- Browserele, împreună sau în combinație cu alte instrumente de informare, inclusiv colaborarea furnizorilor de rețele de publicitate cu editorii, trebuie să transmită informații clare, complete şi vizibile integral pentru a garanta un consimțământ în deplină cunoştință de cauză. Pentru a respecta cerințele Directivei 95/46/CE, browserele trebuie să transmită, în numele furnizorului de rețele de publicitate, informațiile relevante cu privire la scopurile modulelor cookie şi la prelucrarea ulterioară.Astfel, avertismentele generice fără referiri explicite la reteaua de publicitate care introduce modulul cookie nu sunt satisfăcătoare.

[3] http://articles.economictimes.indiatimes.com/2011-05-25/news/29581621_1_data-privacy-rules-privacy-rule-consent-requirement

protejarea, în mod egal, a intereselor tuturor părților implicate. Subliniem că aceasta este şi soluția sugerată de către Comisia Europeană.[4]

Având în vedere complexitatea subiectului, ca şi balanța extrem de sensibilă ce trebuie atinsă între cele două interese, considerăm că, mai ales in situația României de astazi, ar trebui ca subiectul să fie dezbatut într-un grup de lucru, în care să fie reprezentate interesele tuturor părților (MCSI, industria de publicitate online, Autoritatea pentru Protecția Datelor, organizații de protecție a consumatorilor, etc.) şi nu adoptat în mod lapidar printr-o OUG, mai ales că textul actual are toate şansele să fie considerat neconform cu prevederile directivei. Din păcate, acest lucru nu a fost făcut până acum, în timp util, însă MCSI ar trebui să îşi asume această poziție, mai ales că problema nu pare a avea soluții clare la nivelul Uniunii Europene.

În schimb, ar trebui facută o analiză clară şi precisă nu doar a eventualului impact al viitorului text, ci şi a modului de respectare a dispozițiilor legislative actuale cu privire la cookie-uri.

4. Alte observații

Atragem, de asemenea, atenția asupra preluării doar parțial corecte în textul proiectului de ordonanță, la noul art.3¹ care ar urma să fie inclus în Legea nr.506/2004, a prevederilor noului alin.(1b) al art. 4 din Directiva 2002/58/CE. Astfel, deşi în Directivă se menționează faptul că furnizorii **vor stabili** („shall establish") proceduri interne pentru a răspunde solicitărilor privind accesarea datelor cu caracter personal ale utilizatorilor, art. 3¹ prevede că furnizorii **pot** stabili astfel de proceduri. În consecință, pentru a asigura o transpunere corectă a prevederilor Directivei şi pentru mai multă claritate în exprimare, propunem modificarea art.3¹ după cum urmează:

„*Furnizorii **au obligația de a stabili** proceduri interne pentru a răspunde solicitărilor de accesare a datelor cu caracter personal ale utilizatorilor **şi de a oferi ANSPDCP, l**a cerere, informații despre procedurile respective, numărul de solicitări primite, justificarea legală invocată în solicitare şi răspunsul oferit **solicitanților**."*

[4] A se vedea discursul comisarului european pentru agendă digitală, Neelie Kroes – disponibil doar în limba engleză la adresa http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/461&format=HTML&aged=0&language=EN&guiLanguage=en