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

Centrul pentru Jurnalism Independent
staff@cji.ro
www.cji.ro

ActiveWatch
office@activewatch.ro
www.activewatch.ro

Asociaţia Pentru Apărarea Drepturilor Omului din România - Comitetul Helsinki
office@apador.org
www.apador.org

Observaţii la Proiectul de lege privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii

Ca un principiu general, **organizațiile semnatare ale prezentului document au arătat în repetate rânduri, inclusiv prin luări de poziție publice la nivelul Uniunii Europene, că Directiva Europeană 2006/24/EC privind păstrarea datelor de trafic informațional constituie o încălcare a dreptului la viață privată al cetățenilor**[1].

În România, **decizia Curții Constituționale din 8 octombrie 2009**[2] **a declarat o lege similară prezentului proiect ca fiind neconstituțională**. Argumentele Curții s-au bazat în principal pe încălcarea dreptului la viață privată prin obligația general aplicabilă de a păstra date care sunt legate în mod direct de comunicațiile private ale tuturor cetățenilor.

Curtea Constituţională subliniază că nu utilizarea justificată, în condiţiile reglementate de Legea nr.298/2008, este cea care, în sine, prejudiciază într-un mod neacceptabil exercitarea dreptului la viaţă intimă sau libertatea de exprimare, ci obligaţia legală cu caracter continuu, general aplicabilă, de stocare a datelor. Această operaţiune priveşte în egală măsură pe toţi destinatarii legii, indiferent dacă au săvârşit sau nu fapte penale sau dacă sunt sau nu subiectul unor anchete penale, ceea ce este de natură să răstoarne prezumţia de nevinovăţie şi să transforme a priori toţi utilizatorii serviciilor de comunicaţii electronice sau de reţele publice de comunicaţii în persoane susceptibile de săvârşirea unor infracţiuni de terorism sau a unor infracţiuni grave. Or, Legea nr.298/2008, deşi utilizează noţiuni şi proceduri specifice dreptului penal, are o largă aplicabilitate – practic, asupra tuturor persoanelor fizice şi juridice utilizatoare ale serviciilor de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, astfel că nu poate fi considerată ca fiind conformă prevederilor din Constituţie şi din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale referitoare la garantarea drepturilor la viaţă intimă, la secretul corespondenţei şi la liberă exprimare.

Această problemă fundamentală, inerentă directivei actuale, **nu este rezolvată de către prezentul proiect**, astfel încât opinia noastră este că prezentul proiect ar trebui declarat neconstituţional de către Curtea Constituțională a României.

[1] "Pastrarea datelor de trafic trebuie sa fie oprita in Europa - Scrisoare deschisa catre institutiile europene - 26 ianuarie 2011" – www.activewatch.ro, www.apti.ro.
[2] DECIZIA Nr.1.258 din 8 octombrie 2009 referitoare la excepţia de neconstituţionalitate a prevederilor Legii nr.298/2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii, precum şi pentru modificarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice; Publicată în Monitorul Oficial nr.798 din 23.11.2009.

De asemenea, Comisia Europeană a anunțat deja că va propune revizuirea directivei, procesul de dezbatere urmând a fi declanșat în septembrie 2011. **Considerăm că autoritățile române ar fi trebuit și încă trebuie să ia o poziție publică cu privire la Directivă, afirmând în mod ferm necesitatea revizuirii acesteia în sensul respectării dreptului la viață privată al cetățenilor europeni.** În contextul în care alte autorități din alte state (ultima ar fi Senatul olandez[3]) au fost extrem de ferme în acest sens, România trebuie să ia o atitudine consecventă cu decizia Curții Constituționale și să militeze la nivel European pentru anularea Directivei.

Mai mult, considerăm că **autoritățile române ar trebui să refuze implementarea acestei directive, chiar cu riscul declanșării de către Comisia Europeană a unei proceduri de *infringement* împotriva României**. În Germania, un calcul a arătat că statul ar plăti o amendă de 86 de eurocenți/an pe cetățean în cazul neaplicării acestei Directive[4]. Statul român s-ar asigura astfel că nu implementează o măsură nepopulară și nedemocratică și ar deveni un actor cu o voce puternică la nivelul politicilor europene, mai ales în condițiile în care soarta acestei Directive pe termen lung este încă neclară, cu un proces pe rol din Irlanda la Curtea Europeană de Justiție, cu o procedură de revizuire la nivelul Comisiei și cu presiunile în direcția revizuirii sau anulării venite din partea statelor membre și a Parlamentului European. Mai mult decât atât, dincolo de problemele legate de drepturile omului, costul direct al implementării acestei directive plătit de cetățenii români, prin operatorii de comunicații care vor fi obligați să implementeze această lege ar fi mai mult mai mare față de costul unei evenutale amenzi.

Comentariile concrete pe proiect

Cu toate aceastea, având în vedere cele reiterate în cadrul dezbaterii publice din 26 iulie 2011 prezentăm și câteva observații și comentarii concrete pe marginea proiectul de lege supus spre dezbatere publică de către Ministerul Comunicațiilor și Tehnologiei Informațiilor.

0. Legea specială pentru toate cazurile de acces la datele de trafic

Prezentul proiect trebuie să devină singura procedură specială prin care se poate obține acces la datele de trafic reținute de către operatori de comunicații. În caz contrar, va continua să planeze o incertitudine atât pentru operatorii de comunicații electronice, cât și pentru actorii din sistemul juridic cu privire la legea și practica aplicabilă într-un caz sau altul, în funcție de infracțiunea cercetată. Concret, aceasta va putea determina imposibilitatea de a folosi anumite probe în cadrul procesului penal. Mai mult, ne vom putea afla în situația unei reglementări mai dure (adică cu garanții sporite pentru respectarea drepturilor omului) pentru accesul la datele de trafic pentru infracțiunile grave decât pentru cele care nu sunt grave, ceea ce ar fi contrar logicii.

Astfel propunem introducerea unui alineat înainte de art. 1 alin. (3) cu următoarea formulare:

”Prezenta lege reprezintă singura procedură legală de acces la datele de trafic informațional ale operatorilor de comunicații electronice de către autoritățile judiciare competente pentru prevenirea, cercetarea, descoperirea și urmărirea infracțiunilor. Datele de trafic informațional stocate de către operatorii de comunicații electronice nu vor putea fi folosite în alt scop decât cel prevăzut în mod expres în art. 1 alin. (1)”.

---

[3] Vezi detalii in limba engleza la http://www.edri.org/edrigram/number9.14/dutch-senate-data-retention-evaluation

[4] Detalii in limba engleza la http://www.vorratsdatenspeicherung.de/content/view/471/79/lang,en/

1. Excepții de la implementare

Dupa cum s-a discutat în consultarea publică din 26.07.2011, estimăm că toate costurile legate de implementarea acestei legi au șanse mari de distorsionare a pieței comunicațiilor, în special pentru operatorii mici și mijlocii de servicii de acces la Internet. Având în vedere și experiența altor state în acest sens (vezi Marea Britanie), recomandăm excluderea operatorilor de comunicații electronice care au sub 100 000 de abonați de la implementarea acestei legi.

În plus, pentru ca legea 298/2008 a creat o serie de neclarități în ceea ce privește cine are obligațiile de stocare, sugerăm includerea unui articol de clarificare, de genul:
" Prezentul act normativ nu se aplică operatorilor de comunicații electronice private și nici furnizorilor de servicii ale societății informaționale"

2. Securitatea datelor reţinute

În vederea asigurării proporţionalităţii măsurilor de reţinere a datelor şi garantării protecţiei drepturilor şi libertăţilor fundamentale ale indivizilor faţă de accesarea, fără drept şi în afara cadrului legal stabilit prin prezentul proiect de lege, a datelor reţinute de către furnizori, sunt necesare garanţii legale referitoare la securitatea acestor date.

a) Deşi art.13 al proiectului de lege îşi propune să abordeze problema securităţii datelor reţinute, considerăm că actualele prevederi nu sunt suficiente pentru scopul urmărit, întrucât nu există nicio garanţie că protecţia şi securitatea utilizată la nivelul furnizorilor de reţele de comunicaţii electronice este suficientă pentru asigurarea securităţii datelor reţinute, iar termenul „corespunzătoare" din formularea „măsuri tehnice şi organizatorice corespunzătoare" este destul de vag. Considerăm că stabilirea naturii şi gradului măsurilor de protecţie în vederea garantării securităţii datelor reţinute nu trebuie lăsată exclusiv în sarcina furnizorilor, fără o formă de supraveghere din partea unei autorităţi competente (a se vedea, în acest sens, Decizia Curţii Constituţionale a Germaniei în legătură cu neconstituţionalitatea prevederilor legale referitoare la reţinerea datelor[5]).

Astfel propunem introducerea in textul legii a unor prevederi clare care pot asigura securitatea colectării şi păstrării datelor, cum ar fi:

- păstrarea datelor de trafic reținute în conformitate cu prezenta lege într-un sistem informatic independent față de sistemele actuale de operare ale operatorilor de comunicații electronice și neinterconectat pentru fiecare operator de comunicații electronice în parte;
- obligativitatea unui audit anual independent de securitate al acestui sistem informatic, care să fie trimis Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și publicat de aceasta pe site-ul propriu;
- obligativitatea unui audit anual de respectare a vieții private cu privire la ansamblul procedurilor adoptate de către fiecare operator în conformitate cu aplicarea legii 677/2001 și respectarea art XX din Constituție, care să fie trimis Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și publicat de aceasta pe site-ul propriu;
- păstrarea datelor de trafic stocate într-un format care să nu permită citirea lor directă (criptare);

[5] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html

- accesul la sistemul informatic să se poate face doar de către personalul special autorizat al operatorului, care trebuie să extragă doar datele cerute în baza cererii scrise a autorităților judiciare competente. Toate încercările de acces (reușite sau nu) la acest sistem informatic trebuie înregistrate pe un suport informatic nealterabil, ca și tipul de date extrase;
- datele extrase să poată fi trimise doar în formatul original, criptat și printr-un mediu de comunicare securizat.

Aceste obligații (care să fie menționate într-un nou alineat în completarea art.13), trebuie să fie detaliate de către Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii şi/sau Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal prin norme referitoare la măsurile de securitate care ar urma să fie aplicate de către furnizori cu privire la datele reţinute în baza legii. În elaborarea acestor norme, autoritatea/autorităţile ar urma să consulte furnizorii, precum şi alţi actori interesaţi. Autoritatea trebuie să poată verifica respectarea normelor stabilite iniţial şi să poată aplica sancţiuni în cazul încălcării respectivelor norme.

b) Având în vedere faptul că securitatea datelor reţinute poate fi periclitată şi în momentul transmiterii acestora de la furnizori către autorităţile competente, dar şi când acestea sunt în posesia autorităților competente, considerăm necesară şi stabilirea unor norme referitoare la măsurile de securitate aplicabile în acest caz, similare cu cele de mai sus. Astfel de norme ar putea fi detaliate tot de către autoritatea/autorităţile menţionate mai sus, iar implementarea lor ar urma să fie obligatorie.

c) De asemenea, atragem atenţia asupra faptului că proiectul de lege nu menţionează ce se întâmplă cu datele puse la dispoziţia autorităţilor competente, în ce condiţii aceste date sunt stocate (în vederea asigurării securităţii) şi ce se întâmplă cu ele după ce au servit scopului pentru care au fost solicitate furnizorilor (dacă sunt şterse sau dacă sunt arhivate şi în ce condiţii). Astfel de prevederi existau în Legea nr.298/2008, dar au fost eliminate din noul proiect de lege şi considerăm necesară reintroducerea lor.

3. Accesul la datele reţinute

În decizia Curţii Constituţionale se menţionează că *"garanţiile legale privind utilizarea în concret a datelor reţinute - referitoare la excluderea conţinutului ca obiect al stocării datelor, la autorizarea motivată şi prealabilă a preşedintelui instanţei competente să judece fapta pentru care s-a început urmărirea penală – nu sunt suficiente şi adecvate, astfel încât să îndepărteze teama că drepturile personale, de natură intimă, nu sunt violate, astfel încât manifestarea acestora să aibă loc într-o manieră acceptabilă"*.

Observăm că proiectul de lege nu doar că nu conţine soluţii pentru problemele semnalate, dar agravează situaţia prin eliminarea parţială a garanţiilor (chiar dacă insuficiente) oferite prin legea abrogată. Astfel, prevederile din art.16 din Legea nr.298/2008 referitoare la procedurile de solicitare, de către autorităţile competente, a transmiterii de date reţinute şi de emitere a autorizaţiei de solicitare a datelor reţinute nu mai apar în noul proiect de lege, fiind înlocuite cu o prevedere vagă (alin.1 al art.6), conform căreia furnizorii sunt obligaţi să transmită datele reţinute potrivit legii "la solicitarea organelor judiciare sau a organelor cu atribuţii de siguranţă şi securitate naţională, în baza autorizaţiilor emise potrivit legii […] fiind aplicabile dispoziţiile din Codul de procedură penală şi cele din legile speciale în materie." Nu se specifică, însă, care sunt aceste dispoziţii (dacă ele există) şi legi care ar urma să se aplice.

Menţionăm că varianta în vigoare a Codului de Procedură Penală nu conţine prevederi clare referitoare la procedurile aferente accesării datelor de trafic şi de localizare a persoanelor fizice şi juridice reţinute de către furnizorii de reţele publice de comunicaţii şi furnizori de servicii de comunicaţii electronice destinate publicului.

În aceste condiţii, şi pentru a răspunde observaţiilor formulate de către Curtea Constituţională, care consideră că *„reglementarea cât mai exactă a domeniului de aplicare a legii [...] este cu atât mai necesară, având în vedere, în special, natura complexă a drepturilor supuse limitării, precum şi consecinţele pe care un eventual abuz al autorităţilor publice le-ar putea avea asupra vieţii intime a destinatarilor săi, astfel cum aceasta este percepută la nivelul subiectiv al fiecărui individ"*, propunem introducerea unor prevederi care să reglementeze următoarele aspecte:

- *acces la date* - accesul la datele reţinute să fie posibil doar în cazul în care există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni grave, aşa cum acestea este definită la lit.f), alin.(1) al art.2, iar măsura să fie proporţională cu restrângerea drepturilor şi libertăţilor fundamentale (a se vedea, în acest sens, alin.1 al art.139 din Codul de Procedură Penală);

- *stabilirea cu exactitate a procedurii* aferente emiterii autorizaţiei în baza căreia se autorităţile competente pot solicita accesul la datele reţinute. În acest scop pot fi avute în vedere prevederile fostului art.16 din Legea nr.298/2008.

- *transparenţă* - informarea persoanelor vizate în legătură cu accesarea şi utilizarea, de către autorităţile competente, a datelor reţinute. Accesarea şi utilizarea datelor reţinute fără informarea persoanei vizate ar urma să fie posibilă doar în cazul în care o astfel de notificare ar aduce atingere scopului investigaţiei (ar putea fi cazul investigaţiilor desfăşurate de către organele de stat cu atribuţii în domeniul siguranţei şi securităţii naţionale). În cazul investigaţiilor de natură penală, accesarea şi utilizarea datelor reţinute fără informarea persoanei vizate ar urma să fie posibilă doar în baza unei autorizaţii în acest sens din partea unui organ judiciar competent. În aceste cazuri, ar trebui introdusă obligaţia notificării ulterioare (la finalizarea investigaţiei) a persoanei vizate.

Totodată, având în vedere necesitatea introducerii de garanţii referitoare la protecţia persoanelor în ceea ce priveşte accesarea datelor reţinute de către furnizori, considerăm necesară reintroducerea, în cuprinsul proiectului de lege, a prevederilor existente în cuprinsul alin.(1) al art.19 din Legea nr.298/2008: "orice accesare intenţionată sau transfer al datelor păstrate în conformitate cu prezenta lege, fără autorizare, constituie infracţiune şi se pedepseşte cu închisoare de la un an la 5 ani".

4. Distrugerea datelor reţinute, la sfârşitul perioadei de reţinere

Alin.(3) al art.12 din proiectul de lege prevede că, „la sfârşitul perioadei de reţinere, toate datele reţinute exlusiv în temeiul prezente legi, cu excepţia datelor conservate conform legii, puse la dispoziţia autorităţilor competente, potrivit legii, trebuie să fie distruse prin proceduri automatizate, ireversibil."

Considerăm că, din moment ce anumite date au fost puse la dispoziţia autorităţilor competente, aflându-se, deci, în posesia acestora, ele pot fi şterse, la finalul perioadei de reţinere, de către furnizorii de servicii reţele publice de comunicaţii electronice şi furnizorii de servicii de comunicaţii electronice destinate publicului.

5. Terminologia utilizată

Referitor la terminologia utilizată în cuprinsul proiectului de lege, atragem atenţia asupra următoarelor aspecte:

- La art.1 alin.(1) se foloseşte sintagma „organe de stat cu atribuţii în domeniul siguranţei naţionale", în timp ce la art.16 alin.(1) apare sintagma „organe cu atribuţii de siguranţă şi securitate naţională".

Această formulare a fost criticată de ApTI încă de la prima variantă de proiect din 2007[6] şi ne păstrăm opinia cu privire la "*textul lacunar în ceea ce priveşte situatia similară în care accesul este facut de "organele abilitate prin legile care reglementează activitatea de realizare a securităţii naţionale" fără nici o precizare suplimentară în acest sens. Credem ca se impune o explicitare a acestora şi a situaţiilor precise în care există acces la aceste date, ca şi un control judiciar al acestui tip de acces la datele referitoare la traficul informational".*

De altfel şi Curtea Connstituțională a constatat același aspect cu privire la art. 20 (*"aceeaşi manieră ambiguă de redactare, neconformă cu normele de tehnică legislativă, în ceea ce priveşte dispoziţiile art.20 din Legea nr.298/2008"*).

Pentru evitarea confuziilor în interpretarea prevederilor prezentului proiect de lege, este necesară convenirea folosirii unei singure sintagme care să desemneze autorităţile din domeniul siguranţei şi securităţii naţionale și explicitarea clară a acestora, ca și a "legilor speciale în materie" la care se face referire.

- Deşi în titlul proiectului se foloseşte sintagma „furnizori de servicii de comunicaţii electronice destinate publicului sau de reţele publice de comunicaţii", în textul proiectului apar sintagmele „furnizori de servicii şi reţele publice de comunicaţii electronice" şi „furnizori de reţele publice de comunicaţii şi furnizori de servicii de comunicaţii electronice destinate publicului". Având în vedere faptul că legea ar urma să se aplice atât furnizorilor de servicii cât şi furnizorilor de reţele, precum şi faptul că în legislaţia în vigoare în domeniul comunicaţiilor electronice se foloseşte sintagma „furnizori de reţele publice de comunicaţii şi furnizori de servicii de comunicaţii electronice destinate publicului" (a se vedea, spre exemplu, Legea nr.304/2003 pentru serviciul universal şi drepturile utilizatorilor cu privire la reţelele şi serviciile de comunicaţii electronice, republicată), propunem utilizarea pe întreg parcursul legii a acestei sintagme.

Semnatari:

ActiveWatch – Agenţia de Monitorizare a Presei

Asociaţia pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki (APADOR-CH)

Asociaţia pentru Tehnologie şi Internet (APTI)

Centrul pentru Jurnalism Independent (CJI)

Bucureşti
3 august 2011

[6] Text integral disponibil la http://apti.ro/sites/default/files/20070509_opinie_APTI_legedatetrafic.pdf