Către CURTEA CONSTITUȚIONALĂ A ROMÂNIEI
CABINETUL PREȘEDINTELUI

Calea 13 Septembrie nr. 2, Intrarea B1, sectorul 5, București, România

Referitor la Dosarul nr. 1419AI/2014 cu termen de judecată 21 ianuarie 2015

Amicus curiae

Argumente în susținerea obiecției de neconstituționalitate ridicată de către Grupul Parlamentar al Partidului Național Liberal cu privire la dispozițiile Legii 580/2014 privind securitatea cibernetică a României

Formulat de Asociația pentru Tehnologie şi Internet (ApTI) și Asociația pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki - APADOR-CH

Susținut de
Mircea Toma, Președinte, ActiveWatch
Ștefan Cândea, Centrul Român pentru Jurnalism de Investigație
Mihail Bumbeș, Președinte, Asociația Miliția Spirituală
Laura Ștefan, Expert anticorupție, Expert Forum
Violeta Alexandru, Director, Institutul pentru Politici Publice
Tiberiu-Constantin Turbureanu, Președinte, Fundația Ceata
Gabriel Petrescu, Director executiv, Fundația pentru o societate deschisă
Claudiu Marginean, Președinte, Asociatia Copyratul Roman
Vasile Crăciunescu, Președinte, Asociatia Geo-Spatial.org
Elena Calistru, Președinte, Asociația Funky Citizens
Oana Preda, Director Executiv CeRe, Centrul de Resurse pentru Participare Publică

I. Preambul

Organizațiile semnatare cunosc faptul că, din punct de vedere procedural, nu au calitatea de intervenient (parte) în acest contencios constituțional.

Tocmai de aceea, ele depun prezentul *amicus curiae*, instituție juridică distinctă de cea a intervenției și care este recunoscută ca atare de instanțele din sistemele de drept de tip *common law*, spre exemplu, de Curtea Europeană a Drepturilor Omului.

Prin *amicus curiae* este permis celor care au o expertiză într-un anumit domeniu (în speță, respectarea drepturilor omului, libertatea de asociere) să ajute instanța, ca „*prieteni ai instanței*" (amicii curiae), prin furnizarea, cu rol consultativ, de informații/observații relevante pentru soluționarea unei cauze importante.

Precizăm că, recent, calitatea de *amicus curiae* a unei organizații neguvernamentale a fost recunoscută explicit de Curtea Constituțională în cuprinsul Deciziei nr. 447 din 29 octombrie 2013 referitoare la excepția de neconstituționalitate a dispozițiilor Ordonanței de urgență a Guvernului nr. 91/2013 privind procedurile de prevenire a insolvenței și de insolvență.

II. **Neconstituționalitatea legii**

Articolele 2, 3, 16, 17 din **Legii 580/2014 privind securitatea cibernetică a României** („legea criticată") sunt neconstituționale, întrucât încalcă următoarele articole din Constituție:

- art. 26 privind viața intimă, familială și privată;
- art. 27 privind inviolabilitatea domiciliului;
- art. 28 privind secretul corespondenței;
- art. 1 alin (3) privind libera dezvoltare a personalității umane și demnitatea omului;
- art. 1 alin (4) privind principiului separaţiei şi echilibrului puterilor;
- art. 45 privind libertatea economică;
- art. 53 alin (2) privind restrângerea unor drepturi sau libertăți.

De asemenea, în temeiul art. 148 alin. (2) și alin. (4) din Constituție, prevederile criticate reprezintă o încălcare a dreptului la viață privată și la protecția datelor cu caracter personal care sunt protejate de Curtea Europeană a Drepturilor Omului (CEDO) în temeiul art. 8 din Convenția Europene a Drepturilor Omului și de Curtea de Justiție a Uniunii Europene (CJUE), pe baza dreptului Uniunii Europene și a Cartei Drepturilor Fundamentale a Uniunii Europene.

În primul rând, măsurile adoptate de legiuitor prin dispozițiile criticate reprezintă o atingere adusă dreptului la viață privată, așa cum este el ocrotit de art. 26 al Constituției.

În condițiile deja precizate de Curtea Constituțională a României (CCR) în deciziile 1258/2009, 440/2014 și 461/2014, accesul la datele informatice (care pot fi și date de trafic - *vezi explicații*

detaliate la pct. III.2 de mai jos) se poate face doar cu autorizarea sau aprobarea instanței judecătorești.

Solicitările de acces la datele reținute în vederea utilizării lor în scopul prevăzut de lege, formulate de către organele de stat cu atribuții în domeniul securității naționale, nu sunt supuse autorizării sau aprobării instanței judecătorești, lipsind astfel garanția unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date. (par. 63, Decizia CCR 440/2013)

Astfel, articolul 17(1) din legea criticată, prin care nouă instituții publice au acces, fără autorizarea unui judecător, la orice date informatice, nu îndeplinește criteriul apărării efective a dreptului la protecția vieții private. Astfel o parte din cele nouă instituții publice nu au nicio urmă de competență în domeniul securității informatice (cum ar fi SPP sau ORNISS), iar acordarea acestui drept tuturor acestor instituții în condiții similare și vagi ne demonstrează lipsa de predictibilitate a legii.

„Este unanim recunoscut în jurisprudența Curții Europene a Drepturilor Omului, de exemplu în cauza Prințul Hans-Adam II de Liechtenstein împotriva Germaniei, din anul 2001, că statele membre semnatare ale Convenției pentru apărarea drepturilor omului și a libertăților fundamentale și-au asumat obligații de natură să asigure că drepturile garantate de Convenție sunt concrete și efective, nu teoretice și iluzorii, măsurile legislative adoptate urmărind apărarea efectivă a drepturilor". (Decizia CCR 1258/2009)

Conform CJUE în hotărârea Digital Rights Ireland (C 293-12), o reglementare care atinge dreptul la protecția datelor cu caracter personal așa cum este prevăzut în art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene, *„trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime astfel încât persoanele ale căror date au fost păstrate să dispună de garanții suficiente care să permită protejarea în mod eficient a datelor lor cu caracter personal împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date"*.

De altfel și CCR în Decizia nr. 1258/2009 precizează că *„în materia drepturilor personale cum sunt dreptul la viață intimă și libertatea de exprimare, precum și a prelucrării datelor cu caracter personal, regula unanim recunoscută este aceea a garantării și respectării acestora, respectiv a confidențialității, statul având, în acest sens, obligații majoritar negative, de abținere, prin care să fie evitată, pe cât posibil, ingerința sa în exercițiul dreptului sau a libertății"*.

Este necesar să atragem atenția asupra faptului că raționamentul CJUE în hotărârea Digital Rights Ireland, se aplică și măsurilor și politicilor adoptate în ceea ce privește siguranța națională. Așadar, testul de proporționalitate trebuie efectuat nu numai atunci când este vorba de măsuri și programe de supraveghere, dar și atunci când, în numele siguranței naționale, se adoptă măsuri ce reprezintă intruziuni în viața privată.

În acest sens, întreaga lege criticată nu stabilește o modalitate de prevenire a riscurilor de abuz. Mai mult, lipsa elementelor operaționale și a măsurilor de siguranță privind prelucrarea, păstrarea și distribuirea datelor solicitate determină un risc ridicat pentru accesul neautorizat și pentru utilizarea ilicită a datelor. În ceea ce privește distribuirea datelor, trebuie să subliniem că prevederile Legii 677/2001 în ceea ce privește transferul de date, inclusiv transferul internațional de date, sunt pe deplin aplicabile.

În al doilea rând, dispozițiile art. 17 (1) din lege încalcă art. 27 din Constituția României privind inviolabilitatea domiciliului.

Sistemul informatic deținut de o persoană (calculatorul etc.) adaugă la spațiul fizic personalizat (domiciliul) un spațiu virtual personalizat (domiciliul informatic/virtual) care prezintă caracteristici similare domiciliului unei persoane și care trebuie asimilat din punct de vedere al protecției legale domiciliului persoanei. „Ușa" domiciliului informatic/virtual este încuiată cu o cheie specifică, reprezentată de numele de utilizator și de parolă (sau alte metode similare).

De aceea, singura modalitate constituțională de a intra și căuta într-un sistem informatic nu poate fi decât cea pentru intrarea și căutarea într-un domiciliu fizic, adică existența unei autorizații de la judecător. De altfel, noul Cod de procedură penală (și, înainte de acesta, Legea 161/2003) prevede că și percheziția informatică necesită autorizație judecătorească.

De aceeași protecție trebuie să beneficieze nu numai persoanele fizice, ci și persoanele juridice, al căror sediu trebuie protejat ca și domiciliul persoanelor fizice.

Mai mult, în cazul persoanelor juridice (firmelor) furnizoare de servicii internet, prin intrarea și căutarea în sistemele informatice (servere etc.) pe care le dețin sunt accesate și datele privind activitatea abonaților în spațiul virtual. Astfel, se realizează, pe cale ocolită, o percheziție neautorizată de judecător în spațiul virtual al persoanei, spațiu la fel de important ca și spațiul fizic reprezentat de domiciliu.

În al treilea rând, textul adoptat este extrem de vag și creează un context legal incert, discriminatoriu și neconstituțional prin adoptarea de norme aplicabile direct tuturor persoanelor juridice și indirect persoanelor fizice, încălcând astfel articolele din Constituția României precizate în primul paragraf al acestui capitol și în special articolul 45 privind libertatea economică.

În acest sens o persoană juridică nu poate să identifice în mod precis dacă este sau nu un subiect al legii, care sunt obligațiile sale concrete în urma legii, ce anume trebuie să raporteze și către cine.

În ceea ce privește art. 3 din legea criticată, atragem atenția că **doar o parte din siguranța cibernetică reprezintă o componentă a securității naționale**. În alte cuvinte, nu tot ce ține de siguranța cibernetică afectează apărarea și siguranța națională. Așadar, este neproporțional faptul că legea dorește să se aplice tuturor deținătorilor de infrastructuri cibernetice.

De asemenea, raportarea incidentelor de securitate către instituții din domeniul securității statului, ridică probleme de încredere cu privire la utilizarea acestor informații (unele din ele date personale) exclusiv în interesul asigurării securității informatice și nu în alte scopuri, atâta vreme cât nu există o transparență instituțională cu privire la activitățile acesteia.

Precizăm că Uniunea Europeană are deja o propunere de directivă cu privire la subiectul securității informatice, cunoscută ca Directiva NIS (Network & Information Security). Parlamentul European a adoptat această directivă în primă lectură pe 13 martie 2014[1], dar procesul legislativ nu este încă încheiat la nivelul Uniunii Europene.

Cu toate acestea câteva soluții din această directivă pentru un act normativ util au fost propuse de către societatea civilă legiuitorilor români, însă acestea au fost pur și simplu ignorate.

Astfel, directiva europeană:

- identifică categoriile exacte de societăți comerciale (Anexa II) care au infrastructuri critice și doar lor li se aplică obligațiile din directivă;
- impune necesitatea de a avea o autoritate de control din domeniul **civil**, pentru a putea să colaboreze cu instituțiile private pe subiectul securității informației

  Considerentul (10): Autoritățile competente și punctele unice de contact ar trebui să fie organisme civile, sub completă supraveghere democratică și nu ar trebui să îndeplinească nici un fel de rol de serviciu de informații, de aplicare a legii sau de apărare sau să aibă legături organizaționale de orice fel cu organizații active în aceste domenii;
- impune obligații realiste pentru a raporta doar anumite incidente care afectează un număr finit de utilizatori, are o întindere geografică deosebită sau aduce o atingere deosebită datelor personale.

III. Explicații cu privire la noțiunile tehnice

În plus față de argumentele juridice aduse, credem că sunt necesare câteva explicații tehnice de bază pentru a înțelege textul legii și implicațiile sale. Textul actual este extrem de larg și vag, ceea ce duce la o lege cu un **context legal incert, discriminatoriu și neconstituțional**:

1. **„persoanelor juridice de drept public sau privat, care au calitatea de proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetice" (art. 2)**

În condițiile definiției extrem de largi a **infrastructurii cibernetice** (din art. 5 g) spectrul celor cărora li se aplică legea ar fi practic toate persoanele juridice din România. Pentru că toate persoanele juridice au probabil calitatea de **proprietari, administratori, operatori sau utilizatori** ai unor sisteme informatice (ca de exemplu: calculator, laptop, tabletă, telefon, casă

[1] Textul adoptat neconsolidat este disponibil pe site-ul Parlamentului European http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//RO

de marcat fiscală, ceas inteligent, TV inteligent, pompă de benzină cu procesor, contor de electricitate inteligent etc.), a unei aplicații aferente sistemelor informatice (practic orice program informatic de pe aceste dispozitive) sau a unei rețele sau servicii de comunicații electronice (furnizori de telefonie fixă și mobilă, Internet).

Termenii de **proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetice** ridică și alte probleme de interpretare practică deosebit de delicate în contextul virtualizării utilizării de sisteme și aplicații informatice (cunoscut în lumea IT sub termenul *cloud computing*), unde teritoriul unde se află datele sau cine administrează serviciul este mai complicat decât de obicei.

Dar cea mai mare problemă din punct de vedere al drepturilor constituționale este faptul că aproape toate datele informatice ale tuturor persoanelor fizice sunt administrate de aceste persoane juridice mai sus amintite. Astfel, datele includ:

- Toate datele cu privire la traficul de Internet se află în mâinile furnizorilor de servicii Internet;
- Toate datele cu privire la corespondența electronică se află pe serverele unor firme private (de ex. Google, Yahoo - administrează cam 90% din adresele de email private din România);
- Toate datele cu privire la navigarea pe Internet se află în mâinile furnizorilor de servicii ale societății informaționale (de ex. magazine online, procesatori de plăți, proprietari de site-uri web, proprietari de aplicații de pe telefoane, furnizori de publicitate online).

2. **Date informatice**

Art. 17. (1) Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au următoarele responsabilități:

*a. Să acorde sprijinul necesar (...) şi **să permită accesul** reprezentanţilor desemnaţi în acest scop **la datele deţinute,** relevante în contextul solicitării.*

Terminologia articolului 17 (1) ne indică că se vorbește de orice date deținute de către persoanele juridice de la art. 2. În mod logic este vorba despre date informatice, care sunt definite de Codul de procedură penală:

*Art. 138 (5) Prin **date informatice** se înțelege orice reprezentare de fapte, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic.*

SRI a intervenit (deși nu are nicio competența de interpretare normativă) după adoptarea legii[2] pentru a "explica" termenul de "date". Însă conform principiul *Ubi lex non distinguit, nec nos*

[2] Vezi comunicat SRI din 18.01.2015 disponibil la adresa http://www.sri.ro/cu-privire-la-dezbaterea-publica-pe-marginea-prevederilor-legii-securitatii-cibernetice-sri-face-urmatoarele-precizari.html

distinguere debemus[3] nediferențierea tipurilor de date la care se referă legea ne determină să considerăm că în lege este vorba de toate tipurile de date informatice posibile, deci inclusiv:

- **Date cu privire la conținutul comunicației** (de ex. ce a spus Ion Popescu într-un email);
- **Date de trafic ale furnizorilor de comunicații electronice,** (de ex. la ce ora a trimis Ion Popescu un email) situație deja considerată în Curtea Constituțională în deciziile 1258/2009 și 440/2014;
- **Date tehnice (care pot fi și date de trafic) ale unor alți furnizori, dar care pot fi și date personale** (de ex. adresa de IP sau de email a unui abonat la un serviciu online);
- **Date tehnice ale unor furnizori care nu sunt date personale** (de ex. data și ora la care un site web a fost infectat sau lacuna de securitate folosită la un atac).

Nediferențierea cel puțin între aceste tipuri de date face textul legii criticate extrem de vag. De altfel nici măcar comunicatul SRI mai sus menționat nu reușește să distingă în exemplul dat de ei între date personale (adresa de IP) și date pur tehnice.

3. Acces la date informatice

Cei care au propus legea nu au cerut ca subiecții legii să dea aceste date informatice către organele abilitate (*ceea ce ar fi mult mai puțin intruziv*), ci ca să permită „accesul (...) la datele deținute". Datele informatice pot fi stocate în sisteme informatice sau în mijloace de stocare a datelor informatice (de ex. stick de memorie, DVD, hard-disk extern etc.).

Deși înțelegem raționamentul tehnic *(legat probabil de volatilizarea datelor în format digital sau alterarea lor dacă ele nu sunt colectate în mod corect*), accesul direct la date ridică probleme deosebite în contextul în care el nu este făcut în condițiile garantării faptului că, de exemplu:

- accesul se face doar la datele dorite și nu la altele stocate în același loc;
- accesul se face urmând proceduri specifice tehnice de acces la date, care asigură posibilitatea re-expertizării datelor informatice în condiții identice, pentru eventualitatea unei alte expertize dispuse de o instanță de judecată;
- accesul nu alterează sistemul informatic sau servicii informatice oferite.

Mai mult, din cuprinsul art. 138 din Codul de Procedură Penală înțelegem accesul la date drept o metodă specială de supraveghere sau cercetare, care este reglementată strict în condițiile procedurii penale. În acest sens avem definiția din alin (3):

*Prin **acces la un sistem informatic** se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe.*

[3] Unde legea nu distinge, nici noi nu trebuie să distingem

4. Incident cibernetic.

incident cibernetic - eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică;

Un program de calculator de detectare a incidentelor cibernetice pentru un sistem informatic obișnuit raportează aproximativ 1000 de incidente de securitate pe zi (multe dintre ele puțin relevante pentru publicul larg). În condițiile definiției de mai sus și a lipsei unor limitări logice stabilite în lege, toate aceste incidente ar trebui raportate în condițiile art. 17 (1) b).

Lipsa clarității tuturor acestor termeni, ca și a altora pe care nu i-am abordat aici din dorința de a fi exemplificativi și nu exhaustivi, duce la o lege a cărei interpretare este extrem de largă și cu o sferă de aplicare imprecisă, vagă și extrem de greu de identificat pentru subiecții acesteia.

IV. Concluzie

Subiectul securității informatice este unul complex și important pentru toți utilizatorii de sisteme informatice. Și dacă adăugăm natura globală a Internetului, putem realiza și elementul trans-național al problemei. Dar el trebuie să se bazeze întâi pe o cultură a colaborării și a educației în domeniul securității informației, care să plece de la premisa asigurării securității datelor personale ale cetățenilor și nu pe dispoziții legale neconstituționale.

Așa cum am demonstrat, dispozițiile Legii securității cibernetice sunt neconstituționale, raportate la art. 26, 27, 28 art. 1 alin. (3), (4), art. 45 și art. 53 alin. (2) din Constituție, precum și, în temeiul art. 148 alin. (2) și alin. (4), raportate la art. 8 din Convenția Europeană a Drepturilor Omului.

Pentru semnatari,

Bogdan Manolea
Director executiv
Asociația pentru Tehnologie și Internet

Maria-Nicoleta Andreescu
Director executiv
APADOR-CH

București, 19 ianuarie 2015