



Nr. 228 din 15 septembrie 2014

**Către CURTEA CONSTITUȚIONALĂ a ROMÂNIEI  
CABINETUL PREȘEDINTELUI**

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

**Referitor la Dosarul nr.695A/2014 cu termen de judecată 16 septembrie 2014**

**Amicus curiae**

**Argumente în susținerea obiecției de neconstituționalitate ridicată de instituția Avocatul  
Poporului cu privire la dispozițiile Legii pentru modificarea Ordonanței de Urgență a  
Guvernului nr.111/2011 privind comunicațiile electronice**

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

**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.

În acest sens, la fila 5 a deciziei amintite se menționează: “*La dosarul cauzei a fost depusă din partea Asociației pentru Apărarea Drepturilor Omului în România — Comitetul Helsinki, în calitate de amicus curiae, o opinie în sprijinul excepției de neconstituționalitate a*

*dispozițiilor art.81 alin.(3) și ale art.348 din Ordonanța de urgență a Guvernului nr.91/2013.”*

## **II. Argumente de neconstituționalitate ale Legii Criticate**

Punctele 1, 2, 3, 4, și 5 ale art.I din legea criticată sunt neconstituționale, întrucât încalcă art. 26 din Constituție privind viața intimă, familială și privată, art.28 – privind secretul corespondenței, art. 1 alin. (3) din Constituție privind libera dezvoltare a personalității umane și demnitatea omului, și art. 53 alin. (2) din Constituție 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 de Justiție a Uniunii Europene (CJUE), pe baza dreptului Uniunii Europene, și de Curtea Europeană a Drepturilor Omului (CEDO) în temeiul art. 8 al Convenției cu același nume.

**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.**

Măsurile adoptate de legiuitor stabilesc, pe de o parte, faptul că achiziționarea serviciilor de comunicații electronice pentru care plata se face în avans (cartele SIM pre-plătite) este condiționată de furnizarea de către utilizator a datelor personale de identificare cu scopul ca acestea să fie stocate fie în format electronic, fie în format fizic; pe de altă parte, măsurile stabilesc obligația ca, în cazul punctelor de conectare la internet puse gratuit la dispoziția publicului de către persoane juridice (rețele Wi-Fi), utilizatorii conectați în aceste puncte să fie identificați ("*Utilizatorii acestor puncte au obligația de a-și comunica datele de identificare la accesarea acestor servicii*" - Art. I punctul 4).

Colectarea și stocarea datelor de identificare ale persoanei (*definite de art. I, punctul 1 ca fiind "numărul de telefon", "numele, prenumele și codul numeric personal, seria și numărul documentului de identitate"*), ca și lipsa oricărei informații sau garanții cu privire la cine ar avea acces la aceste date și în ce condiții reprezintă o ingerință în dreptul la viață privată.

În conformitate cu jurisprudența CJUE trebuie precizat că "Pentru a stabili existența unei ingerințe în dreptul fundamental la respectarea vieții private, are puțină relevanță dacă informațiile vizate referitoare la viața privată prezintă sau nu prezintă un caracter sensibil sau dacă persoanele interesate au suferit sau nu au suferit eventuale dezavantaje ca urmare a acestei ingerințe"<sup>1</sup>.

De asemenea, Curtea Constituțională a României a reținut în Decizia nr. 1258/2009 și că "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". Posibilitatea conferită de dispozițiile legale criticate, ca un număr nelimitat de persoane juridice de drept privat și drept public să aibă acces la datele de identificare ale utilizatorilor de cartele pre-plătite, pe care apoi să le stocheze în condiții

---

<sup>1</sup> Hotărârea CJUE din 8 aprilie 2014 în cauzele conexe C-293-12 și C-594-12 *Digital Rights Ireland*, punctul 33.

nedefinite de lege și, deci, în afara unui sistem de garanții de securitate a datelor personale, nu îndeplinește criteriul apărării efective a dreptului la protecția vieții private.

În acest sens, Curtea de Justiție a Uniunii Europene a subliniat în cauza *Digital Rights Ireland* faptul că "protecția datelor cu caracter personal, care rezultă din obligația explicită prevăzută la art. 8 alin. (1) din Cartă, prezintă o importanță deosebită pentru dreptul la respectarea vieții private"<sup>2</sup>. Pe de altă parte, Curtea Constituțională a României a reținut în Decizia nr. 1258/2009 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".

Conform CJUE, o reglementare care atinge dreptul la protecția datelor cu caracter personal așa cum este prevăzut în art. 8 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**"<sup>3</sup>.

În cazul de față înregistrarea tuturor cartelelor SIM pre-plătite și identificarea tuturor utilizatorilor de rețele Wi-Fi gratuite împiedică utilizarea anonimă a comunicațiilor electronice și constituie o bază pentru extinderea supravegherii generalizate.

**În al doilea rând, notăm faptul că orice ingerință în exercițiul unui drept, deci și al dreptului la viață privată, pentru a fi considerată de către CEDO conformă cu Convenția europeană, trebuie să îndeplinească, cumulativ, următoarele:**

- ingerința trebuie să fie prevăzută de lege;
- ingerința trebuie să urmărească un scop legitim;
- ingerința trebuie să fie necesară într-o societate democratică.
- ingerința trebuie să fie proporțională cu scopul urmărit.

Condiționalități similare se regăsesc și în art. 53 alin. (2) din Constituția României.

CEDO a statuat pericolul pe care o lege care permite supravegherea secretă îl reprezintă la adresa democrației sub pretextul apărării ei, afirmând că "statele contractante nu pot, în numele luptei împotriva terorismului și spionajului, să adopte orice măsuri pe care acestea le consideră necesare"<sup>4</sup>.

---

<sup>2</sup> Idem, punctul 48.

<sup>3</sup> Idem, punctul 54.

<sup>4</sup> CEDO: *Klass și alții/Republica Federală Germania*, Curtea Europeană a Drepturilor Omului, 6 septembrie 1978 (seria A, nr. 28)

**O să prezentăm pe parcursul acestui *amicus curiae* faptul că legea criticată nu respectă niciunul dintre cele patru principii ce ar trebui să fie îndeplinite cumulativ pentru a se considera că încălcarea dreptului la viață privată este legitimă.**

## **1. Temei juridic**

Orice ingerință în dreptul la viață privată trebuie să fie legală, adică trebuie să fie "*prevăzută de lege*".

Aceasta înseamnă, printre altele, că legea trebuie să fie de o anumită calitate. În acest sens, Curtea Europeană a Drepturilor Omului a dezvoltat două cerințe principale. Legea care limitează dreptul la viață privată trebuie să fie suficient de clară, precisă și previzibilă, și în plus să fie accesibilă.

Claritatea, precizia și previzibilitatea legii înseamnă că legea trebuie să fie "*formulată cu destulă precizie pentru a permite unui cetățean să decidă conduita sa și să prevadă, în mod rezonabil, în funcție de circumstanțele cauzei, consecințele care ar putea rezulta dintr-un fapt determinat.*"<sup>5</sup>.

În contextul special de interceptare a comunicațiilor în scopul anchetelor poliției, CEDO notează că "*legea trebuie să fie suficient de clară în ceea ce privește posibilitatea de a da cetățenilor, în general, o indicație corespunzătoare cu privire la împrejurările și condițiile în care autoritățile publice sunt împuternicite să recurgă la această intervenție secretă și potențial periculoasă asupra respectării vieții private și a corespondenței*"<sup>6</sup>.

Mai mult, CEDO consideră că "dreptul material în sine, spre deosebire de însoțirea practică administrativă, **trebuie să indice domeniul de aplicare și modalitățile de exercitare a acestei puteri discreționare cu suficientă claritate, având în vedere scopul legitim a măsurii în cauză**, pentru a oferi individului o protecție adecvată împotriva arbitrariului"<sup>7</sup>.

În cazul de față, legea românească nu este în conformitate cu principiul temeiului juridic. Într-adevăr:

- Legea nu este propriu-zis despre supravegherea cetățenilor, dar constituie baza care permite o astfel de supraveghere. Ea nu se referă la anumite persoane care ar putea fi autorii unei infracțiuni, ci se referă la fiecare persoană care dorește să acceseze rețeaua de telefonie mobilă sau rețeaua de Internet prin intermediul unui Wi-Fi gratuit.
- În consecință, pentru a permite cetățeanului să își "*adapteze conduita sa în consecință*" și pentru a "*oferi individului o protecție adecvată împotriva ingerinței arbitrare*", legea trebuie să dea "un indiciu adecvat cu privire la împrejurările și condițiile în care autoritățile publice sunt împuternicite să recurgă la această intervenție secretă", și **trebuie să indice domeniul de aplicare și modalitățile de exercitare a acestei puteri discreționare cu suficientă claritate, având în vedere scopul legitim al măsurii în cauză**.
- În cazul nostru specific, observăm că scopurile legii nu sunt indicate. Legea nu menționează nimic în această privință. Numai în expunerea de motive se menționează

<sup>5</sup> Vezi CEDO - *Sunday Times vs. Marea Britanie*, 26 April 1979, Series A no. 30, p. 31, § 49,

<sup>6</sup> Vezi CEDO - *Malone vs. Marea Britanie* citată în Council of Europe, *Case law of the European court of Human rights concerning the protection of personal data*, 30 Jan. 2013 (DP (2013) CASE LAW), op. cit., p. 19

<sup>7</sup> Idem

doă încercări de justificare, care nu pot fi considerate "scopuri" în accepțiunea CEDO (a se vedea al doilea punct de mai jos).

O primă justificare menționată este "discriminarea între consumatori", deoarece lista de utilizatori de cartele preplătite nu este disponibilă on-line. Cu toate acestea, nici detaliile de informare cu privire la utilizatorii înregistrați printr-un abonament nu sunt disponibile, deoarece prezența în listă este o opțiune, și nu o obligație, în conformitate cu Legea 506/2004. Mai mult, noua lege (legea criticată) nu prevede posibilitatea, pentru utilizatorii de cartele preplătite, să fie incluși pe această listă. În plus, această justificare nu explică de ce utilizatorii de Wi-Fi gratuit ar trebui să se înregistreze. În cele din urmă, un anumit consumator are pe deplin dreptul de a avea și un abonament la telefon și / sau conexiune la Internet, și, în plus, să aibă și o cartelă preplătită pentru a folosi un Wi-Fi public gratuit. Prin urmare, justificarea de non-discriminare nu este relevantă în contextul demonstrat.

A doua justificare este că "este dificil de a identifica utilizatorii prepaid, în cazul activităților realizate de aplicare a legii penale sau pentru cunoașterea, prevenirea și riscurile de securitate națională și amenințări teroriste". În primul rând, expunerea de motive nu explică faptul că o astfel de identificare este imposibilă. Activități curente din cadrul poliției sau desfășurate de către procurori duc la identificarea infractorilor, chiar în cazul utilizărilor de multiple cartele preplătite. În al doilea rând, "activitățile legate de aplicarea legii" sunt mult prea vagi pentru a reprezenta un scop acceptabil. Prevenirea riscurilor de securitate națională ar putea fi privită ca un scop legitim dacă ar fi explicită în detaliu, dar oricum măsurile de prevenire, garanțiile și implicațiile acestora trebuie descrise în detaliu în textul legii, nu numai în expunerea de motive. Încă o dată, utilizatorii de Wi-Fi gratuit nu sunt menționați, prin urmare, măsura referitoare la aceștia nu se justifică. De asemenea, este neclar cum vor fi folosite aceste date colectate – în contextul activităților propuse – câtă vreme nu există nici un indiciu cu privire la instituțiile care vor putea avea acces la aceste date și în ce circumstanțe.

## 2. Scop legitim

Articolul 8.2 din Convenția Europeană a Drepturilor Omului prezintă exhaustiv motivele legitime pentru care o ingerință în dreptul la viață privată poate fi legitimă. Aceste obiective sunt interesele de securitate națională, siguranța publică sau bună-starea economică a țării; apărarea ordinii și prevenirea crimei; protejarea sănătății sau a moralei, și protejarea drepturilor și libertăților altora.

Noțiunea de scop legitim este, de asemenea, luată în considerare de către Curtea Europeană a Drepturilor Omului<sup>10</sup>. În plus, Carta Drepturilor Fundamentale a Uniunii Europene solicită ca limitările de viață privată "să răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților altora"<sup>9</sup>.

---

<sup>8</sup> Vezi cazurile raportate în mass-media în ultimii ani - [Apostu \(22 de telefoane cu cartele inter-sanjabile\)](#) – raportata la Stiri.com.ro - 22 de telefoane mobile au fost descoperite acasă și la biroul primarului suspendat al Clujului (30.12.2011) <http://www.stiri.com.ro/stire-18844/22-de-telefoane-mobile-au-fost-descoperite-acasa-si-la-biroul-primarului-suspendat-al-clujului.html> disponibilă și [Fany \(15 cartele folosite\)](#) Stiri de Cluj – "Patronul FANY l-a copiat pe Apostu. A folosit 15 cartele telefonice pentru a nu fi INTERCEPTAT" 28.03.2014 <http://www.stiridecluj.ro/social/patronul-fany-l-a-copiat-pe-apostu-a-folosit-15-cartele-telefonice-pentru-a-nu-fi-interceptat>

<sup>9</sup> Art 52 (1) din Carta – (1) Orice restrângere a exercițiului drepturilor și libertăților recunoscute prin prezenta carte trebuie să fie prevăzută de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți.

Într-adevăr, Recomandarea R (87) 15 a Consiliului Europei<sup>10</sup>, care are scopul de a adapta Convenția privind protecția datelor nr. 108 a Consiliului Europei<sup>11</sup> și principiile CEDO<sup>12</sup> la cerințele specifice sectorului ce privește activitățile polițienești, și limitează scopurile autorizate la "prevenirea unui *pericol real*" și la "*suprimarea unei infracțiuni specifice*". Orice alt scop este permis numai în cazul în care face obiectul unei legislații naționale specifice, ceea ce implică faptul că această legislație specifică scopul și prevede garanții corespunzătoare, așa cum o vom analiza mai târziu.

În plus, Recomandarea 87 (15) prevede că "datele cu caracter personal colectate și stocate de către poliție în scopuri polițienești ar trebui să fie utilizate exclusiv în aceste scopuri", sub rezerva principiilor care reglementează comunicarea de date. Așadar legislația trebuie să interzică în mod explicit orice altă utilizare și să asigure că această interdicție este pusă în aplicare.

### 3. Necesitatea

Acest principiu de "necesitate" a ingerinței **constă în demonstrarea faptului că această interferență este de fapt potrivită pentru a satisface o nevoie socială specifică.**

Într-adevăr, în conformitate cu Curtea Europeană a Drepturilor Omului, orice limitare a vieții private, pentru a fi legitimă, trebuie să fie o necesitate, iar această nevoie trebuie să fie stabilită în mod convingător.<sup>13</sup> Termenul "nevoie" se referă la două tipuri diferite de nevoi: "necesități sociale imperioase" (de exemplu, o problemă socială, care trebuie să fie abordată<sup>14</sup>), și o nevoie de interferență specific propusă (care trebuie să fie adecvată pentru a satisface nevoia socială identificată<sup>15</sup>).

Prin urmare, principiul necesității trebuie să îndeplinească două cerințe:

#### 3.1 Să demonstreze o nevoie socială specifică:

Ingerința trebuie să fie "*necesară având în vedere faptele și circumstanțele în cazul specific*"<sup>16</sup>, care presupune în primul rând **identificarea "necesității sociale specifice care trebuie să fie abordată"**, "*în sfera mai largă a scopului legitim urmărit*", cu scopul de a proteja acest aspect special<sup>17</sup>.

<sup>10</sup> Recomandarea nr. R (87) 15 a Comitetului de Miniștri ai statelor membre ce reglementează utilizarea datelor personale în sectorul polițienesc - versiune în limba română disponibilă la <http://www.dataprotection.ro/servlet/ViewDocument?id=539>

<sup>11</sup> Vezi Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal nr. 108 din 1981 ratificată de România prin Legea nr. 682 din 28 ianuarie 2001

<sup>12</sup> Vezi Memorandumul Explicativ al Recomandării R (87) 15 a Consiliului Europei

<sup>13</sup> Vezi CEDO *Crémieux v. France*, 25 February 1993, Req. n° 11471/85, A256-B, § 38, <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57805>

<sup>14</sup> Vezi Grupul de lucru privind protecția datelor constituit în temeiul Articolului 29 – Avizul 01/2014 privind aplicarea noțiunilor de necesitate și de proporționalitate și protecția datelor în sectorul asigurării respectării legii – 27.02.2014 disponibil la [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211\\_ro.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_ro.pdf)

<sup>15</sup> Op cit fn 14

<sup>16</sup> *The Sunday Times împotriva Regatului Unit, Cererea nr. 6538/74 (CEDO, 6 noiembrie 1980)*

<sup>17</sup> Op cit fn 14

Această necesitate trebuie să fie imperios necesară, cu alte cuvinte, trebuie să aibă un anumit **"nivel superior de gravitate, de urgență sau de efect imediat asociat cu nevoia la care măsura încearcă să răspundă**

". Îi poate fi dăunător societății în cazul în care necesitatea nu este rezolvată, luând în considerare punctele de vedere ale societății și posibile opinii divergente cu privire la acest aspect special de "nevoie"<sup>18</sup>.

Mai mult, existența acestei nevoi severe sau de urgență **trebuie să fie dovedită**. De exemplu, într-un caz în care reclamantul a fost împiedicat să facă anumite declarații referitoare la pericolele supuse de cuptoarele cu microunde, Curtea Europeană a Drepturilor Omului a ajuns la concluzia că *"nu a existat nici o dovadă că vânzarea de cuptoare cu microunde a fost afectată de comentariile reclamantului"*<sup>19</sup>.

În cazul de față, nevoia de ingerință instituită de către noua lege românească nu este stabilită, nici explicată – nici în documentele depuse, nici în singura dezbatere publică organizată pe marginea acestui proiect de lege. Opiniile critice și argumentele societății civile cu privire la inutilitatea unei asemenea legi, ca și explicații cu privire la cazuri în care lipsa unei asemenea legi ar fi dus la probleme majore – au fost respinse fără a se prezenta alte argumente.

### **3.2. Să demonstreze că ingerința este potrivită pentru a satisface acea nevoie:**

Stabilirea necesității ingerinței, într-un anumit caz, înseamnă, de asemenea, stabilirea că această ingerință este necesară ca să se ajungă la scopul urmărit. Cu alte cuvinte, această măsură necesară poate efectiv atenua prejudiciul cauzat societății<sup>20</sup>.

În 2004, Grupul de lucru privind protecția datelor constituit în temeiul Articolului 29 a observat că decizia privind retenția datelor, care a propus *"stocarea tuturor datelor de trafic, a utilizator și a abonaților"*, nu a furnizat *"argumente convingătoare că păstrarea datelor de trafic pentru o astfel de măsură la scară largă este singura opțiune fezabilă pentru combaterea criminalității sau protejarea securității naționale"*. De asemenea, Grupul de lucru a observat că *"instituțiile de aplicare a legii nu au reușit să furnizeze dovezi cu privire la necesitatea unor astfel de măsuri de anvergură"*<sup>21</sup>.

Mai recent, CJUE a reamintit că *"principiul proporționalității impune ca actele instituțiilor comunitare să fie adecvate pentru atingerea obiectivelor legitime urmărite de reglementarea în cauză (...)"*<sup>22</sup>.

În cele din urmă, cercetarea unei necesități interferențiale poate implica revizuirea *"eficienței măsurilor existente"*, care vizează abordarea nevoii sociale imperioase vizate, *"dincolo de*

<sup>18</sup> Op cit fn 14 pct 3.15- 3.19

<sup>19</sup> Vezi CEDO - *Hertel v. Switzerland*, 25 Aug. 1998, apl. n° 25181/94, available at <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-59366>

<sup>20</sup> Vezi în acest sens Hotărârea CJUE din 8 aprilie 2014 în cauzele conexe C-293-12 și C-594-12 *Digital Rights Ireland* și Grupul de lucru privind protecția datelor constituit în temeiul Articolului 29 – Avizul 01/2014 privind aplicarea noțiunilor de necesitate și de proporționalitate și protecția datelor în sectorul asigurării respectării legii – 27.02.2014 disponibil la [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211\\_ro.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_ro.pdf)

<sup>21</sup> Grupul de lucru privind protecția datelor constituit în temeiul Articolului 29 - Opinia 9/2004 - Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.

<sup>22</sup> Hotărârea CJUE din 8 aprilie 2014 în cauzele conexe C-293-12 și C-594-12 *Digital Rights Ireland*

*măsura propusă*", și trebuie să explice "de ce aceste măsuri existente nu mai sunt suficiente" și modul în care măsura propusă va aduce remedii<sup>23</sup>.

În speță, necesitatea de a limita dreptul la viața private constituită de noua lege românească nu este nici stabilită, nici explicată. Nu este propusă nici o analiză a măsurilor existente și a eficacității lor.

#### **4. Proporționalitate**

Principiul proporționalității este "*recunoscut ca unul dintre principiile centrale care guvernează aplicarea drepturilor și libertăților*" și este cuprins în Convenția Europeană a Drepturilor Omului și în protocoalele sale adiționale.

Analiza jurisprudenței CEDO a Curții Europene a Drepturilor Omului subliniază un anumit număr de factori care sunt folosiți pentru a se asigura că ingerința nu merge "*mai departe decât este necesar pentru a îndeplini obiectivul legitim urmărit*"<sup>24</sup>. Acești factori pot fi clasificați în trei categorii de nevoi:

##### **4.1. Ingerința trebuie să fie strict necesară:**

Ingerința trebuie să fie limitată la ceea ce este strict necesar. Acest lucru înseamnă că ingerința trebuie să fie adecvată pentru contextul său, care trebuie să fie adecvat în raport cu scopul urmărit în ceea ce privește domeniul de aplicare, și că acesta trebuie să fie limitată prin măsuri de protecție corespunzătoare.

##### **4.2 Potrivit contextului său:**

Adaptarea ingerinței la contextul său, înseamnă, printre altele, luarea în considerare a mai multor elemente, cum ar fi următoarele:

###### **4.2.1 Gradul de severitate al nevoii sociale:**

Așa cum a fost evidențiat de către Grupul de lucru privind protecția datelor constituit în temeiul Articolului 29, "*cu cât mai severă problema și / sau un mai mare sau mai sever sau substanțial prejudiciul sau dauna la care societatea ar putea fi expusă, cu atât mai mult o ingerință poate fi justificată*". Atunci când scopul ingerinței este siguranța publică, și mai precis prevenirea și descoperirea infracțiunilor, gradul de severitate al nevoii sociale trebuie evaluat cu privire la infracțiunea specifică pentru care măsura este destinată, și la prejudiciul pe care infracțiunea ar cauza-o societății în cazul în care nu sunt abordate.

În cazul legii criticate, nici nevoia socială nu a fost identificată, nici scopurile specifice care urmează a fi abordate.

###### **4.2.2. Proporționalitatea cu comportamentul specific care se dorește a fi limitat<sup>25</sup>:**

###### **4.2.3. Adecvat scopului urmărit:**

Domeniul de aplicare al ingerinței nu trebuie să depășească ceea ce este necesar pentru a atinge scopul urmărit. Acest lucru înseamnă, printre altele, limitareacât mai strictă a volumului de intruziuni în viața privată (de exemplu, a informațiilor cu caracter personal colectate), a numărului de persoane afectate, și a cazurilor de exercitare a măsurii (competențele

<sup>23</sup> Op cit fn 14 pct 3.15- 3.19 3.26

<sup>24</sup> Op cit fn 14 pct 3.15- 3.20

<sup>25</sup> Jeremy McBride, "Proportionality and the European Convention on Human Rights", in The principle of Proportionality in the Laws of Europe, publicata de Evelyn Ellis, Hart Publishing, 1999, pp. 25.



autorităților de aplicare a legii), iar acțiunea trebuie să fie în special limitată la ceea ce este necesar și la timpul în care măsura este eficientă<sup>26</sup>.

În cazul legii criticate, nici una din aceste probleme nu a fost luată în considerare.

Mai mult - așa cum se poate observa, activitățile de colectare date cu caracter personal cu scopul prevenirii actelor infracționale corespund în concret cu ceea ce în materie penală poartă denumirea de **activitate de supraveghere/control cu scopul de adunare probe**, activități specifice exclusiv stadiului de urmărire penală, a cărui începere este condiționată, la rândul său, de anumite evenimente/circumstanțe speciale. Restrângerea/limitarea anumitor drepturi prin simpla accesare, colectare, prelucrare și reținere a acestora, se consideră a fi legală și este justificată doar de începerea urmăririi penale, pentru că, așa cum vom încerca să arătăm, doar o astfel de procedură poate asigura protecția corespunzătoare a vieții persoanelor implicate.

Există de asemenea similitudini între obligația de colectare/stocare a datelor din legea criticată, pe de o parte și actele de stocare/cercetare a sistemelor informatice, pe de altă parte, aceasta din urmă purtând denumirea de "**percheziție informatică**". Art. 168 NCPP definește această instituție procedural penală ca fiind "*procedeul de cercetare, descoperire, identificare și strângere a probelor stocate într-un mediu informatic sau suport de stocare a datelor informatice realizat prin intermediul unor mijloace tehnice și proceduri adecvate, de natură a asigura integritatea*". Este important a fi menționat că actul de percheziție (adică activitatea de stocare și cercetare a acestor date) este supus **controlului procurorului**, care îl inițiază **doar** atunci când descoperirea și strângerea probelor este **necesară**. Ulterior, actul de percheziție va fi supus în aceeași măsură controlului judecătoresc, care va încuviința efectuarea percheziției informatice **doar atunci când cererea este întemeiată**, condiție expres arătată în cadrul alin.(5) a aceluiași art.168 sus menționat.

În plus, în afara de **rigurozitatea** care se impune actului de inițiere a unei astfel de proceduri, chiar și desfășurării în sine îi sunt specifice **anumite reguli menite să asigure legalitatea, transparența acesteia și, nu în ultimul rând protejarea vieții private** a persoanelor implicate. Percheziția în sistem informatic se efectuează **de către un specialist** care funcționează în cadrul organelor judiciare sau din afara acestora, **în prezența procurorului** sau a organului de cercetare penală. Prezența procurorului, respectiv a organului de cercetare penală nu poate fi suplinită de nicio altă persoană, justificarea acestei prezențe constând în aceea că aceste organe **au rolul de a verifica și controla ca actul de percheziție** să fie efectuat fără ca faptele și împrejurările din viața personală a celui percheziționat, să devină în mod nejustificat publice. Prezența acestora sunt un exemplu de transpunere în concret a rolul statului de garant al legalității și ocrotirii **efective și reale** a fiecărui individ în parte, situație care nu poate fi identificată în cazul legii criticate, căreia îi este specifică, dimpotrivă, lipsa oricărei garanții.

Dacă **doar** circumstanțe speciale sunt de natură a justifica începerea urmăririi penale sau acte specifice precum este cel de percheziție informatică, aceasta se datorează caracterului excepțional pe care aceste măsuri îl au față de **regula generală a non-imixtiunii statului în viața individului**.

#### 4.2.4. Limitat de garanții adecvate:

<sup>26</sup> Vezi *Crémieux v. France*, 25 February 1993, Req. n° 11471/85, A256-B, § 40, <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57805>

Pentru a asigura proporționalitatea ingerinței, garanții "adecvate și eficiente" trebuie puse în aplicare.

Aceste garanții constau în primul rând în prevederile legale<sup>27</sup> care detaliază în mod clar limitele de ingerință (printre altele, următoarele aspecte atunci când se ingerința se adoptă în scopul de a asigura siguranța publică: la motivele necesare pentru a cere măsurile care constituie ingerința, cazurile în care măsura poate avea loc, durata măsurii), și modul în care respectarea acestor restricții va fi aplicată și controlată - de exemplu:

- măsuri tehnice care să se asigure de ștergerea datelor după o anumită perioadă de timp;
- autorizarea și supravegherea unei autorități independente<sup>28</sup>, care ar trebui să fie, în principiu, un judecător "*cel puțin în ultimă instanță*" în domeniile "*în care abuzul este potențial atât de ușor în cazuri individuale și ar avea (...) consecințe dăunătoare pentru societatea democratică, ca un întreg*"<sup>29</sup>, care este, în general, în cazul în care se organizează ingerința în scopuri polițienești;
- drepturile de acces și de verificare acordate persoanelor fizice în cauză;
- clarificarea procedurii care trebuie urmată pentru exercitarea acestor drepturi, inclusiv dreptul la apel în cazul în care dreptul de acces este interzis<sup>30</sup>.

Celelalte garanții care urmează să fie puse în aplicare ar trebui să provină în principal de la acest temei juridic (punerea în aplicare a măsurilor tehnice, organizarea judiciară și alocarea de resurse pentru a asigura eficiența controalelor judiciare etc.).

În cazul legii criticate, nici măcar una dintre aceste garanții nu au fost propuse.

Astfel, deși legea criticată aduce schimbări importante în regimul comercializării și utilizării cartelor SIM preplătite, precum și în regimul utilizării rețelelor publice de internet, aceasta **nu conține o procedură clară** prin care agenții din unitățile de vânzare a cartelelor preplătite (care, conform practicii, pot fi chioșcuri de ziare, benzinării, magazine de cartier, supermarketuri ș.a.m.d.) **vor colecta numele, codul numeric personal, seria și numărul cărții de identitate ale utilizatorului, și nici condițiile în care vor stoca aceste date cu caracter personal**. În ceea ce privește măsura identificării utilizatorilor rețelelor publice de internet de către agenții economici sau de către alți furnizori de astfel de rețele, singura măsură certă cu privire la stocarea datelor de identificare a utilizatorilor este ca acestea să fie stocate timp de 6 luni pe un echipament electronic gestionat de furnizorul rețelei publice Wi-Fi, urmată de distrugerea "ireversibilă" a datelor la expirarea acestei perioade, cu excepția datelor solicitate de către "autoritățile prevăzute de lege".

Toate elementele operaționale ale măsurilor propuse de normele criticate indică **prezența arbitrariului în ingerințele aduse dreptului la viață privată**: există incertitudine cu privire la:

---

<sup>27</sup> Vezi CEDO: *Klass și alții/Republica Federală Germania*, Curtea Europeană a Drepturilor Omului, 6 septembrie 1978 (seria A, nr. 28) Paragraf 50 și următoarele, disponibilă la <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510>

<sup>28</sup> Vezi fn 14 Paragraf 3.24

<sup>29</sup> *CEDO: Klass și alții/Republica Federală Germania*, Curtea Europeană a Drepturilor Omului, 6 septembrie 1978 (seria A, nr. 28)

<sup>30</sup>

<sup>□</sup>, *CEDO M.G. vs. Marea Britanie*, appl. n° 39393/98,.; *CEDO: Klass și alții/Republica Federală Germania*, Curtea Europeană a Drepturilor Omului, 6 septembrie 1978 (seria A, nr. 28)

- modalitatea în care datele de identificare ale utilizatorilor cartelelor preplătite vor fi stocate și accesate;
- cine are de dreptul de a accesa aceste date și în ce condiții;
- cine va trebui de fapt să colecteze aceste date (furnizorul de telefonie mobilă sau societatea comercială care vinde aceste cartele);
- cine sunt persoanele care au acces la bazele de date locale create de către agenții economici/alte persoane juridice conținând datele de identificare ale utilizatorilor rețelelor Wi-Fi publice;
- dacă există și o bază de date centralizată cu aceste informații sau nu (și dacă nu există o baza de date centralizată, dacă există o interconectare între bazele de date locale) etc.

Un alt aspect care merită a fi reținut este împrejurarea că, așa cum se poate constata din conținutul textului legii criticate, păstrarea datelor și utilizarea ulterioară sunt efectuate fără ca utilizatorul să fie informat cu privire la aceasta, fapt considerat a imprima în conștiința persoanelor vizate sentimentul că viața lor privată face obiectul unei supravegheri constante, aspect constatat prin Decizia CCR nr.440/2014.

#### **4.3.Efectul ingerinței nu poate să ducă la suprimarea unui drept legal**

În cazul nostru, ceea ce se dorește este a nu se permite dreptul de a accesa anonim internetul sau rețelele telefonice, deși acest drept este prevăzut în mod explicit în mai multe legislații europene, iar anonimitatea este considerată ca parte a dreptului la viața privată. De fapt, anonimitatea comunicării este imperios necesară în anumite condiții – de exemplu pentru descoperirea unor activități ilegale – cum ar fi legea avertizorilor de integritate<sup>31</sup> sau raportarea de cazuri de corupție la liniile telefonice gratuite anticorupție.<sup>32</sup>

#### **4.4 Necesitatea socială nu poate fi “abordată în mod satisfăcător într-un fel mai puțin restrictiv”<sup>33</sup>:**

În plus, Curtea verifică dacă obiectivul interferenței lui "*poate fi abordat în mod satisfăcător într-un alt, mod mai puțin restrictiv*". De exemplu, "*un ordin prin care un jurnalist trebuia să dezvăluie sursa informațiilor lui referitoare la afacerilor unei companii a fost considerat ca ar fi nejustificat (...) în măsura în care obiectivul a fost de a împiedica difuzarea de informații confidențiale de la această preocupare legitimă care a fost deja asigurată de o publicație de restricție a informațiilor care au fost comunicate*"<sup>34</sup>.

În cazul nostru, legiuitorul nu a luat în considerare nicio altă măsură care ar fi putut să fie implementată pentru a atinge scopul propus de legea criticată.

### **III. Concluzie**

**În concluzie atingerea dreptului la viață privată al tuturor utilizatorilor de cartele SIM preplătite din România (aproximativ 67% din numărul total de utilizatori al serviciilor de**

<sup>31</sup>

Legea nr. 571/2004 privind protecția personalului din autoritățile publice, instituțiile publice și din alte unități care semnalează încălcări ale legii (publicată în Monitorul Oficial nr. 1214 din 17 decembrie 2004)

<sup>32</sup> Se primesc peste 8000 de apeluri pe an cu privire la fapte anticorupție conform DNA <http://www.mediafax.ro/social/peste-4-600-de-apeluri-in-6-luni-la-telverde-anticoruptie-cele-mai-multe-sesizari-pentru-luare-de-mita-12974985>

<sup>33</sup> Vezi o aplicare a acestui principiu in decizia *V. v. European Parliament*, 5 July 2011, case F-46/09, § 139, disponibilă la <http://curia.europa.eu/juris/liste.jsf?language=en&num=F-46/09>

<sup>34</sup> Vezi □ Jeremy McBride, op cit, p. 26, referindu-se la cazul *CEDO to Goodwin v. United Kingdom*, judgment of the Court, 27 Mar. 1996

comunicații mobile<sup>35</sup> - cca 13 milioane de cartele preplătite sunt pe piața românească), precum și al tuturor persoanelor care se conectează la rețelele Wi-Fi publice (ca de exemplu rețelele Wi-Fi oferite gratuit în piețe publice, în biblioteci, în universități, în restaurante, în parcuri etc.) încalcă **toate cele patru elemente care ar trebui îndeplinite cumulativ - temeiul juridic, scopul legitim, necesitatea și proporționalitatea – pentru ca această ingerință să fie necesară într-o societate democratică.**

Reglementarea legii criticate este generală, fără elemente diferențiatore, iar măsurile ce se doresc a fi impuse corespund mai degrabă unui sistem de supraveghere generală în care toți cetățenii sunt considerați suspecti.

Această ingerință în dreptul la viață privată "privește în egală măsură pe toți destinatarii legii, indiferent dacă au săvârșit sau nu fapte penale sau dacă sunt sau nu subiectul unor anchete penale, **ceea ce este de natură să răstoarne prezumția de nevinovăție** și să transforme *a priori* toți utilizatorii serviciilor de comunicații electronice (în speță, toți utilizatorii cartelelor SIM preplătite) sau de rețele publice de comunicații (în speță, toți utilizatorii rețelelor Wi-Fi publice sau la care este oferit acces în spații publice) în persoane susceptibile de săvârșirea unor infracțiuni de terorism sau a unor infracțiuni grave".<sup>36</sup>

***În concluzie, dispozițiile Legii pentru completarea OUG nr. 111/2011 privind comunicațiile electronice sunt neconstituționale, raportate la art. 26, art. 1 alin. (3) și art. 53 alin. (2) din Constituție, precum și, întemeiul art. 148 alin. (2) și alin. (4), raportate la art. 8 CDFUE.***

**Pentru semnături, Maria-Nicoleta Andreescu  
Director Executiv APADOR-CH**

---

<sup>35</sup> Vezi statistici oficiale ale Autorității Naționale de Reglementare în Comunicații (ANCOM) - <https://statistica.ancom.org.ro:8000/sscpds/public/categories/communications>

<sup>36</sup> Decizia Curții Constituționale nr. 1258 din 8 octombrie 2009, publicată în M. Of. nr. 798/2009 din 23 noiembrie 2009