# STRATEGII ŞI POLITICI DE SECURITATE

# O ANALIZĂ COMPARATIVĂ A JURISPRUDENŢEI CURŢII DE JUSTIŢIE EUROPENE ŞI A CURŢII CONSTITUŢIONALE A ROMÂNIEI ÎN DOMENIUL STOCĂRII METADATELOR COMUNICĂRII TELEFONICE SAU ELECTRONICE

**Valentin STOIAN***

**Abstract:**

*The aim of the paper is to compare and contrast the jurisprudence of the European Court of Justice and the Romanian Constitutional Court on the topic of metadata retention. The paper will argue that both Courts, when considering the effect on the right to privacy, essentially see metadata retention and use as on a par with the interception of the content of communication.*

*Firstly, the paper will commence with a summary of the directive and will discuss its main provisions. Further, the centerpiece of the paper will be the comparison of the Digital Rights Ireland decision and the RCC decisions. The common arguments of the two courts will be drawn out and systematized in a table. This will be presented according to the character of the action of metadata retention and to the type of infringement detected by the Court (essential rights violation or disproportionality).*

**Keywords**: *jurisprudence, European Court of Justice, Romanian Constitutional Court, metadata retention*

## Introducere

Luna aprilie 2014 a generat o provocare serioasă la adresa celor care susţin reglementarea retenţiei metadatelor la nivel european. Printr-o decizie fără precedent, (*Digital Rights Ireland v. Minister of Communication*, C-293/12 şi C-594/12), Curtea Europeană de Justiţie (Luxemburg) a declarat că Directiva 2006/24/EC asupra retenţiei metadatelor comunicaţiilor telefonice sau electronice este invalidă. Invaliditatea acesteia a fost stabilită de Curte nu doar *ex nunc* (pentru viitor) ci şi *ex tunc* (pentru trecut) (Rauhofer & Sithigh, 2014).

* Institutul Naţional de Studii de Intelligence, Academia Naţională de Informaţii „Mihai Viteazul"

Astfel, directiva din 2006 a fost anulată complet, procedurile de *infrigement* deja pornite au fost retrase, iar Suediei i s-a returnat o amendă de 3 milioane de euro plătită pentru neimplementarea acestei directive (Luxembourg Weekly, 17.05.2014).

Înainte ca Curtea de la Luxemburg să îşi anunţe decizia, tema stocării metadatelor a fost intens dezbătută în mai multe state membre ale UE. Stocarea metadatelor a fost supusă judecăţii Curţilor Constituţionale în mai multe ţări europene, legile care transpuneau directiva fiind de multe ori respinse de aceste instanţe. Astfel, în 2008, Curtea Supremă Administrativă a Bulgariei a anulat legea care transpunea directiva în legislaţia naţională, iar în 2010 acelaşi rezultat a fost obţinut în faţa Curţii Constituţionale din Germania (De Vries et al., 2011). Situaţii similare au apărut în 2011 în Cipru şi în Republica Cehă (Guild & Carrera, 2014; Kosta, 2013, p. 339). În România, situaţia a fost deosebit de interesantă, deoarece guvernul a încercat transpunerea directivei nu o dată, ci de două ori şi a suplimentat cadrul juridic al identificării apelantului prin legea înregistrării cartelelor *pre-paid*. Toate cele trei tentative s-au soldat cu eşecuri, având în vedere că Curtea Constituţională a României a respins aceste legi prin trei decizii separate (1258/2009, 440/2014, 461/2014). „Drumul către Luxemburg" (De Vries et al., 2011) a fost presărat de mai multe decizii invalidând legislaţia care prevedea retenţia metadatelor, aceasta fiind considerată ca intrând în contradicţie cu drepturile omului.

Scopul lucrării este de a compara jurisprudenţa Curţii Europene de Justiţie şi a Curţii Constituţionale a României în domeniul stocării metadatelor. Lucrarea argumentează că, în ceea ce priveşte relaţia dintre dreptul la viaţă privată şi stocarea metadatelor, ambele Curţi privesc această procedură ca implicând o interferenţă la fel de gravă precum interceptarea conţinutului comunicaţiilor.

În primul rând, lucrarea va prezenta un rezumat al Directivei 2006/24/EC. Partea a doua a lucrării, reprezentând punctul cheie al acesteia, va fi comparaţia între jurisprudenţa celor două curţi (Curtea Europeană de Justiţie şi Curtea Constituţională a României). Argumentele comune ale celor două curţi vor fi prezentate şi sistematizate într-un tabel. Criteriile pe care se va baza tabelul sunt caracteristicile legislaţiei retenţiei metadatelor şi tipul de încălcare sesizat de Curte (violarea esenţială a drepturilor sau acţiune disproporţionată).

**Directiva 2006/24/EC asupra retenţiei metadatelor şi „drumul către Luxemburg"**

Directiva 2006/24/EC a fost adoptată în urma atacurilor teroriste de la Londra şi Madrid din 2004 şi 2005, reprezentând, de la momentul adoptării acesteia şi până în Aprilie 2014, principalul act legislativ care guverna păstrarea datelor de localizare a traficului telefonic sau electronic (Brown, 2010). Directiva obliga statele membre să creeze un cadru legislativ care să impună furnizorilor de servicii telefonice şi de internet să stocheze, pentru minimum şase luni şi maximum doi ani, „datele de indentificare a traficului atât pentru persoane fizice cât şi pentru persoane juridice, precum şi datele necesare pentru identificarea abonatului sau utilizatorului înregistrat"(Directive 2006/24/EC; Directive 2002/58/EC).

Obligaţia astfel stabilită se extindea la o paletă largă de date precum numărul de telefon şi adresele atât ale apelantului cât şi ale apelatului (obligaţia se extindea atât pentru apeluri la care nu s-a răspuns, deoarece acestea pot fi utilizate de către grupuri teroriste pentru declanşarea unor dispositive explozive) (Guarino, 2014, p. 249-255), ID-ul userului, adresa IP sau numele ambelor părţi angajate în comunicarea online, momentul şi durata apelului telefonic, momentul accesării serviciului de internet, date necesare pentru identificarea echipamentului şi a locaţiei acestuia (International Mobile Subscriber Identity-IMSI, International Mobile Equipment Identity IMEI), linia abonamentului numeric (DSL), ID-ul celulei din interiorul căreia s-a iniţiat apelul (Guarino, 2014). Într-un final, Directiva cerea statelor membre să se asigură că datele sunt protejate faţă de accesul neautorizat şi sunt disponibile doar personalului guvernamental autorizat, fiind distruse la sfârşitul perioadei de stocare. Însă, Directiva lăsa la latitudinea statelor membre modul cum acest acces este reglementat, stipulând că „procedurile care trebuie să fie urmate şi condiţiile care trebuie să fie îndeplinite pentru a obţine acces la datele păstrate în conformitate cu cerinţele de necesitate şi proporţionalitate sunt definite de fiecare stat membru, în dreptul intern al fiecăruia, sub rezerva dispoziţiilor relevante ale dreptului Uniunii Europene sau ale dreptului internaţional public şi, în special, a dispoziţiilor Convenţiei Europene a Drepturilor Omului, astfel cum au fost interpretate de către Curtea Europeană pentru Drepturile Omului" (Guarino, 2014).

În preambul, Directiva îşi stabilea două scopuri majore: armonizarea legislaţiilor naţionale în domeniul stocării metadatelor şi crearea de instrumente pentru „investigarea, detectarea şi pedepsirea infracţiunilor serioase" (Directive 2006/24/EC). Pentru a justifica adoptarea acestor măsuri, Directiva se referă în mod expres la declaraţia Consiliului Europei din 13 iulie

2005, care a condamnat atacurile teroriste din 13 iulie 2005, reafirmând necesitatea de a adopta măsuri comune asupra stocării metadatelor, cât mai curând posibil. De asemenea, preambulul Directivei declara că stocarea metadatelor trebuie să ia în considerare dreptul la viaţă privată aşa cum a fost enunţat atât de Convenţia Europeană a Drepturilor Omului (Articolul 7) cât şi de Carta Fundamentală a Drepturilor Omului în Europa (Articolele 7 şi 8), dar şi că acest drept poate fi limitat pentru motive cum ar fi „securitatea naţională sau ordinea publică, prevenirea dezordinii sau criminalităţii sau în vederea protecţiei drepturilor şi libertăţilor celorlalţi". Astfel, preambulul Directivei afirma „Deoarece păstrarea datelor s-a dovedit a fi un instrument de investigare atât de necesar şi eficace pentru aplicarea legii în mai multe state membre şi, în special, în ceea ce priveşte problemele grave, cum sunt criminalitatea organizată şi terorismul, este necesară siguranţa că datele păstrate sunt puse la dispoziţia autorităţilor de aplicare a legii pentru o anumită perioadă, sub rezerva condiţiilor prevăzute de prezenta Directivă. Adoptarea unui instrument de păstrare a datelor care să respecte cerinţele articolului 8 din CEDO este, prin urmare, o măsură necesară" (Directive 2006/24/EC).

Directiva a fost prima dată atacată de către guvernul Irlandei, în faţa Curţii de Justiţie a UE fiind criticată pentru nerespectarea procedurii necesare pentru a o adopta. Irlanda a criticat Directiva în faţa Curţii din Luxemburg, arătând că nu trebuia adoptată utilizând procedurile primului pilon al al UE[1], ci ale celui de-al treilea, având în vedere că scopul său principal era combaterea crimei organizate şi terorismului, iar „prevenirea distorsiunilor pieţiei comune" era doar un obiectiv „accidental" (Kosta, 2013). CJUE a respins această abordare, susţinând că Directiva nu reglementa accesul organelor naţionale de impunere a legii la date, ci se adresa furnizorilor de servicii de telefon şi de internet. Această caracteristică a directivei a reprezentat, în opinia Curţii, o dovadă suficientă pentru a susţine că scopul principal al directivei este reglementarea pieţei interne.

Chiar şi înainte de decizia CJUE din 2014, legislaţiile naţionale care transpuneau directiva au fost respinse de Curţile Constituţionale ale mai multor ţări membre. Curtea Supremă Administrativă a Bulgariei s-a concentrat pe faptul că agenţiile de impunere a legii ar putea accesa, fără mandat, datele stocate printr-un calculator specializat. Aceasta a fost

[1] Atunci când Directiva a fost adoptată şi când această speţă a fost decisă iniţial, Uniunea funcţiona pe sistemul celor trei piloni, Comunităţile Europene fiind distincte şi utilizând un alt mod de a lua decizii decât Politica Externă şi de Securitate şi Cooperarea în domeniul Justiţiei şi Afacerilor Interne. Aceste distincţii au dispărut o dată cu Tratatul de la Lisabona.

considerată, de către Curtea din Bulgaria, o violare a Articolului 32(1) din Constituţia Bulgariei şi a Articolului 8 al Convenţiei Europene a Drepturilor Omului (Kosta, 2013). Prin decizia din 2010, Curtea Constituţională a Germaniei nu a evaluat directiva *per se*, ci a stabilit că obligaţia de a stoca datele fără discriminare (fără a lua în considerare dacă persoana ale cărei comunicaţii sunt stocate este suspectată de o infracţiune) şi lipsa unei autorizaţii judiciare pentru accesul la date este o violare disproporţionată a Articolului 10(1) din Legea Fundamentală a Germaniei, articol ce protejează secretul corespondenţei. Conform Curţii Constituţionale Germane, stocarea datelor nu este ne-constituţională în sine, dar intră în conflict cu dreptul la viaţă privată şi trebuie supusă unui „control riguros al proporţionalităţii"(Kosta, 2013; de Vrije set al.). O abordare similară a fost propusă şi de Curtea Constituţională a Cehiei în 2011, susţinând că obligaţiile impuse furnizorilor de telecomunicaţii sunt vagi şi că accesul nediscriminatoriu la date este inacceptabil, acesta trebuind să se bazeze pe „suspiciuni bine fondate" (Kosta, 2013, p. 355). De asemenea, în 2011, Curtea Supremă din Cipru, a avut de rezolvat o plângere civilă a unor persoane ale căror date de comunicaţii au fost cerute de poliţie. Curtea a respins cererile poliţiei, în trei din patru cazuri, afirmând că permiterea accesului la datele de trafic ar viola secretul comunicaţiilor (Kosta, 2013, p. 354).

### *Digital Rights Ireland v. Ministry of Communications* şi Deciziile Curţii Constituţionale a României

În motivaţia Deciziei sale din Aprilie 2014, Curtea Europeană de Justiţie a pornit de la premisa că stocarea datelor de comunicaţie intră în conflict cu dreptul la viaţă privată (Articolul 7 al Cartei) şi cu dreptul la protecţia datelor personale (Articolul 8 din Cartă). Principalul motiv pentru care aceste drepturi sunt afectate este că „Aceste date, privite ca întreg, pot conduce la concluzii foarte precise în ceea ce priveşte viaţa privată a persoanelor căror date au fost reţinute" (European Court of Justice, 8.04.2014). Acest fapt, în sine, nu presupune invalidarea Directivei, ţinând cont de faptul că Articolul 52(1) al Cartei permite limitarea drepturilor: „Orice restrângere a exerciţiului drepturilor şi libertăţilor recunoscute prin prezenta cartă trebuie să fie prevăzută de lege şi să respecte substanţa acestor drepturi şi libertăţi. Prin respectarea principiului proporţionalităţii, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare şi numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesităţii protejării drepturilor şi libertăţilor celorlalţi" (European Court of Justice, 8.04.2014). Prin urmare, Curtea a stabilit că este

necesar să întreprindă o verificare a proporţionalităţii încălcării drepturilor fundamentale.

În primul rând, Curtea a stabilit că esenţa dreptului la viaţă privată nu a fost încălcată, deoarece Directiva nu permitea interceptarea conţinutului comunicaţiilor. Mai mult, Curtea a susţinut că Directiva serveşte un scop legitim, având ca ţel „prevenirea, cercetarea, detectarea şi urmărirea penală a infracţiunilor şi, în special, a criminalităţii organizate" (European Court of Justice, 8.04.2014). În continuare, Curtea a susţinut că testul crucial pe care trebuie să îl treacă Directiva este cel al proporţionalităţii, însemnând că „legile Uniunii Europene trebuie să fie adecvate scopului ce urmează a fi atins, şi să nu depăşească ceea ce este necesar pentru a atinge acele obiective" (European Court of Justice, 8.04.2014). Având în vedere că încălcarea dreptului la viaţă privată este foarte serioasă, CJUE a afirmat că discreţia permisă Parlamentului European este foarte redusă.

În a doua parte a speţei, Curtea critică Directiva, susţinând că este nevoie de o analiză care să pună în balanţă dreptul la viaţa privată şi scopul legitim (deşi nu neapărat decisiv) al Directivei. Curtea a luat în considerare **caracterul general al Directivei**, în special faptul că aceasta stipulează stocarea tuturor datelor create de toate comunicaţiile electronice ale cetăţenilor europeni. Astfel, decizia se axează pe reţinerea datelor persoanelor care nu sunt, nici măcar indirect, într-o situaţie „care să poată conduce la urmărirea penală" (European Court of Justice, 8.04.2014), precum şi pe lipsa unor limitări din punct de vedere al duratei, ariei geografice sau circumstanţelor personale. De asemenea, Curtea arată că nu există **limite pentru folosirea datelor**: absenţa procedurilor (cum ar fi aprobarea prealabilă data de un judecător) sau un criteriu obiectiv pentru limitarea accesului la date de către autorităţile naţionale (European Court of Justice, 8.04.2014).

În ceea ce priveşte **stocarea datelor**, decizia în speţa supusă analizei arată că Directiva nu realizează o distincţie între date utile şi date inutile pentru a stabili perioada de stocare. În cele din urmă, Curtea susţine că protecţia datelor stocate nu este realizată la un nivel corespunzător, deoarece furnizorilor le este permisă stabilirea nivelului de protecţie inclusiv prin luarea în considerare a considerentelor economice (European Court of Justice, 8.04.2014) şi deoarece nu este impusă obligaţia distrugerii ireversibile a datelor la sfârşitul perioadei de stocare. O problemă extrem de serioasă este faptul că Directiva nu impune stocarea datelor pe teritoriul UE, având ca rezultat situaţia în care „nu se poate asigura verificarea respectării

standardelor de protecţie de către o autoritate independentă" (European Court of Justice, 8.04.2014).

Prima lege care transpunea Directiva 2006/24/EC în România a fost Legea 298/2008. Aceasta obliga furnizorii de servicii de telecomunicaţii să stocheze datele „de trafic şi de localizare a persoanelor fizice şi juridice, precum şi datele conexe necesare pentru identificarea abonatului sau a utilizatorului înregistrat" (Law 298/2008). Legea enumeră datele stipulate în Directivă şi impune obligaţia stocării pe o perioadă de şase luni, perioada minimă cerută de Directivă. Această lege creează, de asemenea, o distincţie între procedurile pe care trebuie să le urmeze organele de impunere a legii şi procurorii, pe de-o parte, şi „organele de stat cu atribuţii în domeniul securităţii naţionale", pe de altă parte (European Court of Justice, 8.04.2014). În timp ce primele trebuie să ceară un mandat specific din partea autorităţilor judiciare, cea de-a doua categorie nu avea această obligaţie.

Prima decizie a Curţii Constituţionale a României (CCR) în acest domeniu a fost emisă în Octombrie 2009, într-o speţă în care se discuta constituţionalitatea legii 298/2008 (Decizia Curţii Constituţionale a României nr. 1258/Octombrie 2009). Curtea şi-a început argumentarea prin evocarea unor aspecte similare precum cele din decizia CJUE (care nu fusese încă emisă la momentul respectiv): limitarea drepturilor fundamentale este permisă atât timp cât aceasta este necesară pentru un scop legitim cum ar fi securitatea naţională, ordinea publică, prevenirea şi urmărirea penală a infracţiunilor, atât timp cât această limitare este proporţională, nediscriminatorie şi nu afectează însăşi esenţa dreptului (Decizia Curţii Constituţionale a României nr. 1258/Octombrie 2009). Primul argument al Curţii se referă la tipul de date care urmează să fie stocate conform cerinţelor Legii nr. 298. Se stipulează că „legea se referă la datele de trafic şi de localizare, precum şi la datele conexe necesare pentru identificarea abonatului sau a utilizatorului înregistrat" (Decizia Curţii Constituţionale a României nr. 1258/Octombrie 2009). CCR a considerat că formularea „date conexe" este mult prea vagă şi nu identifică în mod clar datele ce trebuie reţinute. Această formulare vagă permite interpretarea arbitrară şi nu permite adresanţilor legii să o înţeleagă şi să îşi adapteze comportamentul în consecinţă.

De asemenea, CCR a criticat formularea vagă a articolului 20 al Legii, „În scopul prevenirii si contracarării ameninţărilor la adresa securităţii naţionale, organele de stat cu atribuţii în acest domeniu pot avea acces, în condiţiile stabilite prin actele normative ce reglementează activitatea de realizare a securităţii naţionale, la datele reţinute de furnizorii de servicii şi reţele publice de comunicaţii electronice" (Decizia Curţii Constituţionale

a României nr. 1258/Octombrie 2009). Deoarece nu există o specificare clară a ameninţărilor la adresa securităţii naţionale, Curtea a afirmat că acest articol este potenţial supus interpretărilor arbitrare, orice acţiune putând fi interpretată ca o ameninţare la adresa securităţii naţionale.

Cea mai serioasă critică menţionată de CCR este **caracterul continuu al stocării**, care, împreună cu **absenţa unor limite asupra utilizării datelor** (lipsa obligativităţii unui mandat emis de judecător) reprezintă o încălcare a însăşi esenţei dreptului la viaţă privată. De asemenea, Curtea a întreprins şi un test de proporţionalitate, susţinând că o măsură care încalcă un drept poate fi proporţională doar dacă impunerea sa încetează atunci când cauza care a necesitat-o dispare. Deşi datele referitoare la comunicaţiile tuturor sunt stocate, această măsură nu se aplică doar atunci când apare o necesitate justificată şi nu încetează la dispariţia acesteia. În plus, CCR a susţinut că datele unei persoane ce primeşte un apel sunt, de asemenea, stocate, expunând persoana la o intruziune nejustificată. CCR a concluzionat că caracterul general şi continuu al stocării datelor este o violare inacceptabilă a dreptului la viaţă privată (Decizia Curţii Constituţionale a României nr. 1258/Octombrie 2009). Un lucru pe care decizia CCR nu îl clarifică este dacă sursa neconstituţionalităţii este faptul că substanţa dreptului este încălcată sau dacă măsura stocării este pur şi simplu disproporţionată.

România a transpus din nou Directiva 2006/24/EC prin Legea 82/2012. Această lege a clarificat expresia „date conexe" criticată de Curtea Constituţională în decizia precedentă, stipulând că legea se aplică „datelor de trafic şi de localizare a persoanelor fizice şi a persoanelor juridice, precum şi datelor necesare pentru identificarea unui abonat sau unui utilizator înregistrat" (Law 82/2012). De asemenea, Legea 82/2012 a extins sfera de aplicare a stocării metadatelor, permiţând utilizarea acestora pentru urmărirea unui număr mult mai mare de infracţiuni decât în legea anterioară. Această lege a menţinut distincţia dintre organele de impunere a legii şi organe cu atribuţii în domeniul securităţii naţionale, obligând primele să ceară un mandat, dar exceptând cea de-a doua categorie.

Această lege a fost din nou contestată la Curtea Constituţională, iar decizia acesteia a fost data publicităţii în iunie 2014, la doar două luni de la decizia CJUE. În primul rând, Curtea a susţinut că ambiguităţile Legii 298/2008 nu au fost eliminate, din moment ce Legea 82 stipula că se aplică „datelor de trafic şi de localizare a persoanelor fizice şi a persoanelor juridice, precum şi datelor necesare pentru identificarea unui abonat sau unui utilizator înregistrat" (Decizia Curţii Constituţionale a României 440/2014). CCR a comparat obligaţiile impuse de Legea 82/2012 cu cele ale Legii

298/2008, afirmând că motivele care au dus la invalidarea celei de-a doua subzistă şi la prima. Astfel, Legea 82 conţinea, în opinia Curţii, o obligaţie de stocare a datelor cu caracter general, precum şi lipsa unor garanţii, cum ar fi mandatul judecătoresc, faţă de folosirea abuzivă a acestora de către autorităţile de stat (Decizia Curţii Constituţionale a României 440/2014).

De asemenea, CCR a stabilit o distincţie între stocare şi utilizarea metadatelor, afirmând că prima procedură nu este, în sine o încălcare a dreptului la viaţa privată. Pe de altă parte, accesarea datelor reprezintă, în viziunea Curţii, o încălcare a acestui drept. Legea 82 obliga organele de impunere a legii să ceară un mandat din partea autorităţii judecătoreşti, această obligaţie nefiind impusă şi „organelor de stat cu atribuţii în domeniul securităţii naţionale" (Decizia Curţii Constituţionale a României 440/2014). Accesarea fără mandat a metadatelor stocate este, în opinia Curţii, o încălcare inacceptabilă a dreptului la viaţă privată. De asemenea, Curtea a afirmat că securitatea datelor nu este asigurată corespunzător, furnizorii nefiind controlaţi cu adevărat (Decizia Curţii Constituţionale a României 440/2014).

Cadrul normativ în domeniul stocării metadatelor a fost suplimentat prin impunerea unei obligaţii asupra distribuitorilor de cartele *pre-paid* şi a celor care oferă servicii de internet wi-fi de a identifica pe utilizatorii acestor servicii. A fost propusă o iniţiativă legislativă, dar aceasta a fost trimisă Curţii Constituţionale de către Avocatul Poporului înainte de promulgare. Conform acestei iniţiative, distribuitorii de cartel *pre-paid* sau cei care oferă servicii de acces la internet prin wi-fi gratis erau obligaţi să ceară datele de identificare a propriilor clienţi. Curtea Constituţională a României a criticat această abordare, afirmând că extinderea sferei de aplicare a legii va duce la stocarea metadatelor unui număr mult mai mare de persoane (nu doar cei care deţin un abonament de telefonie mobilă, ci şi care care achiziţionează cartele *pre-paid* sau cei care accesează internetul de la hotspoturi wi-fi), precum şi la procesarea acestor date de un număr mult mai mare de operatori (de exemplu, vânzătorii de cartel *pre-paid* şi cei care oferă internet liber în cafenele). Această extindere nu aduce cu sine, în opinia Curţii, o obligaţie corelativă de confidenţialitate impusă celor care colectează aceste date personale. Aceste motive sunt suficiente, în opinia Curţii, pentru a declara legea neconstituţională (Decizia Curţii Constituţionale a României 461/16 Septembrie 2014).

Trei judecători ai Curţii Constituţionale au emis o opinie separată, afirmând că legea supusă analizei se referă doar la stocarea şi nu la utilizarea datelor. Deşi impunerea unor garanţii pentru utilizarea în siguranţă a datelor stocate, cei trei judecători au afirmat că, din moment ce stocarea metadatelor nu

este, în sine, neconstituţională, extinderea sau reducerea sferei de aplicare a celor care le colectează nu este, în sine, problematică din punct de vedere constituţional (Decizia Curţii Constituţionale a României 461/16 Septembrie 2014).

Principala concluzie care poate fi trasă din această analiză este că există o confuzie în deciziile Curţii Constituţionale. Din lectura acestora nu se desprinde clar dacă stocarea metadatelor încalcă însăşi esenţa dreptului la viaţă privată sau este doar un mijloc disproporţionat de a atinge un ţel legitim. CCR pare să susţină ambele variante, în ciuda imposibilităţii logice ca ambele să fie adevărate în acelaşi timp. O acţiune care încalcă însăşi esenţa dreptului la viaţă privată nu poate fi, în acelaşi timp, un mijloc disproporţionat de a atinge un scop legitim. Spre deosebire de Curtea Constituţională a României, Curtea de Justiţie a UE a sesizat această distincţie, afirmând că stocarea metadatelor este un mijloc disproporţionat, dar nu încalcă esenţa dreptului.

A doua concluzie a analizei este că ambele organe juridice nu disting între interceptarea conţinutului unei comunicaţii şi stocarea metadatelor acesteia. Atât CCR cât şi CJUE afirmă că stocarea metadatelor generează o frică legitimă de supraveghere, că nu ar trebui aplicată cu caracter de generalitate, ci doar în situaţii specifice, în urma autorizării judecătoreşti.

| **Caracteristica stocării metadatelor**<br>**Motive pentru invalidare** | **Caracter general/ nediscriminatoriu** | **Caracter continuu ( pe o durată lungă de timp)** | **Posibilitatea de accesare a datelor stocate fără mandat** | **Absenţa garanţiilor împotriva accesului neautorizat** |
|---|---|---|---|---|
| Încalcă esenţa dreptului | DCC 1289/2009 | DCC 440/2014<br>DCC 1289/2009 | DCC 1289/2009<br>DCC 440/2014 | DCC 461/2014 |
| Este un mijloc dispropoţionat pentru atingerea unui scop legitim | *Digital Rights Ireland* | *Digital Rights Ireland* | *Digital Rights Ireland* | *Digital Rights Ireland* |

## Concluzii

Analizând comparativ argumentele celor două Curţi, există motive comune pentru care Directiva 2006/24/EC şi legile care o transpuneau au fost invalidate. În primul rând, trebuie menţionat faptul că ambele Curţi au stabilit o distincţie între stocarea şi utilizarea metadatelor. În timp ce prima este o operaţiune tehnică, doar cea de-a doua afectează direct dreptul la viaţă

privată. Ambele Curţi au considerat că accesul la metadatele stocate generează probleme dacă are caracter continuu şi general. S-a argumentat că este necesară restrângerea sferei persoanelor ale căror metadate sunt accesate la acelea asupra cărora planează o suspiciune rezonabilă de implicare în activitate infracţională. Alte criterii care ar putea fi utilizate pentru a limita accesul nediscriminatoriu la metadate sunt localizarea geografică sau perioada de timp în care echipamentul a fost utilizat.

Un alt motiv crucial pentru invalidarea acestor legi a fost existenţa unei distincţii între organele de impunere a legii (care au nevoie de mandat pentru a accesa metadatele stocate) şi serviciile de informaţii care nu au nevoie de mandat. Ambele Curţi au considerat că stocarea metadatelor şi utilizarea acestora nu este radical diferită de interceptarea conţinutului comunicaţiilor, având, precum aceasta din urmă, nevoie de autorizare judecătorească. De asemenea, ambele Curţi au susţinut că este necesară impunerea unor garanţii stricte pentru a preveni accesul neautorizat la metadatele stocate, incluzând localizarea acestora fizică în Europa.

Situaţia recentă, creată ca urmare a atacurilor teroriste din Franţa, din ianuarie 2015, care a condus la adoptarea unei legi de către această ţară ce prevede stocarea metadatelor comunicaţiilor va genera aprinse dezbateri în această ţară. Decizia Consiliului Constituţional Francez asupra acestei legi va reprezenta un nou moment de reflecţie în ceea ce priveşte relaţia dintre stocarea metadatelor şi dreptul la viaţă privată (BBC.co.uk, 6.05.2015).

## Referinţe bibliografice:

1. Brown, Ian (2010). *Communications Data Retention in an Evolving Internet*, *International Journal of Law and Information Technology*, Vol 19, No 2.
2. De Vries, Katja, Bellanova, Rocco, De Hert, Paul, and Gutwirth, Serge (2011). *The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn't it ?)* in Gutwirth, S., Poullet, Y., De Hert, P. & Leenes, R. (eds.) *Privacy and data protection: an element of choice*. Springer, 3-24, disponibil la http://works.bepress.com/serge_gutwirth/53, Accesat 15.01.2015.
3. Directiva 2006/24/EC amendând Directiva 2002/58/EC, disponibilă la http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, Accesat 7.01.2015.
4. European Court of Justice, *Digital Rights Ireland Ltd* (C293/12) *v. Minister for Communications, Marine and Natural Resources, 8.04.2014* disponibil la http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=125076 Accesat 15.01.2014.
5. European Court of Justice, *Ireland v. European Parliament and Council of the European Union,* disponibil la http://curia.europa.eu/juris/document/

document.jsf?text=&docid=72843&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=190003, Accesat 15.01.2015.
6. Ganj, Cristian (2009). *The Lives of Other Judges: Effects of the Romanian Data Retention Judgmen*t. Disponibil pe SSRN: http://ssrn.com/abstract=1558043 or http://dx.doi.org/10.2139/ssrn.1558043, Accesat 15.01.2015.
7. Guarino, Alessandro (2014). What Now? Data Retention Scenarios after ECJ Ruling, in Reimer, Helmut, Pohlmann, Norbert, Schneider, Wolfgang (eds.), *ISSE 2014 Securing Electronic Business Processes,* Springer Vieweg, 249-255, disponibil la http://www.academia.edu/7998655/What_now_Data_retention_in_the_EU_after_the_ECJ_ruling, Accesat 15.01.2015.
8. Guild, Elspeth and Carrera, Sergio (2014). *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive*. CEPS Liberty and Security in Europe Papers No. 65. Disponibil la SSRN:http://ssrn.com/abstract=2445901, Accesat 15.01.2015.
9. Kosta, Eleni (2013). *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, SCRIPT-ed 10/2013; 10(3):339. DOI: 10.2966/scrip.100313.339, http://script-ed.org/wp-content/uploads/2013/10/kosta.pdf, Accesat la 15.01.2015.
10. Legea 298/2008. Disponibilă la http://www.cdep.ro/proiecte/2008/400/30/9/pr439_08.pdf, Accesat 15.01.2015.
11. Legea 82/2012, disponibilă la http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-nr822012-privind-retinerea-datelor.html, Accesat 15.01.2015.
12. *Luxembourg Weekly*, 17.05.2014, *Reflections on EU law and CJEU jurisprudence,* disponibil la http://luxembourgweekly.blogspot.ro/2014/05/c29312-and-c59412-digital-rights.html, Accesat 15.01.2015.
13. Rauhofer, Judith and Mac Sithigh, Daithi (2014). *The Data Retention Directive that Never Existed*. SCRIPTed, 2014, 11(1); *Edinburgh School of Law Research Paper,* No. 2014/34. Disponibil la SSRN: http://ssrn.com/abstract =2467244, Accesat 15.01.2015.
14. *Decizia Curţii Constituţionale a României 440/2014*, Disponibilă la http://www.legi-internet.ro/jurisprudenta-it-romania, Accesat 15.01.2015.
15. *Decizia Curţii Constituţionale a României 1258/Octombrie 2009*, disponibilă la http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html, Accesat 15.01.2015.
16. *Decizia Curţii Constituţionale a României 461/16th Septembrie 2014*, disponibilă la http://www.ccr.ro/files/products/Decizie_461_2014.pdf, Accesat 15.01.2015.
17. BBC.co.uk, 6.05.2015, *French parliament approves new surveillance rules*, disponibil la http://www.bbc.co.uk/news/world-europe-32587377, Accesat 6.05.2015.