POLICY BRIEF

Diferențe grave de agendă: dezbaterea antiterorism în România și în UE

CRPE Policy Brief nr. 36 / Februarie 2015

Autori: Cristian Ghinea, Alexandru Damian

După fiecare atentat care a zguduit conştiinţa publică, a existat o tendinţă de a accelera procesul de cooperare şi unificare a legislaţiei antiteroriste în UE - fără a ignora însă realitatea că domeniul justiţie şi afaceri interne (JAI) rămâne unul în esenţă interguvernamental.

După atacurile de la 11 septembrie au apărut Mandatul European de Arestare și agenția de cooperare judiciară a UE - EUROJUST. Atacul de la Madrid din 2005 a dus la adoptarea primei strategii europene anti-terorism[1]. Iar după atentatul de la metroul din Londra, guvernul britanic și-a propus, în cele șase luni când urma să dețină Președinția Consiliului, adoptarea unei decizii europene privind unificarea modelelor de reținere a datelor de comunicații . Deși Londra dorea adoptarea unei decizii cadru a Consiliului, deci doar o armonizare între ministerele de Interne a regulilor din fiecare țară, Comisia și Parlamentul European au forțat atunci adoptarea unei directive. Așa a început în 2006 epopeea directivei privind reținerea datelor, poreclită de presa românească directiva Big Brother și apoi legea Big Brother 1, epopee încheiată la nivel european abia în 2014 cu o decizie de respingere la Curtea Europeană de Justiție.

Deci politica antitero a UE este în mod tradițional marcată de momentele cu mare încărcătură emoțională. Totuși, anumite elemente rămân constante în angrenajul instituțional:

- la nivel de Consiliu, miniștrii de Interne din Consiliul JAI domină agenda, ceea ce face ca în mod sistematic Consiliul să aibă o poziție foarte favorabilă agențiilor polițienești și de securitate.
- Parlamentul European obișnuiește să pună frână inițiativelor Consiliului, ridicând de obicei obiecții privind apărarea vieții private și a datelor personale. În cadrul Parlamentului, Comisia de Libertăți Civile, Justiție și Afaceri Interne (LIBE) face agenda și imprimă o traiectorie liberală dezbaterilor parlamentare.
- După ce Consiliul o mandatează să facă o propunere legislativă, Comisia Europeană face de obicei un

1. Camino Mortera-Martinez, "After Paris: What's next for the EU's counter-terrorism policy?", Center for European Reform, Londra, 27 ianuarie 2015

joc complex de căutare a echilibrului, astfel încît propunerea să conţină ideile Consiliului JAI, dar să şi aibe şanse de a întruni o majoritate parlamentară. Mai rar, Comisia respinge chiar ideea de a iniţia legislaţie (cum a fost cazul cu ideea de a reglementa la nivel UE înregistrarea cartelelor pre-pay).

Toate aceste jocuri instituţionale fac să treacă perioade destul de lungi între momentul în care guvernele exprimă dorinţa unei reglementări la nivel european şi decizia finală de a legifera. Complicatul joc instituţional european asigură şi că emoţia stârnită de atentate nu se transferă în măsuri pripite. Partea proastă este că unele state membre adoptă legislaţie sub imperiul urgenţei, ceea ce face ca diferenţele legislative între state să crească constant în domeniul antiterorism, în loc să scadă. După Paris, Marea Britanie şi Belgia au adoptat deja măsuri de izolare / ridicare a cetăţeniei potenţialilor teroriști, măsuri care nu au şanse de a fi urmate curând de legislaţie similară la nivel european (şi, de fapt, măsurile sunt atât de dure încât nu ar trece niciodată prin Parlamentul European).

După atentatul de la Paris din ianuarie 2015, frenezia propunerilor din Consiliu a reînceput. Au fost câteva momente cheie în scurta perioadă care a trecut de la atentatul din Paris: chiar în ziua marşului internaţional al solidarităţii, la care au participat şefii de state adunaţi la Paris, miniștrii de Interne din 14 state membre[2] dădeau publicităţii o declaraţie cu câteva propuneri de legiferare la nivel european. Acestea aveau să fie reluate după o reuniune informală a Consiliului JAI în 29 - 30 ianuarie (Declaraţia de la Riga)[3], care a pregătit reuniunea şefilor de state în Consiliul European informal, din 12 februarie.

Declaraţia[4] de după această reuniune rezumă direcţiile principale pe care s-a căzut de acord între şefii de state şi de guverne, care constituie cele mai probabile puncte ale viitoarei activităţi de legiferare. Declaraţia stabileşte trei direcţii principale: măsuri comune de securitate, prevenirea radicalizării şi cooperare internaţională - fiecare cu subpuncte, din care le vom rezuma pe cele mai importante, urmând ca în capitolele următoare să detaliem istoricul unora dintre aceste măsuri:

1) în ce priveşte asigurarea securităţii cetăţenilor: adoptarea rapidă a Directivei privind schimbul de informaţii despre pasagerii liniilor aeriene; îmbunătăţirea cooperării în sistemul Schengen pentru controlul indivizilor care prezintă riscuri de securitate, pe baza unor indicatori comuni de risc, care urmează a fi definiţi de către Comisia Europeană; îmbunătăţirea cooperării în cadrul Europol şi Eurojust; îmbunătăţirea cooperării între serviciile de securitate din statele membre; adoptarea rapidă a directivei privind securitatea cibernetică.

2) în ce priveşte prevenirea radicalizării textul declaraţiei este destul de vag, îndeamnă la cooperarea statelor pentru a dezvolta strategii comprehensive pentru a evita ca proprii cetăţeni să fie atraşi în orbita reţelelor teroriste (iniţiative de informare şi educare).

3) în ce priveşte cooperarea cu partenerii internaţionali se declară intenţia UE de a lucra, prin serviciul diplomatic european, împreună cu statele din Orientul Mijlociu, Africa de Nord şi subsahariteană contra reţelelor teroriste.

Paşii următori stabiliţi de declaraţie: Consiliul va reveni asupra chestiunilor antiteroriste în iunie, iar Comisia va propune o strategie antitero până în aprilie.

Sunt câteva observaţii care se cer făcute după acest Consiliul European:

Ucraina a eclipsat antiterorismul

Acest Consiliu European informal a fost convocat cu scopul de a agrea noi măsuri antiteroriste, după evenimentele de la Paris. Dar între Paris şi 12 februarie, agenda liderilor a fost acaparată de alte urgenţe. Angela Merkel şi Francois Hollande au venit direct de la Minsk, unde terminaseră negocierile cu Vladimir Putin privind situaţia din Ucraina. Atenţia presei a fost acaparată complet de subiectul Ucraina şi declaraţiile liderilor europeni dinainte şi de după Consiliu au fost aproape toate despre Ucraina. Deşi s-a dorit ca, prin această reuniune, subiectul ”antiterorism”să fie ridicat la cel mai înalt nivel de decizie, de fapt nu s-a întâmplat asta, iar liderii au agreat un text despre măsurile antiterorism evident pregătit dinainte.

2. Letonia, Germania, Austria, Belgia, Danemarca, Austria, Germania, Belgia, Spania, Italia, Olanda, Polonia, Marea Britanie și Suedia.

3. “Declaraţia comună în urma reuniunii informale a miniștrilor Justiţiei şi Afacerilor Interne în Riga pe 29 şi 30 ianuarie 2015”

4. ”Declaraţia membrilor Consiliului European după Reuniunea informală din 12 februarie 2015”, publicată pe site-ul Consiliului, analiza a fost făcută direct pe versiunea în engleză.

Cele mai multe idei post-Paris s-au pierdut pe drum

După atentatele de la Paris au circulat multe idei despre care ar trebui să fie reacţia UE. Unele dintre ele erau panicarde, altele foarte îndrăznețe. De pildă, ministrul spaniol de Interne a propus reintroducerea controalelor la frontiere în interiorul spaţiului Schengen pentru a opri indivizii periculoşi. Potrivit unor relatări din presă, Spania şi Franţa au menţinut această propunere şi în 12 februarie, dar ea a fost respinsă de ceilalţi lideri. O altă idee care a circulat a fost crearea unui serviciu secret european. În acest moment, UE dispune de un centru analitic de intelligence[5] în cadrul serviciului diplomatic european - are 70 de angajaţi, nu dispune de agenţi în teren, lucrează doar cu surse deschise şi cu informaţii trimise benevol de serviciile secrete ale statelor membre. Ideea creării unui adevărat serviciu secret european a murit în faţa obstacolelor juridice: nu există bază în Tratat şi nici voinţă politică pentru o discuţie pe termen lung asupra subiectului.

Propuneri care au pierdut din anvergură

Din ideea unui serviciu secret european a rămas în declaraţia din 12 februarie doar un îndemn ca serviciile de securitate naţionale să coopereze mai bine. Probabil nu se va alege mare lucru din acest îndemn, pentru că serviciile secrete tind să trateze informaţia ca pe un bun de valoare care îşi pierde din această valoare în caz de punere la comun. Experienţele recente cu scurgeri masive de date de la serviciile secrete americane (scandalurile Snowden, Wikileaks) au fost interpretate în comunitatea de securitate ca fiind urmările nefaste ale iniţiativelor americane post 9/11: acuzate că nu au oprit atentatele din cauză că nu au împărtăşit între ele secretele deţinute, agenţiile americane au pus informaţiile în baze de date cu acces larg. Asta a făcut ca scurgeri de informaţii care în trecut rămâneau minore să aibă în prezent dimensiuni catastrofice, pentru că oficiali de rang minor sau chiar contractori externi (ca Snowden) au acces la informaţii mult peste ce le e necesar în activitatea de bază. Lecţia trasă de serviciile secrete, inclusiv cele europene, este: cu cât împărtăşeşti mai multă informaţie cu atât mai mare va fi efectul unei scurgeri, deci mai bine să nu riscăm. Un simplu îndemn al liderilor europeni,

5. Centrul de Analiză a Informaţiilor (EU INTCEN)

> *„După atentatul de la Paris din ianuarie 2015, frenezia propunerilor din Consiliu a reînceput.*

fără măsuri concrete legislative, nu va schimba optica reticentă a serviciilor fiecărui stat faţă de punerea la comun a informaţiilor.

În mod similar s-au pierdut pe drum şi ideile de schimbare a tratatului Schengen. Declaraţia post-Consiliu vorbeşte strict de îmbunătăţirea folosirii sistemului Schengen aşa cum este el în prezent. Aici a fost importantă şi reticenţa exprimată public de Comisie faţă de propunerile spaniole şi franceze. În viziunea Comisiei, statele membre nu folosesc suficient mecanismele de care dispun. Sistemul Schengen permite statelor să pună pe lista de avertizare anumiţi indivizi atunci când vin din afara spaţiului Schengen - urmând a fi urmăriţi de serviciile poliţieneşti ale celorlalte state în care intră ulterior şi care vor fi automat informate. Însă există diferenţe mari în modul de activare a listei de avertizare, cu alte cuvinte nu există proceduri unice de a determina cine prezintă un risc. Declaraţia însărcinează Comisia să propună aceste proceduri unice. Asta este departe de a reinstitui controale la frontiere, aşa cum s-a vorbit iniţial.

Un nou suflu pentru directivele blocate în PE

Declaraţia liderilor UE oferă sprijin politic pentru două directive care au fost întârziate / blocate în Parlamentul European: cea privind schimbul de informaţii privind pasagerii aerieni şi cea privind securitatea cibernetică.

Vom reveni asupra acesteia din urmă, pentru că România s-a grăbit să legifereze domeniul înainte de a avea adoptată directiva europeană, dar a făcut-o într-o formă respinsă deja de Curtea Constituţională.
Directiva privind registrul pasagerilor companiilor aeriene (PNR) prevede crearea unei baze de date comune care să conţină nume, adrese, numere de paşaport, informaţii privind cardurile de credit sau rute de călătorie ale pasagerilor. A fost propusă încă din 2011 şi respinsă de către LIBE în aprilie 2013.

Însă situaţia din Irak - Siria, mai ales în ce priveşte cetăţenii europeni care merg să lupte acolo, a readus subiectul pe agenda PE, chiar înainte de atacurile de la Paris. Raportul Europol privind combaterea terorismului în UE[6] semnalează creşterea acestui pericol începând cu 2013. Astfel încât chiar raportorul LIBE asupra directivei anunţa în noiembrie 2014 „creşterea ameninţării la nivelul UE în comparaţie cu situaţia de acum un an" (când propunerea de directivă fusese respinsă)[7]. Desigur că evenimentele de la Paris au dat un nou impuls, motiv pentru care tema acestei directive apare în declaraţia din 12 februarie.

Pe de altă parte, ideea păstrării datelor pasagerilor este complicată de respingerea de către Curtea Europeană de Justiţie a Directivei privind reţinerea datelor de telecomunicaţii. Curtea a impus limite stricte pentru acces, limite care vor fi valabile şi pentru accesul la datele pasagerilor. La momentul actual, un nou raport privind PNR este aşteptat la sfârşitul lunii februarie, care urmează să ţină cont de efectele respingerii Directivei privind reţinerea datelor şi eventuala necesitate de a încorpora mai multe măsuri privind protecţia datelor personale.

De remarcat că înainte de reuniunea Consiliului European, Parlamentul s-a grăbit să voteze în 11 februarie (cu majoritate largă) o rezoluţie[8] prin care a transmis voalat limitele pe care ar urma să le accepte în viitoarea reglementare. Rezoluţia (propusă de un grup de europarlamentari de la mai multe grupuri politice, între care din România Cristian Preda, Monica Macovei, Traian Ungureanu şi Daniel Buda) exclude orice propunere care ar suspenda libertăţile de circulaţie Schengen şi în schimb îndeamnă la o mai bună folosire a sistemului informatic Schengen (care în esenţă e şi ideea rămasă la final în declaraţia Consiliului); spune că orice legiferare privind colectarea de date trebuie să respecte legislaţia europeană privind protecţia datelor; subliniază că politicile antiteroriste şi de securitate (servicii secrete) trebuie să lucreze sub "supraveghere democratică total independentă".

Strategia preventivă a PE a avut efect, iar declaraţia şefilor de state a ţinut cont de limitele indicate de europarlamentari.

Pentru România, punctele 2 (prevenirea radicalizării) şi 3 (cooperarea internaţională) din declaraţia Consiliului European prezintă un interes limitat. Nu au fost semnalate cazuri de cetăţeni români care au plecat să lupte în Siria/ Irak. Au existat în ultimii ani semnale de la liderii comunităţii musulmane tradiţionale din România (concentrată în Dobrogea) că există clerici radicali care au început să atragă tinerii de credinţă islamică (mai ales urmaşii foştilor studenţi arabi rămaşi în România), dar fenomenul e departe de dimensiunile avute în ţările mai sus pomenite. Deci această dezbatere interesează România doar pentru viitorul mediu său îndepărtat.

Măsurile de la primul punct sunt însă de interes, mai ales din perspectiva recentelor dezbateri interne privind aşa numitele legi "Big Brother".

Dintre cele trei legi "Big Brother"[9], doar prima dintre ele a avut ca motivaţie transpunerea unei directive europene - Directiva privind retenţia datelor, cea iniţiată de Guvernul britanic după atentatele din metroul londonez din 2005. Însă şi celelalte două au conexiuni interesante - şi neaşteptate - cu legislaţia europeană.

6. Europol, "Raportul Europol privind situaţia şi tendinţele terorismului în Uniunea Europeană", 2014

7. Timothy Kirkhope, raportor al Comisiei pentru Libertăţi Civile, Justiţie şi Afaceri interne privind propunerea de directivă a Parlamentului European şi a Consiliului privind utilizarea datelor din registrul cu numele pasagerilor pentru prevenirea, depistarea, cercetarea şi urmărirea penală a infracţiunilor de terorism şi a infracţiunilor grave, în cadrul reuniunii Comisiei LIBE din noiembrie 2014

8. "Rezoluţia Parlamentului European privind măsuri antiteroriste", 11 februarie 2015, Strasbourg, adoptată cu 532 voturi pentru, 136 împotrivă şi 36 de abţineri

9. Pentru o descriere a acestor legi, a se vedea articolele "Care e faza cu Big Brother?", apărut in Dilema Veche nr. 572 şi "Concluzii la dezbaterea Big Brother - Cine are dreptate?", apărut in Dilema Veche nr. 573, autor: Cristian Ghinea.

Politica antitero a UE şi efectele asupra legislaţiei interne din România

Legislaţie românească	Echivalent în legislaţia comunitară	Stadiul legislaţiei comunitare în domeniu
Legea retenţiei datelor (Big Brother 1)	Da, directivă adoptată în 2006	Directiva Respinsă de Curtea Europeană de Justiţie Legea de transpunere respinsă de două ori de CCR
Legea înregistrării cartelelor pre-pay şi a reţelelor wi-fi (Big Brother 2)	Nu	A existat o propunere de a crea legislaţie europeană doar pentru cartelele pre-pay, Comisia a respins propunerea
Legea securităţii cibernetice (Big Brother 3)	Nu încă, se află în dezbatere.	Propunerea se află în dezbatere în PE. Legea românească nu respecta forma de directivă care a trecut de Parlamentul European; CCR a respins legea.

Big Brother 1 - reţinerea datelor de comunicaţii

Curtea Constituţională din România (CCR) a respins în 2009 prima lege de transpunere şi a fost confirmată în opţiunea sa de Curtea Europeană de Justiţie în 2014. Ulterior deciziei curţii din Luxemburg, CCR a respins cu unanimitate de voturi şi a doua lege de transpunere a directivei[10].

Este interesant că respingerea directivei de către Curtea Europeană nu anulează automat legile de transpunere votate de Parlamentele naţionale, rămânând la latitudinea statelor membre să-şi stabilească paşii următori. Scopul iniţial al acestei directive era de a unifica regulile de reţinere a datelor de către companiile din domeniu. Acest scop a fost atins prin legile de transpunere. Chiar după desfiinţarea directivei, scopul rămâne atins, cu excepţia statelor membre unde legea naţională este explicit desfiinţată de instanţe sau de Curtea Constituţională - cum e cazul României. Cazul Marii Britanii e special: guvernul de la Londra a decis după respingerea directivei să implementeze un nou set de legi la nivel naţional - "DRIPA" (Data Retention and Investigatory Powers Act 2014). Legile au stârnit proteste din cauza adoptării rapide (trei zile), ce nu a lăsat loc niciunei dezbateri consistente.

Big Brother 2 - cartele pre-pay si reţelele wi-fi

Dezbaterea europeană privind înregistrarea utilizatorilor de cartele pre-pay a precedat-o pe cea românească, fiind o prelungire a discuţiilor ce au urmat implementării de către statele membre a directivei privind păstrarea datelor. În 2011, creşterea numărului de state membre care au adoptat măsuri care necesită înregistrarea cartelor (Danemarca, Spania, Italia, Grecia, Slovacia şi Bulgaria, măsură susţinută ulterior şi de Polonia, Cipru, Lituania) a determinat Comisia Europeană să evalueze necesitatea acţiunii la nivelul UE. Principalul argument pentru reglementarea unui cadru european s-a axat pe posibilitatea cumpărării unei cartele preplătite dintr-un alt stat membru şi utilizarea sa cu scopul comiterii de infracţiuni, fără posibilitatea identificării persoanei în cauză[11]. Curios e că România nu s-a numărat atunci printre ţările care au susţinut necesitatea adoptării unor măsuri la nivelul UE.
Ulterior discuţiilor, Comisia nu a fost convinsă de neces-

10. Curtea Constituţională a României, DECIZIA nr.440 din 8 iulie 2014 referitoare la excepţia de neconstituţionalitate a dispoziţiilor Legii nr.82/2012 privind reţinerea datelor generate sau prelucrate de furnizorii de reţele publice de comunicaţii electronice şi de furnizorii de servicii de comunicaţii electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice şi ale art.152 din Codul de procedură penală".

11. Comisia Europeană, "Raport de evaluare a Directivei privind păstrarea datelor", Aprilie 2011

itatea de a acționa în această privință[12]. În România, discuțiile privind înregistrarea utilizatorilor de cartele SIM preplătite, apărute în spațiul public în urma atentatului din iulie 2012 din Bulgaria în care atentatorii au folosit asemenea cartele, s-au concretizat în urma modificării ordonanței de Guvern din 2011 (OU111/2011) privind comunicațiile electronice, decizie adoptată ulterior de Parlament în iulie 2014. În plus față de dezbaterea de la nivelul UE, România a adăugat obligația operatorilor de rețele wi-fi publice să solicite și să stocheze datele personale ale utilizatorilor.

Curtea Constituțională a respins însă și această lege în septembrie 2014. Imediat după atacul de la Paris, a fost convocată de către ministrul de Interne Gabriel Oprea o ședință comună a Grupului Interministerial Strategic pentru prevenirea și combaterea macrocriminalității și a Comitetului Național pentru Situații Speciale de Urgență, având pe ordinea de zi "necesitatea asigurării instrumentarului normativ necesar structurilor din domeniul securității naționale"[13]. După aceste denumiri complexe și limbaj greoi se întrevede folosirea Parisului ca oportunitate de a relua legile respinse de Curte, fără a pleca de la oferirea de soluții pentru problemele semnalate în decizia de respingere.

Big Brother 3 - securitatea cibernetică

Forma legii securității cibernetice adoptate de Parlamentul la 19 decembrie 2014 vine în flagrantă contradicție cu direcția în care mergea dezbaterea la nivel european. E interesant că în cazul respingerii acestei legi (decizia CCR nr. 17/2015) Curtea din Romăna invocă o formă a directivei europene care nu e finală, ci e forma votată de Parlamentul European. Considerăm acesta un precedent de bun augur: dezbaterile legislative din România trebuie să țină cont de cele din UE, care vor fi aplicabile României în viitorul imediat.

Diferența majoră constatată de Curte între directiva NIS și legea securității cibernetice se referă la autoritățile de coordonare în materie de securitate cibernetică. În ultima variantă a directivei, cea adoptată de PE în martie 2014, acestea sunt prevăzute ca fiind organisme civile, sub completă supraveghere democratică[14]. Legea Securității Cibernetice prevede ca autoritate națională în domeniul securității cibernetice Serviciul Român de Informații, iar ca punct de contact Centrul Național de Securitate Cibernetică, aflat în componența SRI-ului[15].

Este greu de înțeles de ce guvernul României propune în mai 2014 și parlamentul votează în decembrie 2014 o lege care face din SRI instituție de coordonare când PE votase în martie 2014 faptul că statele membre ar trebui să dea acest rol unor instituții civile.

Câteva concluzii - Big Brother și legislația europeană

Toate dezbaterea privind accesul statului la comunicații privește două aspecte: a) colectarea datelor și b) accesul organelor de stat la datele colectate. În ambele aspecte există chestiuni aflate în dezbatere, dar esențial este să știm că din perspectiva pro-rule of law se dorește păstrarea tuturor datelor pentru toți cetățenii și un acces cât mai larg la acestea. Din perspectiva pro-privacy se dorește o targetare a colectării pentru focus asupra indivizilor cu risc și restrângerea accesului la date (pe o perioadă limitată, doar pentru infracțiuni foarte grave, doar anumite instituții).

Directiva privind reținerea datelor (Big Brother 1) a încercat să găsească un echilibru între aceste două perspective. De pildă, perioada de reținere a datelor a fost redusă în PE față de cererea inițială a Consiliului JAI. Cum însă subiectul era controversat și nu existau posibilități de consens între PE și Consiliu, Președinția britanică a negociat cu PE soluția de a lasă foarte multe aspecte de implementare la latitudinea statelor membre. Astfel, puncte cheie precum lista de infracțiuni pentru care statul capătă acces la date, instituțiile care au acces și procedura concretă constituie decizie a fiecărui stat (art. 4). Această chestiune s-a dovedit a fi crucială pentru traseul legii în România.
Decizia CCR are două componente majore: a) preia argumentația Curții Europene de Justiție din decizia de respingere a directivei omonime și b) respinge modul în care a reglementat Parlamentul mecanismul de acces la

12. Idem

13. Comunicat al Ministerului Afacerilor Interne, 08 ianuarie 2015

14. Amendamentul 11, Considerentul 10 a (nou), Rezoluția legislativă a Parlamentului European din 13 martie 2014 referitoare la propunerea de directivă a Parlamentului European și a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune

15. Articolul 10(1), Articolul 10(4), Legea Securității Cibernetice, adoptată de Parlament la 19 Decembrie 2014

date în cazul serviciilor secrete.

Decizia Curţii Europene de Justiţie critică directiva pentru că nu oferă mecanisme de protecţie a datelor personale şi prevede praguri atât de înalte de protecţie a vieţii private încât e de înţeles de ce ideea de a re-vota o nouă Directivă în domeniu nu e foarte atractivă (apare ca propunere în documentul pregătit de European Counter-Terrorism Coordinator înainte de reuniunea de la Riga[16], dar nu a fost preluată nici în declaraţia JAI de la Riga, nici în declaraţia Consiliului European din 12 februarie). Curtea Europeană a înclinat balanţa foarte mult în direcţia pro-privacy şi cel mai probabil nu va mai există reglementare unitară europeană în domeniu.

CCR a preluat ca atare argumentele Curţii Europene în ceea ce priveşte primul punct. Dar cel mai important aspect al deciziei Curţii din România a fost cel privind accesul la date. Judecătorii constituţionali consideră că s-a creat prin legea de transpunere un regim diferenţiat de acces: organele judiciare o fac cu mandat de la judecător, în vreme ce serviciile secrete nu au această restricţie. Pentru a ajunge la acest argument, Curtea constată că legea Big Brother 1 nu precizează modul în care serviciile secrete accesează datele, ci face doar referire la legile speciale ale serviciilor (legea securităţii naţionale din 1991, legea de organizare a SRI din 1992 şi legea SIE din 1998).

Analizând aceste legi speciale, Curtea dovedeşte că ele permit serviciilor secrete să acţioneze fără restricţii din partea puterii judecătoreşti atunci când acţiunilor lor pot aduce atingere drepturilor fundamentale. Practic, asistăm la un caz spectaculos în care presiunea europenizării ajunge indirect într-o zonă gri ce nu a fost rezolvată de la începuturile tranziţiei româneşti: controlul civil asupra serviciilor secrete. Statul român a folosit prerogativa de a decide la nivel naţional modalităţile de acces la datele de telecomunicaţii pentru a prelungi o excepţie paralegală creată pentru serviciile secrete. Interesant este că până să trebuiască să transpună directiva europeană, România nu avea nici un fel de reglementare în materie. Există însă dovezi anecdotice că SRI obligă (pentru a le acorda avize) companiile de telecomunicaţii să îi permită acces direct la serverele unde se păstrau aceste date. Deci legea Big Brother 1, chiar aşa permisivă cu SRI, a pus cel puţin bazele unui cadru legal în domeniu. După decizia Curţii, Parlamentul e obligat să restrângă acest cadru şi să aducă serviciile secrete la ordine. Din păcate, instituţia care ar trebui să facă acest lucru refuză sistematic acest rol. Controlul parlamentar asupra serviciilor secrete este cu totul necredibil şi disfuncţional în România.

Comisia parlamentară de control a SRI ar trebui să informeze opinia publică care era regimul de acces al SRI la datele de telecomunicaţii înainte de adoptarea legii de transpunere a directivei, care au fost mecanismele create în perioadă în care legea a fost în vigoare (a retras SRI legătură la servere?) şi care este situaţia în acest moment, când legea a fost declarată neconstituţională. De pildă, ar trebui să ştim clar că respingerea legii la Curte nu a reîntors situaţia din teren la faza iniţială (acces nelimitat şi nereglementat) al SRI la serverele de comunicaţii.

Problema implicării neavenite a serviciilor de informaţii devine şi mai explicită în cazul legii securităţii cibernetice (Big Brother 3). Practic, adoptarea Big Brother 3 reprezintă o măsură preventivă ca răspuns la iminenta adoptare a Directivei NIS care presupune în ultima sa formă desemnarea unei entităţi civile ca autoritate naţională în materie. Altă explicaţie nu găsim dilemei mai sus amintite: de ce decide România să ofere rolul de coordonator către SRI după ce PE a decis că statele membre sunt obligate să desemneze o instituţie civilă.

Şi mai absurd e că entitatea civilă de care se vorbeşte în ultima formă a Directivei NIS are deja un corespondent în România: Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), creat în 2011, în coordonarea Ministerului Comunicaţiilor. În mod evident, CERT-RO este o instituţie mai potrivită să se ocupe de coordonarea domeniului după adoptarea directivei NIS, deşi ne însuşim punctul de vedere exprimat de APTI că CERT-RO ar trebui reformat pentru a fi deplin compatibil cu directiva, deoarece în comitetul său de coordonare intră instituţii militarizate (MAN, SRI)[17].
Dacă în cazul Big Brother 1 avem un efect colateral al reglementării la nivel european - CCR a ajuns prin analiza legii de transpunere să critice excepţia paralegală a serviciilor de informaţii - în cazul Big Brother 3 vorbim despre o lovitură legislativă preventivă a SRI, care a iniţiat proiectul de lege prin care şi-a arogat statutul de instituţie coordonatoare înainte de a intra în vigoare directiva europeană care i-ar interzice în mod expres să ocupe acesta poziţie.

16. Center for European Policy Studies, "The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda"; CEPS Paper nr. 81 din februarie 2015

17. Asociaţia pentru Tehnologie şi Internet, "Opinia ApTI cu privire la Proiectul de lege privind securitatea cibernetică", 11 iunie 2014.

Despre autori:

Cristian GHINEA este directorul Centrului Român de Politici Europene şi coordonează proiecte în domeniul politicii externe, justiţiei şi anticorupţiei. Este absolvent de Ştiinţe Politice şi a studiat guvernare europeană la London School of Economics (2007 – 2008). Este autorul volumului „Eu votez DNA – De ce merită să apărăm instituţiile anticorupţie" apărut la Editura Humanitas în 2012 şi scrie de peste 15 ani editoriale pentru revista "Dilema Veche".

Alexandru DAMIAN este cercetător în cadrul Centrului Român de Politici Europene, având ca domenii de interes politica externă şi de securitate a UE, respectiv domeniul justiţiei şi lupta anticorupţie. Este licenţiat în Ştiinţe Politice şi a urmat un Masterat axat pe Studii de Securitate în cadrul Universităţii Libere din Bruxelles.

Acest Policy Brief a fost elaborat în cadrul proiectului Influenţi, alerţi şi informaţi în negocierile din UE – Expertiză şi consultare în politici europene finanţat prin granturile SEE 2009 – 2014, în cadrul Fondului ONG în România; Pentru informaţii oficiale despre granturile SEE şi norvegiene accesaţi www.eeagrants.org;

SRAC Certificat Nr.9532 ISO 9001

Centrul Român de Politici Europene, 2015
Stirbei Voda 29, Cod postal, 010101 Bucureşti
www.crpe.ro/en
Contact: Telefon +40 371 083 577, Fax +40 371 875 089