STUDIA UNIVERSITATIS MOLDAVIAE, 2014, nr.8(78)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.35-45

INVALIDAREA DIRECTIVEI 2006/24 CE DE CĂTRE CURTEA DE JUSTIȚIE A UNIUNII EUROPENE – DECIZIE-BOMBĂ ÎN FAVOAREA PROTECȚIEI DREPTURILOR OMULUI

Natalia SUCEVEANU

Universitatea de Stat din Moldova

Protecția datelor personale este astăzi, mai mult ca niciodată, un subiect de actualitate în dreptul Uniunii Europene. Hotărârea emisă la 8 aprilie 2014 de către Curtea de Justiție a Uniunii Europene (CJUE) în două cauze conexate (C-293/12 şi C-594/12 *Digital Rights Ireland Ltd* împotriva *Minister of Communications, Marine and Natural Resources, Minister of Justice, Equality and Law Reform, Commissioner of the Garda Siochana*) declară nevalidă Directiva 2006/24/CE a Parlamentului European şi a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice. Chiar dacă Curtea de Justiție estimează că retenția datelor în legătură cu furnizarea serviciilor de comunicații electronice poate constitui un instrument util în lupta împotriva anumitor infracțiuni grave, cum ar fi terorismul, ea stabileşte în egală măsură că această conservare a datelor constituie o ingerință foarte amplă şi deosebit de gravă în viața privată a indivizilor, care, chiar şi justificată, este una disproporționată. După invalidarea Directivei 2006/24 CE de către Curtea de Justiție ca urmare a violării principiului proporționalității în lumina articolelor 7, 8 şi 52 parag. 1 ale Cartei, Comisia şi noul Parlament European vor fi obligate să procedeze la o rescriere a Directivei. Decizia CJUE luată pe 8 aprilie este una de referință pentru legislația drepturilor omului. Această decizie este, probabil, cea mai importantă hotărâre a CJUE cu privire la drepturile omului, deoarece este prima care invalidează o directivă pentru încălcarea drepturilor omului prevăzute în Carta drepturilor fundamentale a UE.

Cuvinte-cheie: *Curtea de Justiție a Uniunii Europene, Carta drepturilor fundamentale a Uniunii Europene, Directiva 2006/24 CE, păstrarea datelor personale, securitatea datelor, dreptul la protecția datelor cu caracter personal, dreptul la viață privată, dreptul la libertatea de exprimare, principiul proporționalității, ingerință, transpunere, implementare, invalidare.*

INVALIDATION OF THE DIRECTIVE/2006/24/EC BY THE COURT OF JUSTICE OF THE EUROPEAN UNION – A BOMB DECISION IN FAVOUR OF HUMAN RIGHTS' PROTECTION

Protection of personal data more than ever constitutes a subject matter referred to the topicality in the context of law of the European Union. The judgment issued by the Court of Justice of the European Union (CJEU) on 8th of April 2014 in two joined cases (C-293/12 and C-594/12 *Digital Rights Ireland Ltd* v *Minister of Communications, Marine and Natural Resources, Minister of Justice, Equality and Law Reform, Commissioner of the Garda Siochana,* invalidated the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks. Albeit the Court of Justice estimates that the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks can represent an useful tool against serious crimes, such as terrorism, it also establishes that, this data retention represents a wide-range and particularly serious interference into private life, which even justified, is one disproportionate. Following the Court's invalidation of the Directive 2006/24/EC, as result of the infringement of the principle of proportionality in the light of the articles 7, 8 and 52 para. 1 of the Charter, Commission and the new European Parliament will be bounded to write back the Directive. The Court's decision from 8th of April is a landmark judgment for the human rights' legislation. This decision is likely the most important judgment of the CJUE regarding human rights, in respect that is the first one, which invalidates a directive for the infringement of the human rights established in the Charter of Fundamental Rights of the European Union.

Keywords: *Court of Justice of the European Union, Charter of Fundamental Rights of the European Union, Directive 2006/24/EC, personal data retention, data security, right to the protection of personal data, right to freedom of expression, principle of proportionality, interference, transposition, implementation, invalidation.*

Introducere

Protecția datelor personale este astăzi, mai mult ca niciodată, un subiect de actualitate în dreptul Uniunii Europene. După votarea în prima lectură la 12 martie 2014 a noului Pachet legislativ în domeniul datelor personale [1] de către Parlamentul European în vechea sa componență, Curtea de Justiție, la rândul său, s-a

pus în apărarea dreptului fundamental la viaţa privată şi la protecţia datelor personale, consacrate în articolele 7 şi 8 ale Cartei drepturilor fundamentale a Uniunii Europene [2]. Hotărârea emisă la 8 aprilie 2014 de către Curtea de Justiţie a Uniunii Europene (CJUE) în două cauze conexate (C-293/12 şi C-594/12 *Digital Rights Ireland Ltd* împotriva *Minister of Communications, Marine and Natural Resources, Minister of Justice, Equality and Law Reform, Commissioner of the Garda Siochana*) [3] declară nevalidă Directiva 2006/24/CE a Parlamentului European şi a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice. Chiar dacă Curtea de Justiţie estimează că retenţia datelor în legătură cu furnizarea serviciilor de comunicaţii electronice poate constitui un instrument util în lupta împotriva anumitor infracţiuni grave, cum ar fi terorismul, ea stabileşte în egală măsură că această conservare a datelor constituie o ingerinţă foarte amplă şi deosebit de gravă în viaţa privată a indivizilor, care, chiar şi justificată, este una disproporţionată.

În primul caz (C-293/12), organizaţia irlandeză pentru apărarea drepturilor fundamentale pe internet *Digital Rights* introduce la 11 august 2006 un recurs în faţa Înaltei Curţi din Irlanda (*High Court*). Proprietara unui telefon portabil care a fost înregistrat contestă legalitatea măsurilor legislative şi administrative naţionale privind conservarea datelor în legătură cu furnizarea serviciilor de comunicaţii electronice care au transpus Directiva 2006/24 CE. Înalta Curte din Irlanda a sesizat Curtea de Justiţie a Uniunii Europene (CJUE) prin intermediul chestiunilor prejudiciale întrebând Curtea dacă măsurile dispuse prin intermediul Directivei nu sunt disproporţionate şi lipsite de necesitate în raport cu scopul lor, dacă sunt în conformitate cu anumite drepturi prevăzute de Tratatul privind Funcţionarea Uniunii Europene (TFUE) şi dacă sunt compatibile cu drepturile fundamentale garantate de Carta drepturilor fundamentale a Uniunii Europene. Curtea de Justiţie a examinat numai chestiunea referitoare la compatibilitatea Directivei 2006/24 CE cu dreptul la respectarea vieţii private (art.7 din Cartă şi art.8 CEDO), dreptul la protecţia datelor cu caracter personal (art.8 din Cartă) şi dreptul la libertatea de exprimare (art.11 din Cartă şi art.10 CEDO). Aceeaşi întrebare preliminară a fost pusă CJUE şi în cel de-al doilea caz (C-594/12) de către Curtea Constituţională a Austriei (*Verfassungsgerichtshof).*

În vederea asigurării corespunderii dreptului derivat cu dreptul primar, CJUE a punctat incompatibilitatea prevederilor Directivei. Ea declară nevalabilă Directiva 2006/24 CE, a cărei ingerinţă în drepturile fundamentale este într-adevăr justificată, însă disproporţionată, iar securitatea protecţiei datelor personale nu este garantată. Această decizie radicală a CJUE nu surprinde, având în vedere că Directiva 2006/24 CE nu a fost în general bine primită de către popoarele statelor membre, dar şi criticată ani la rând.

Istoricul Directivei 2006/24 CE

În ceea ce priveşte *păstrarea* şi *utilizarea datelor în scopul aplicării legii*, aceste măsuri au fost abordate pentru prima dată la nivelul UE de Directiva 97/66/CE din 15 decembrie 1997 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul telecomunicaţiilor. Această Directivă a prevăzut pentru prima dată, în art.14(1), *posibilitatea* ca statele membre să adopte astfel de măsuri legislative, dacă este necesar pentru protecţia securităţii publice sau a ordinii publice, inclusiv pentru bunăstarea economică a statului, atunci când activităţile se referă la securitatea statului şi la aplicarea dreptului penal. Dispoziţia respectivă a fost dezvoltată în continuare în Directiva 2002/58/CE din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice (Directiva asupra confidenţialităţii şi comunicaţiilor electronice), care prevede *posibilitatea* ca statele membre să adopte măsuri legislative care derogă de la principiul confidenţialităţii comunicaţiilor, inclusiv, în anumite condiţii, păstrarea, accesul şi utilizarea datelor în scopul aplicării legii. În temeiul articolului 15 alineatul (1), statele membre *pot* restrânge sfera de aplicare a drepturilor şi obligaţiilor în materie de confidenţialitate, inclusiv prin păstrarea datelor pentru o perioadă limitată, atunci când această restrângere constituie o măsură „necesară, corespunzătoare şi proporţională în cadrul unei societăţi democratice pentru a proteja securitatea naţională (de exemplu, siguranţa statului), apărarea, siguranţa publică sau pentru prevenirea, investigarea, detectarea şi urmărirea penală a unor fapte penale ori a folosirii neautorizate a sistemelor de comunicaţii electronice". Ca urmare a prevederilor Directivei 97/66/CE şi ale Directivei 2002/58/CE asupra confidenţialităţii şi comunicaţiilor electronice, care permit statelor membre să adopte legislaţie în materie de păstrare a datelor, operatorii din unele state membre au trebuit să achiziţioneze echipamente pentru păstrarea datelor şi să angajeze personal care să recupereze date în numele autorităţilor de aplicare a legii, în timp ce furnizorii din alte state membre nu au fost supuşi acestei obligaţii, ceea ce a cauzat denaturări pe piaţa internă. În plus, tendinţele în modelele de afaceri şi în ofertele de servicii, cum ar fi creşterea tarifelor forfetare, serviciile de comunicaţii electronice preplătite şi gratuite,

au avut drept consecinţă faptul că, treptat, operatorii au încetat să stocheze datele privind traficul şi localizarea în scopul facturării, reducând, astfel, disponibilitatea acestor date pentru justiţia penală şi în scopul aplicării legii[*].

În acest context, Directiva 2006/24/CE din 15 martie 2006 privind păstrarea datelor a impus statelor membre *obligaţia* ca furnizorii de servicii de comunicaţii electronice accesibile publicului şi de reţele de comunicaţii publice să păstreze datele de comunicaţii în scopul cercetării, detectării şi urmăririi penale a infracţiunilor grave, astfel cum au fost definite de fiecare stat membru în dreptul intern. Directiva a modificat articolul 15 alineatul (1) din Directiva 2002/58/CE asupra confidenţialităţii şi comunicaţiilor electronice, prin adăugarea unui alineat care prevede că articolul 15 alineatul (1) nu se aplică datelor păstrate în temeiul Directivei 2006/24/CE privind păstrarea datelor. Prin urmare, statele membre puteau deroga în continuare de la principiul confidenţialităţii comunicaţiilor. Directiva (privind păstrarea datelor) reglementează doar păstrarea datelor pentru scopul mai limitat de cercetare, detectare şi urmărire penală a infracţiunilor grave. Această relaţie juridică complexă între Directiva 2006/24 CE privind păstrarea datelor şi Directiva 2002/58/CE privind confidenţialitatea în mediul electronic, corelată cu lipsa unei definiţii în cele două directive a noţiunii „infracţiune gravă", au îngreuiat diferenţierea, pe de o parte, a măsurilor adoptate de statele membre în vederea transpunerii obligaţiilor în materie de păstrare a datelor prevăzute în Directiva 2006/24/CE şi, pe de altă parte, a practicii mai generale din statele membre în materie de păstrare a datelor, permisă în temeiul articolul 15 alineatul (1) din Directiva 2002/58/CE.

Directiva 2006/24/CE a constituit rezultatul unui proces de legiferare la nivel UE, care s-a desfăşurat într-un mod extrem de rapid, perioada de adoptare a Directivei fiind una dintre cele mai scurte din istoria UE – Comisia a înaintat propunerea pe 21 septembrie 2005, iar pe 15 martie 2006 proiectul de directivă a fost adoptat.

Primele demersuri privind păstrarea datelor au fost lansate în urma atacurilor teroriste care au avut loc la Madrid în aprilie 2004. În acel moment, Marea Britanie, Suedia, Franţa şi Irlanda au venit cu propunerea unui plan privind păstrarea datelor care urma să ia forma unei Decizii cadru a Consiliului (de Miniştri al) Uniunii Europene. Marea Britanie, ţară care în 2005 a deţinut preşedinţia Uniunii Europene, şi-a consolidat şi mai mult poziţia de susţinere şi de promovare a acestui proiect, ca rezultat al atacurilor teroriste de la Londra din 2005. În acelaşi timp, Comisia Europeană, la rândul său, urmărea să-şi prezinte propriul proiect de directivă în materie de reţinere şi păstrare a datelor. Prin urmare, dezbaterile în ceea ce priveşte formarea unui cadru normativ la nivel UE, axat pe subiectul păstrării datelor, au vizat, inclusiv, procedura de adoptare a unei asemenea decizii, mai cu seamă dacă această decizie presupune implicarea instituţiilor UE, cum ar fi Comisia şi Parlamentul European şi atunci aceasta urma să fie adoptată în cadrul pilonului I – comunitar şi supranaţional sau ţinea de competenţa celui de-al III-lea pilon – cooperare poliţienească şi judiciară în materie penală, interguvernamental.

Conform structurii de luare a deciziilor care funcţiona în cadrul Uniunii până la intrarea în vigoare a Tratatului de la Lisabona (1 decembrie 2009), deciziile din pilonul I erau adoptate cu majoritatea voturilor exprimate de guvernele statelor membre şi de Parlamentul European, ca urmare a unei propuneri venite din partea Comisiei, în cadrul procedurii de co-decizie (actualmente, procedură legislativă ordinară), care presupune o participare parlamentară deplină. Însă, în ceea ce priveşte deciziile privind chestiunile de securitate, acestea erau adoptate, de regulă, prin consens sau unanimitate în cadrul celui de-al III-lea pilon, care cuprindea numai statele membre, iar Parlamentul European era împuternicit doar cu prerogativa de a emite o opinie asupra subiectului pus în discuţie.

[*] Raportul Comisiei către Consiliu şi către Parlamentul European de evaluare a Directivei 2006/24/CE privind păstrarea datelor se baza pe notificările de transpunere primite de Comisie de la 25 de state membre, inclusiv Belgia, care până la acel moment a transpus Directiva doar parţial. În Austria şi Suedia proiectele de lege în materie erau în dezbatere. În aceste două state membre nu exista nicio obligaţie de păstrare a datelor, dar autorităţile de aplicare a legii puteau solicita şi obţine date privind traficul de la operatori, în măsura în care astfel de date erau disponibile. După ce Republica Cehă, Germania şi România au notificat iniţial transpunerea Directivei, legislaţia naţională aferentă de transpunere a Directivei a fost anulată de Curţile Constituţionale din aceste ţări. Comisia a apreciat transpunerea Directivei ca fiind una inegală, menţionând că în momentul întocmirii Raportului legislaţia de transpunere era în vigoare în 22 de state membre, iar evaluarea Directivei privind păstrarea datelor a fost foarte problematică din cauza marjei considerabile de care dispuneau statele membre pentru a adopta măsuri privind păstrarea datelor în temeiul articolului 15 alineatul (1) din Directiva privind confidenţialitatea în mediul electronic. Existau diferenţe considerabile între legislaţiile de transpunere în domeniile care reglementează limitarea scopului, accesul la date, perioadele de păstrare, protecţia şi securitatea datelor, precum şi statisticile.

În consecinţă, în aceste condiţii, legiuitorilor din cadrul UE le revenea sarcina de a decide asupra unei probleme juridice complicate, şi anume: dacă legislaţia din domeniul reţenţiei şi păstrării datelor putea fi adoptată în baza celui de-al III-lea pilon sau nu. În acelaşi timp, este important a menţiona că reacţia statelor membre vis-à-vis de acest conflict de competenţă a fost una diferită. Irlanda a anunţat că intenţionează să sesizeze Curtea de Justiţie a Uniunii Europene (CJUE), motivând că reglementarea acestui domeniu reprezintă o prerogativă a statelor membre şi, prin urmare, Irlandei ar fi trebuit să i se permită menţinerea dreptului său de veto. Slovacia a reiterat şi ea anumite rezerve privitoare la procedura de reglementare, specificând faptul că este de acord cu conţinutul Directivei propuse de Comisie, dar obiectează în privinţa plasării acesteia în cadrul primului pilon. Pe de altă parte, Suedia, unul dintre statele membre cele mai dornice de a introduce legislaţia UE privind păstrarea datelor, a indicat asupra faptului că, în cazul în care această decizie nu ar fi guvernată de primul pilon, atunci Comisia şi Consiliul ar fi cele care ar sesiza CJUE.

Textul propus de Consiliu se deosebea de proiectul Comisiei prin faptul că prevedea o perioadă minimă de păstrare a datelor, de 1 an, pentru toate categoriile de date, cu posibilitatea de extindere a acestui termen până la 4 ani[*]. De asemenea, acest text stabilea ca obiectiv esenţial aplicarea de către toate statele membre a aceloraşi norme în materie de păstrare a datelor. Scopul acestei acţiuni era de a armoniza domeniul reţinerii traficului de date pentru a permite desfăşurarea cercetărilor penale. Proiectul de decizie al Consiliului prevedea numărul minim de infracţiuni care ar permite organelor de drept să acceseze datele, printre care „participarea în cadrul unei organizaţii criminale, terorism, traficul de fiinţe umane, exploatarea sexuală a copiilor, traficul de droguri, spălarea banilor, fraudă, rasism, deturnarea şi „furtul unui vehicul". Datele colectate trebuiau să conţină informaţii privind identificarea sursei, destinaţia şi ora unei comunicaţii, la fel ca şi detalii referitoare la persoana-abonat al oricărui „dispozitiv de comunicaţie". Cu toate acestea, abonaţii nu dispun de dreptul de a verifica, dacă informaţia reţinută privind comunicarea lor personală este corectă şi nici de a contesta juridic deciziile despre utilizarea acesteia de autorităţile UE. Conform aceluiaşi proiect, un stat membru nu putea invoca temeiuri precum protecţia drepturilor omului şi a vieţii private, pentru a refuza cererea privind oferirea de informaţii venită din partea unui alt stat membru. Totuşi, proiectul prevedea că transmiterea datelor serviciilor de securitate şi organelor de drept putea fi efectuată doar cu autorizare judecătorească [5]. Atât Comisia, cât şi Serviciul Juridic al Consiliului au contestat legalitatea acestei iniţiative, deoarece se făcea uz de structura celui de-al treilea pilon, prin care Parlamentul European este înlăturat definitiv de la procesul de luare a deciziilor. În cele din urmă, nefiind capabili să ajungă la un consens în cadrul şedinţei Consiliului, miniştrii de justiţie UE au respins propunerea Consiliului şi au hotărât să recurgă la ajutorul Comisiei şi al Parlamentului European pentru adoptarea unei decizii, acceptând astfel „propunerea de compromis" parvenită din partea Comisiei, care, spre deosebire de proiectul Consiliului, sugera că statele membre ar trebui să dispună de mai multă libertate la elaborarea propriilor norme şi reguli în materie de păstrare a datelor. Irlanda şi Slovacia au votat împotrivă, reafirmând că acestea privesc securitatea naţională ca fiind o problemă de competenţă naţională şi nicidecum de nivelul UE.

În acelaşi timp, au fost exprimate şi alte preocupări privind legalitatea Directivei, mai cu seamă de anumiţi membri ai Parlamentului European, care afirmau că Directiva cu privire la păstrarea datelor ar încălca Convenţia Europeană privind Drepturile Omului (CEDO), dat fiind faptul că aceasta prevede protecţia vieţii private şi stabileşte că datele nu ar trebui reţinute pentru „mai mult decât este necesar" [5]. De asemenea, reprezentantul liberal din partea Germaniei în Parlamentul European, *Alexander Alvaro*, a menţionat că legislaţia UE în materie de păstrare a datelor ar putea fi contestată în instanţele naţionale, cu probabilitatea ca Curtea Supremă a Germaniei să ridice problema corespunderii acesteia cu Constituţia [6].

În acest context, este important a menţiona că în unele state membre legile de transpunere a Directivei în dreptul intern au fost anulate, pe motiv că erau neconstituţionale, de către Curţile Constituţionale a României [7] (octombrie 2009), a Germaniei [8] (martie 2010) şi a Republicii Cehe [9] (martie 2011).

În 2006, Irlanda (reclamant), alături de Slovacia (în calitate de intervenient din partea reclamantului), au solicitat CJUE să se expună asupra faptului dacă Directiva privind păstrarea datelor a fost adoptată conform cadrului juridic cuvenit, cu alegerea temeiului juridic corect (cauza C-301/06, *Irlanda v. Parlamentul European*). Prin Hotărârea din 10 februarie 2008, CJUE a respins această acţiune, statuând că Directiva vizează în mod preponderent funcţionarea pieţei interne, astfel era necesar ca Directiva să fie adoptată în temeiul art.114 TFUE (ex-art.95 din Tratatul CE).

[*] Directiva 2006/24/CE stabileşte obligaţia de asigurare a păstrării datelor pentru perioade de cel puţin 6 luni şi cel mult 2 ani.

Majoritatea statelor membre au transpus integral prevederile Directivei pe parcursul anilor 2010 şi 2011. În ceea ce priveşte Suedia şi Austria, iniţial, legislaţia naţională de transpunere a Directivei a fost respinsă de parlamentele acestor state membre, pentru ca mai apoi să fie totuşi adoptată. Până în acest moment, 26 din cele 28 de state membre UE, în afară de Germania şi Belgia, au transpus legislaţia UE în materie de păstrare a datelor. Legislaţia în materie de păstrare a datelor a fost adoptată şi în ţările membre ale Spaţiului Economic European (SEE), Islanda, Liechtenstein şi Norvegia.

Anumite reglementări ale legislaţiei UE în materia păstrării datelor, în speţă art.3, 5 şi 6 din Directiva 2006/24/CE, care instituie obligaţia de păstrare a datelor, categoriile de date care sunt păstrate şi perioadele de păstrare a acestora, au fost transpuse şi de către Republica Moldova la art.20 al Legii comunicaţiilor electronice, nr.241 din 15 noiembrie 2007. Potrivit art.20 alin.(3) al Legii 241/2007, furnizorii de reţele şi/sau de servicii de comunicaţii electronice, indiferent de tipul de proprietate, sunt obligaţi să păstreze toate informaţiile disponibile, generate sau procesate în procesul furnizării propriilor servicii de comunicaţii electronice, necesare pentru identificarea şi urmărirea sursei de comunicaţii electronice, identificarea destinaţiei, tipului, datei, orei şi duratei comunicaţiei, identificarea echipamentului de comunicaţii al utilizatorului sau al altui dispozitiv utilizat pentru comunicaţie, identificarea coordonatelor echipamentului terminal de comunicaţii mobile şi să asigurare prezentarea acestor informaţii organelor împuternicite în condiţiile legii. Informaţiile ce ţin de serviciile de telefonie mobilă sau fixă vor fi păstrate o perioadă de un an, iar cele ce ţin de reţeaua Internet – de 6 luni. Obligaţia de păstrare se referă inclusiv la tentativele de apel eşuate.

Modul de transpunere şi implementare a Directivei 2006/24/CE în statele membre ale UE

Conform art.1 al Directivei 2006/24/CE, statele membre au obligaţia de a adopta măsuri care să asigure că datele sunt păstrate şi sunt disponibile în vederea cercetării, detectării şi urmăririi penale a infracţiunilor grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern. Bulgaria, Estonia, Irlanda, Grecia, Spania, Lituania, Luxemburgul, Ungaria, Olanda şi Finlanda au definit „infracţiunile grave" prin trimitere la o pedeapsă minimă cu închisoarea, la posibilitatea impunerii unei pedepse privative de libertate sau la o listă a infracţiunilor definite în altă parte în legislaţia naţională. Danemarca, Franţa, Italia, Letonia, Polonia, Slovacia şi Slovenia prevăd obligativitatea păstrării datelor nu doar în vederea cercetării, detectării şi urmăririi penale în legătură cu infracţiunile grave, ci şi în legătură cu toate infracţiunile, precum şi pentru prevenirea criminalităţii sau din motive generale de securitate naţională şi/sau securitate publică. Legislaţia statelor membre precum Cipru, Malta, Portugalia, Marea Britanie se referă la „infracţiuni grave" sau la „delicte grave", fără a le defini. Majoritatea statelor membre care au transpus Directiva, în conformitate cu legislaţia naţională, permit accesul la datele păstrate şi utilizarea acestora în scopuri care depăşesc cadrul Directivei, inclusiv prevenirea şi combaterea criminalităţii, în general, şi a riscurilor la adresa vieţii şi integrităţii corporale. Deşi acest lucru este permis în temeiul Directivei privind confidenţialitatea în mediul electronic, gradul de armonizare realizat de legislaţia UE în acest domeniu rămâne limitat [4].

Directiva se aplică în cazul „furnizorilor de servicii de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice" (art.1 alin.(1)). Finlanda şi Marea Britanie nu impun operatorilor mici obligaţia de păstrare a datelor, deoarece, în opinia lor, atât furnizorul, cât şi statul ar trebui să suporte costurile care depăşesc beneficiile generate pentru sistemele de justiţie penală şi pentru aplicarea legii. Letonia, Luxemburgul, Olanda şi Polonia menţionează că au pus în aplicare măsuri administrative alternative.

Articolul 4 din Directiva 2006/24/CE prevede că statele membre au obligaţia de „a se asigura că [datele păstrate] sunt furnizate numai autorităţilor naţionale competente în cazuri specifice şi în conformitate cu dreptul intern". Statele membre sunt cele care definesc în legislaţia lor naţională „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, sub rezerva dispoziţiilor relevante ale dreptului Uniunii Europene sau ale dreptului internaţional public şi, în special, a dispoziţiilor CEDO, astfel cum au fost interpretate de către Curtea Europeană pentru Drepturile Omului". În toate statele membre, forţele naţionale de poliţie şi, cu excepţia jurisdicţiilor de drept cutumiar (Irlanda şi Marea Britanie), procurorii pot avea acces la datele păstrate. Bulgaria, Grecia, Spania, Lituania, Luxemburgul, Malta şi Slovenia citează serviciile de securitate, serviciile de informaţii sau serviciile militare printre autorităţile competente. Estonia, Irlanda, Spania, Ungaria şi Polonia menţionează autorităţi fiscale şi/sau vamale, iar Finlanda, Portugalia, Polonia şi Estonia citează autorităţile de frontieră. Marea Britanie permite altor autorităţi publice să aibă acces la date, în cazul în care acestea sunt autorizate în scopuri specifice în temeiul legislaţiei secundare. În majoritatea statelor membre

este necesară autorizarea judiciară pentru fiecare cerere de acces la datele păstrate. Unele state membre solicită ca autorizarea să fie acordată de o autoritate de înalt nivel, dar nu de un judecător: Ungaria – procurorul şi agenţiile naţionale de securitate pot accesa astfel de date fără un ordin judecătoresc; Polonia – în cazul poliţiei, al poliţiştilor de frontieră şi al inspectorilor fiscali, cererile trebuie autorizate de un înalt funcţionar din cadrul organizaţiei; Franţa – autorizare de către Ministerul de Interne; Italia – ordonanţă motivată emisă de procuror. În Malta şi Irlanda, singura condiţie pare a fi ca cererea să fie formulată în scris.

Directiva se aplică reţelei de telefonie fixă, telefoniei mobile, accesului la Internet, poştei electronice şi telefoniei prin Internet. Directiva reglementează, de asemenea, încercările nereuşite de apeluri telefonice, respectiv o comunicaţie în care un apel telefonic a fost conectat cu succes, dar nu a primit răspuns sau o comunicaţie în care a avut loc o intervenţie a sistemului de gestionare a reţelei, precum şi situaţiile în care datele privind aceste încercări sunt generate sau prelucrate şi păstrate sau înregistrate în jurnalul electronic de către operatori. În temeiul Directivei, se interzice păstrarea datelor care dezvăluie conţinutul comunicaţiei. Majoritatea statelor membre prevăd păstrarea fiecăreia dintre aceste categorii de date în legislaţia lor de transpunere.

Statele membre au obligaţia de a se asigura că datele sunt păstrate pe perioade de cel puţin şase luni şi de cel mult doi ani. Perioada maximă de păstrare poate fi prelungită de un stat membru care „se confruntă cu situaţii specifice care justifică extinderea pe o perioadă limitată"; o astfel de prelungire trebuie comunicată Comisiei care, în termen de şase luni de la data notificării, poate decide să o aprobe sau să o respingă. Mai multe state membre prevăd o perioadă unică pentru toate categoriile de date: Polonia – 2 ani; Letonia – 1,5 ani; Bulgaria, Danemarca, Estonia, Grecia, Spania, Franţa, Olanda, Portugalia, Finlanda, Regatul Unit – 1 an; România, Cipru, Luxemburgul, Lituania – 6 luni. Unele state membre au definit perioade diferite de păstrare în funcţie de categoriile de date: Irlanda şi Italia prevăd doi ani pentru datele de telefonie fixă şi mobilă şi un an pentru datele privind accesul la Internet, poşta electronică şi telefonia prin Internet; Slovenia indică 14 luni pentru datele de telefonie şi opt luni pentru datele referitoare la Internet; Slovacia prevede un an pentru telefonia fixă şi mobilă şi şase luni pentru datele referitoare la Internet; Malta prevede un an pentru datele privind telefonia fixă, mobilă şi prin Internet şi şase luni pentru accesul la Internet şi poşta electronică. Ungaria păstrează toate datele timp de un an, cu excepţia datelor privind încercările nereuşite de apeluri telefonice care sunt păstrate doar şase luni.

În temeiul Directivei, statele membre au obligaţia de a se asigura că operatorii respectă, cel puţin la nivel minim, patru principii de securitate a datelor, şi anume, că datele păstrate: (a) sunt de aceeaşi calitate şi sunt supuse aceleiaşi securităţi şi protecţii ca şi datele din reţeaua [publică de comunicaţii]; (b) sunt supuse măsurilor tehnice şi organizaţionale adecvate pentru a fi protejate împotriva distrugerii accidentale sau ilegale, pierderii accidentale sau modificării, depozitării, prelucrării, accesării sau divulgării neautorizate sau ilicite; (c) se supun măsurilor tehnice şi organizaţionale adecvate pentru a se asigura că accesarea acestora poate fi făcută numai de către personal special autorizat *şi* (d) sunt distruse la finalul perioadei de păstrare, cu excepţia celor care au fost accesate şi reţinute [în scopul stabilit în Directivă]. Aproape toate statele membre au transpus aceste patru principii în legislaţia relevantă. Estonia, Spania şi Letonia au transpus două sau trei dintre aceste principii, dar nu prevăd în mod explicit dispoziţii privind distrugerea datelor la expirarea perioadei de păstrare. Italia şi Finlanda prevăd distrugerea datelor. Majoritatea statelor membre au o autoritate de supraveghere care răspunde de monitorizarea aplicării principiilor. În majoritatea cazurilor, aceasta este autoritatea pentru protecţia datelor.

Privitor la chestiunea privind vechimea de păstrare a datelor, majoritatea statelor membre consideră că utilizarea datelor păstrate, cu o vechime mai mare de trei sau chiar şase luni, este mai puţin frecventă, dar aceasta poate fi esenţială. În primul rând, datele referitoare la Internet sunt solicitate, în general, mai târziu decât alte mijloace de probă în cursul cercetărilor penale. Analiza datelor privind reţeaua de telefonie fixă şi a datelor de telefonie mobilă duce, adesea, la potenţiale piste, ceea ce generează cereri suplimentare de date mai vechi. În al doilea rând, investigarea infracţiunilor deosebit de grave, a unei serii de infracţiuni, a criminalităţii organizate şi a incidentelor teroriste tinde să se bazeze pe date păstrate mai vechi, care reflectă timpul necesar pentru a planifica aceste infracţiuni, pentru a identifica modelele de comportament infracţional şi relaţiile dintre complicii la o infracţiune şi pentru a stabili intenţia de a săvârşi o infracţiune. Adesea, activităţile care au legătură cu infracţiuni financiare complexe sunt detectate doar după câteva luni. În al treilea rând, şi în mod excepţional, statele membre au solicitat date privind traficul deţinute în alt stat membru, care,

de obicei, nu poate comunica aceste date decât cu autorizare judiciară, ca răspuns la o scrisoare rogatorie din partea unui judecător din statul membru care solicită datele respective.

Caracterul constituţional al legilor interne de transpunere a Directivei a fost contestat în câteva state membre. Curtea Constituţională din România, Curtea Constituţională din Germania şi Curtea Constituţională din Republica Cehă au anulat în octombrie 2009, martie 2010 şi, respectiv, martie 2011 legile de transpunere a Directivei în dreptul intern pe motiv că erau neconstituţionale. Curtea Constituţională a României [8], bazându-se pe jurisprudenţa Curţii Europene a Drepturilor Omului, a constatat că domeniul de aplicare şi scopul legii de transpunere erau ambigue şi că garanţiile erau insuficiente şi a hotărât că o „obligaţie legală care impune reţinerea în mod continuu" a tuturor datelor privind traficul pe o perioadă de şase luni era incompatibilă cu dreptul la respectarea vieţii private şi libertatea de exprimare, prevăzute la articolul 8 din Convenţia europeană a drepturilor omului. Curtea Constituţională a Germaniei [9] a hotărât că păstrarea datelor a generat un sentiment de supraveghere, care ar putea afecta exercitarea liberă a drepturilor fundamentale. Aceasta a recunoscut în mod explicit că păstrarea datelor pentru utilizări strict limitate, în condiţii de securitate a datelor suficient de ridicate, nu ar încălca Legea Fundamentală a Germaniei. Curtea a subliniat că păstrarea unor astfel de date constituie o restricţionare gravă a dreptului la viaţă privată şi, în consecinţă, aceasta ar trebui să fie permisă doar în anumite circumstanţe extrem de limitate şi că o perioadă de păstrare de şase luni este limita maximă a ceea ce ar putea fi considerat drept proporţional. Datele ar trebui solicitate numai în cazul în care există deja o suspiciune privind săvârşirea unei infracţiuni grave sau dovada unui pericol la adresa securităţii publice, iar recuperarea datelor ar trebui să fie interzisă pentru anumite comunicaţii privilegiate (şi anume, cele legate de o necesitate emoţională sau socială) care au la bază principiul confidenţialităţii. De asemenea, datele ar trebui codate, cu o supraveghere transparentă a utilizării lor. Curtea Constituţională a Cehiei [9] a anulat legislaţia de transpunere pe motiv că, fiind o măsură care afecta exercitarea drepturilor fundamentale, aceasta nu era formulată suficient de precis şi de clar. Curtea a criticat caracterul insuficient de restrictiv al limitării scopului, luând în considerare amploarea şi domeniul de aplicare ale obligaţiei de păstrare a datelor. Aceasta a apreciat că autorităţile cu competenţe în materie de acces şi utilizare a datelor păstrate, precum şi procedurile aferente nu erau definite suficient de clar în legislaţia de transpunere pentru a asigura integritatea şi confidenţialitatea datelor. Prin urmare, cetăţenii dispuneau de garanţii insuficiente împotriva eventualelor abuzuri de putere ale autorităţilor publice. Totuşi, ulterior, România şi Republica Cehă au asigurat retranspunerea Directivei în legislaţia lor naţională.

În ceea ce priveşte neîndeplinirea obligaţiei de transpunere (procedura de infringement), Comisia a intentat trei acţiuni în constatarea neîndeplinirii obligaţiilor de transpunere: în 2009, în privinţa Suediei (C-185/09), Irlandei (C-202/09) şi Greciei (C-211/09), altă acţiune în 2010, împotriva Austriei (C-189/09), şi a treia acţiune în 2011, contra Suediei (C-270/11), în urma cărora Curtea a stabilit impunerea de penalităţi financiare în temeiul articolului 260 din Tratatul privind funcţionarea Uniunii Europene.

Aspecte-cheie ale declarării nevalabile a Directivei 2006/24 CE

Vom analiza în cele din urmă acele dispoziţii de fond care au ridicat unele probleme de compatibilitate a Directivei cu drepturile fundamentale, aşa cum ele sunt recunoscute de Carta drepturilor fundamentale a UE, pentru a ne convinge de ce Curtea de Justiţie nu a avut nicio dificultate în a stabili că obligaţia de conservare a datelor în domeniul comunicaţiilor electronice prevăzute în Directivă constituie o ingerinţă deosebită în drepturile fundamentale ale individului, în pofida faptului că aceasta poate fi justificată în lupta contra criminalităţii.

Ingerinţa în protecţia vieţii private şi a datelor personale

Prestatorii de servicii de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice au obligaţia de a păstra datele necesare pentru urmărirea şi identificarea sursei unei comunicaţii şi destinaţia acesteia, pentru a determina data, ora, durata şi tipul unei comunicaţii, echipamentul de comunicaţie al utilizatorilor, precum şi pentru a localiza echipamentul de comunicaţie mobilă, cu scopul de a le face accesibile autorităţilor naţionale competente de prevenirea, cercetarea, depistarea şi urmărirea unor infracţiuni grave (art.3 şi 5). Figurează, astfel, numele şi adresa abonatului sau a utilizatorului înregistrat, numărul de telefon al apelantului şi numărul apelatului, precum şi o adresă Internet Protocol (IP) pentru serviciile Internet. Aceste date permit să se cunoască cu ce persoană şi prin ce modalitate a comunicat un abonat sau un utilizator înregistrat, să se determine durata comunicării, precum şi locul de unde aceasta a avut loc, să se cunoască frecvenţa comunicaţiilor abonatului sau ale utilizatorului înregistrat cu anumite persoane într-o perioadă determinată.

STUDIA UNIVERSITATIS MOLDAVIAE, 2014, nr.8(78)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.35-45

Aceste date pot furniza indicaţii precise cu privire la viaţa privată a persoanelor ale căror date sunt păstrate, cum sunt obiceiurile din viaţa cotidiană, locurile de şedere permanente sau temporare, deplasările zilnice sau alte tipuri de deplasări, activităţile desfăşurate, relaţiile sociale şi mediile sociale frecventate. Chiar dacă Directiva 2006/24 CE nu autorizează păstrarea conţinutului comunicaţiilor şi al informaţiilor consultate utilizând un serviciu de comunicaţii electronice (art.1 parag.2 şi art.5 parag.2), păstrarea datelor sus-menţionate poate avea o incidenţă asupra libertăţii de exprimare a abonaţilor (art.11 al Cartei), protecţiei vieţii private (art.7 al Cartei) şi protecţiei datelor cu caracter personal (art.8 al Cartei) [10]. Conservarea datelor în sectorul comunicaţiilor electronice vine să stabilească un regim de reglementare derogatoriu de la prevederile Directivei 95/46/CE, în speţă, de la art. 5, 6 şi 9 din Directiva 2002/58/CE (Directiva asupra confidenţialităţii şi comunicaţiilor electronice), care stabilesc normele aplicabile prelucrării de către furnizorii de reţele şi servicii a datelor privind traficul şi localizarea generate prin utilizarea serviciilor de comunicaţii electronice. Aceste tipuri de date trebuie să fie şterse sau făcute anonime atunci când acestea nu mai sunt necesare în scopul transmiterii unei comunicări.

Obligaţia de conservare impusă prin Directiva 2006/24 CE constituie o evidentă ingerinţă în drepturile fundamentale, puţin contează că informaţiile conservate ar avea un caracter sensibil sau că interesaţii ar suferi eventuale inconveniente. De altfel, accesul autorităţilor naţionale competente la date antrenează o ingerinţă suplimentară [11], iar ingerinţa astfel organizată prin prezenta Directivă este de o mare amploare. Ea trebuie considerată ca fiind deosebit de gravă de vreme ce păstrarea datelor şi utilizarea lor ulterioară sunt efectuate fără ca abonatul sau utilizatorul înregistrat să fie informaţi cu privire la aceasta şi este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viaţa lor privată face obiectul unei supravegheri constante.

Justificarea ingerinţei în lupta contra criminalităţii

Dacă nu încape nicio îndoială că este vorba de o ingerinţă, aceasta îşi poate găsi o justificare în art.52, parag.1 al Cartei, care prevede anumite limitări în exercitarea drepturilor şi libertăţilor consacrate. Altfel spus, drepturile recunoscute sunt fundamentale, fără a avea totuşi un caracter absolut. Limitările trebuie, totuşi, să fie prevăzute prin lege, să respecte conţinutul lor esenţial, precum şi principiul proporţionalităţii, să fie necesare şi să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau pentru a proteja drepturile şi libertăţile altuia.

Vorbind despre conţinutul esenţial al drepturilor fundamentale, ingerinţa nu este de natură să aducă atingere acestuia, deoarece Directiva 2006/24 CE nu autorizează păstrarea conţinutului comunicaţiilor electronice. Articolul 7 al Directivei prevede adoptarea măsurilor tehnice şi organizaţionale apropriate contra distrugerii accidentale sau ilicite, pierderii sau alterării accidentale a datelor. De asemenea, Directiva răspunde unui obiectiv de interes general, căci vizează garantarea şi disponibilitatea datelor conservate în vederea cercetării, detectării şi urmăririi infracţiunilor grave. Obiectivul material al acestei Directive este de a contribui la lupta contra criminalităţii grave. Potrivit jurisprudenţei CJUE, constituie un obiectiv de interes general al Uniunii lupta contra terorismului internaţional [12], precum şi lupta contra criminalităţii grave, în vederea garantării securităţii publice [13]. De altfel, art.6 al Cartei enunţă dreptul oricărei persoane la libertate, dar şi la siguranţă. De asemenea, Consiliul Justiţie şi Afaceri Interne al UE din 19 decembrie 2002 a relevat că datele în legătură cu utilizarea comunicaţiilor sunt utile în vederea prevenirii infracţiunilor şi luptei contra criminalităţii. Conservarea acestor date corespunde întru totul unui obiectiv de interes general.

Utilizarea tehnologiilor de informaţie şi comunicaţie (TIC) facilitează comiterea infracţiunilor; astfel, este necesar de a permite autorităţilor poliţieneşti să controleze indivizii prin intermediul acestor procedee. În particular, telefonia mobilă şi Internetul constituie astăzi mijloace de comunicaţie esenţiale, cu ajutorul cărora o supraveghere eficientă poate fi pusă în aplicare. Prin urmare, Directiva 2006/24 CE răspunde acestui obiectiv de securitate naţională, dar trebuie, în egală măsură, să satisfacă principiul proporţionalităţii.

Ingerinţa este justificată, dar se dovedeşte a fi disproporţionată, iar securitatea datelor nu este garantată

Potrivit unei jurisprudenţe constante a Curţii [14], principiul proporţionalităţii cere ca actele instituţiilor Uniunii să fie susceptibile să realizeze obiectivele legitime urmărite de reglementarea în cauză şi să nu depăşească limitele a ceea ce este adecvat şi necesar pentru realizarea acestor obiective. Respectarea acestor condiţii constituie obiectul unui control jurisdicţional şi, de vreme ce ingerinţele în drepturile fundamentale sunt atinse, puterea de apreciere a legiuitorului Uniunii Europene se poate adeveri a fi una limitată, în funcţie, în

special, de domeniul vizat, de natura dreptului în cauză garantat de Cartă, de natura şi gravitatea ingerinţei, precum şi de finalitatea acesteia. În speţă, ţinând cont de rolul important pe care îl joacă protecţia datelor cu caracter personal în raport cu dreptul fundamental la respectarea vieţii private, dar şi de amploarea şi de gravitatea ingerinţei în acest drept care rezultă din Directiva 2006/24, puterea de apreciere a legiuitorului Uniunii ar trebui sa fie una redusă.

Judecătorul european exercită, deci, un control jurisdicţional strict. El trebuie să verifice dacă conservarea datelor permite realizarea obiectivului urmărit de Directiva 2006/24 CE. Având în vedere importanţa crescândă a mijloacelor de comunicaţii electronice, datele conservate permit autorităţilor naţionale competente să dispună de mijloace utile pentru elucidarea infracţiunilor grave. Eficacitatea luptei contra criminalităţii poate depinde de utilizarea pe larg a tehnicilor de anchetă moderne.

Prin urmare, un astfel de obiectiv de interes general, oricât de fundamental ar fi, nu poate justifica *per se* faptul de a considera o măsură de păstrare, precum cea instituită de Directiva 2006/24/CE, ca fiind necesară în scopul combaterii menţionate. Este necesar, printre altele, ca drepturile fundamentale la respectarea vieţii private şi la protecţia datelor cu caracter personal să fie privite *a fortiori* atunci când datele sunt supuse unui tratament automatizat şi există un risc eminent de acces ilicit la aceste date. Or, Curtea relevă că Directiva 2006/24/CE acoperă în mod generalizat toate persoanele şi toate mijloacele de comunicare electronică, precum şi ansamblul datelor de trafic, fără a face vreo diferenţiere, limitare sau excepţie în funcţie de obiectivul combaterii infracţiunilor grave. Mai mult, nu se cere ca persoanele, ale căror date au fost conservate, să se afle, chiar şi indirect, într-o situaţie susceptibilă să genereze urmărirea penală. Directiva nu prevede niciun criteriu obiectiv care să permită delimitarea accesului autorităţilor naţionale competente la date şi utilizarea lor ulterioară în scopul prevenirii, detectării sau urmăririi penale în legătură cu infracţiuni care, având în vedere amploarea şi gravitatea ingerinţei în drepturile fundamentale consacrate în art.7 şi 8 din Cartă, pot fi considerate ca fiind suficient de grave pentru a justifica o astfel de ingerinţă. Ea se limitează la a face trimitere, de manieră generală, la infracţiunile grave, în modul în care acestea au fost definite de legislaţiile naţionale ale statelor membre. De asemenea, nicio condiţie materială sau procedurală de acces la aceste date nu este prevăzută, iar fiecare stat membru îşi adoptă propria procedură de urmat cu respectarea exigenţelor privind necesitatea şi proporţionalitatea, fără ca vreun criteriu obiectiv să fie impus sau aşteptat din partea statelor, de asemenea, nici un control prealabil – fie unul jurisdicţional, fie efectuat de către o autoritate independentă. În fine, Directiva 2006/24 CE impune conservarea datelor în cursul unei perioade între 6 şi 24 de luni, fără a se face vreo distincţie între categoriile de date prevăzute la articolul 5 din această Directivă, în funcţie de utilitatea lor eventuală în scopul realizării obiectivului urmărit, în funcţie de persoanele vizate sau în funcţie de alte criterii obiective, pentru a fi într-adevăr limitată la strictul necesar.

Această argumentare îşi găseşte sprijinul în poziţia exprimată de Parlamentul European în cursul adoptării la 12 martie 2014 a noului Pachet legislativ în domeniul datelor personale. Eurodeputaţii au estimat că măsurile de securitate, în special în cadrul luptei contra terorismului, trebuie să respecte obligaţiile în materia drepturilor fundamentale ale omului. Dacă guvernele afirmă că programele de supraveghere masivă sunt necesare în lupta contra terorismului şi denunţă cu fermitate terorismul, această luptă în niciun caz nu poate justifica existenţa programelor de supraveghere a grupurilor care nu sunt ţintă, secrete, chiar şi ilegale. Prin urmare, aceste programe au fost apreciate ca fiind incompatibile cu principiile necesităţii şi proporţionalităţii, în vigoare într-o societate democratică.

În speţă, Directiva 2006/24 CE nu prevede reguli clare şi precise care ar guverna natura şi întinderea ingerinţei în drepturile fundamentale consacrate la articolele 7 şi 8 ale Cartei. Trebuie de luat în considerare că ingerinţa este de o vastă amploare şi de o gravitate particulară în ordinea juridică a Uniunii. Curtea declară nevalabilă Directiva, iar decizia Curţii nu surprinde, căci chiar Comisia Europeană avea să lanseze, începând cu 2009, un proces de evaluare a Directivei, care a dat naştere unui raport publicat în anul 2011 [4]. Ea constată o transpunere inegală a Directivei, o armonizare insuficientă şi admite, în egală măsură, că proporţionalitatea în procesul de stocare şi conservare a datelor nu era garantată. Controlorul european pentru protecţia datelor personale a emis la 31 mai 2011 un aviz, prin care şi-a exprimat îngrijorări serioase în privinţa necesităţii şi proporţionalităţii măsurilor, denunţând, de asemenea, existenţa unei mari marje de manevră de care dispuneau statele membre în privinţa finalităţii utilizării datelor, dar şi a condiţiilor de acces [15]. O revizuire a Directivei era luată în calcul, însă nu a văzut lumina zilei. Prin decizia sa, Curtea constrânge, de acum înainte, Comisia Europeană să reformuleze un text mai echilibrat.

Securitate insuficientă a protecţiei datelor personale

Pe lângă caracterul disproporţionat al ingerinţei, Curtea de Justiţie a relevat absenţa unor garanţii şi reguli în securitatea şi protecţia datelor personale conservate de către furnizorii de servicii de comunicaţii electronice. În particular, Directiva 2006/24 CE nu prevede nicio protecţie eficientă pentru a garanta deplina integritate şi confidenţialitate contra riscurilor de abuz, precum şi contra oricărui acces şi oricărei utilizări ilicite a acestor date. Nicio măsură tehnică sau organizaţională nu este susţinută de prezenta Directivă. De asemenea, operatorii sunt autorizaţi să ţină cont de costurile implementării măsurilor de securitate. Este evident că aceştia nu pot aplica un nivel ridicat de protecţie pentru toate datele, ţinând seama de costurile exorbitante necesare operaţionalizării măsurilor de securitate. În fine, Directiva nu garantează distrugerea iremediabilă a datelor la încheierea perioadei de conservare a acestora. Este vorba aici despre unul din punctele slabe majore ale legislaţiei cu privire la datele personale, pe care îl regăsim şi în cadrul aplicării Directivei 95/46 CE. Respectarea principiului finalităţii este dificil de a fi garantată şi nu ne rămâne decât să sperăm că reforma prevăzută prin propunerea de regulament din 25 mai 2012 va permite ca această exigenţă să fie mai bine satisfăcută graţie consolidării sancţiunilor.

Într-un final, Curtea a constatat că actul UE nu impune ca datele în cauză să fie păstrate pe teritoriul Uniunii, astfel încât nu se poate considera că controlul exercitat de o autoritate independentă, impus în mod expres la art.8 alin.(3) din Cartă, al respectării cerinţelor de protecţie şi de securitate, astfel cum sunt menţionate la cele două puncte precedente, este garantat în totalitate. Or, un astfel de control efectuat în temeiul dreptului Uniunii constituie un element esenţial al respectării protecţiei persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal. Controlul asupra respectării legislaţiei în materia datelor personale este pus pe seama autorităţilor naţionale independente, precum şi a Centrului European pentru protecţia datelor personale. Proiectul de regulament din 25 ianuarie 2012 confirmă această logică, consolidând competenţele acestor autorităţi, dar şi exigenţele cu privire la independenţa lor.

După invalidarea Directivei 2006/24 CE de către Curtea de Justiţie ca urmare a violării principiului proporţionalităţii în lumina articolelor 7, 8 şi 52 parag.1 ale Cartei, Comisia şi noul Parlament European vor fi obligate să procedeze la o rescriere a Directivei.

Concluzii

Şi dacă decizia Curţii punctează unele dificultăţi deja cunoscute, ea este una meritorie şi eficientă prin dorinţa sa de a pune capăt unei situaţii puţin respectuoase a drepturilor fundamentale ale cetăţenilor UE. Textul care va lua locul vechii directive va trebui să asigure o protecţie mai sporită cetăţenilor UE şi va trebui să se concretizeze printr-o reducere a marjei de manevră a statelor şi prin condiţii mai stricte în ceea ce priveşte conservarea datelor în domeniul comunicaţiilor electronice. Judecătorul european forţează aici legiuitorul european să reacţioneze, iar acesta nu este un merit mai puţin important al hotărârii din 8 aprilie 2014.

Decizia CJUE luată pe 8 aprilie este una de referinţă pentru legislaţia drepturilor omului. Invalidarea Directivei are consecinţa retragerii tuturor legilor interne de implementare a Directivei care contravin deciziei Curţii. Dacă o ţară vrea să introducă o astfel de lege la nivel naţional, o poate face pe baza articolul 15 din Directiva 2002/58/CE, respectând în acelaşi timp prevederile stabilite de CJUE: transparenţă, necesitate, proporţionalitate. Această decizie este, probabil, cea mai importantă hotărâre a CJUE cu privire la drepturile omului, deoarece este prima care invalidează o directivă pentru încălcarea drepturilor omului prevăzute în Carta drepturilor fundamentale a UE.

Bibliografie:

1. Proiectul de regulament al Parlamentului şi Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date din 25 ianuarie 2012 (COM (2012) 0011) şi Proiectul de directivă privind protecţia datelor procesate în scopul prevenirii, detectării, investigării şi punerii sub urmărire a infracţiunilor şi a altor activităţi judiciare (COM (2012) 0010).
2. *A se vedea*: CJUE 13 mai 2014, Cauza C-131/12 Google Spain SL, Google Inc. împotriva Agencia Española de Protección de Datos (AEPD), Mario Costeja González în: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=244667
3. http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=245146

4. Raportul Comisiei către Consiliu şi către Parlamentul European de evaluare a Directivei 2006/24/CE privind păstrarea datelor, Bruxelles, 18.4.2011. Accesibil în: www.csm1909.20/csm/linkuri/05_05_2011-40961_ro.pdf
5. Accesibil în: http://euobserver.com/justice/7292
6. Accesibil în: http://euobserver.com/justice/20548
7. Decizia nr.1258 din 8 octombrie 2009 a Curţii Constituţionale a României referitoare la excepţia de neconstituţionalitate a prevederilor Legii nr.298/2008 privind reţinerea datelor generate sau prelucrate de furnizorii de servicii electronice destinate publicului sau de reţele publice de comunicaţii, precum şi pentru modificarea Legii nr.506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice. Accesibil în: www.legi-internet.ro/fileadmin/editor-folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf
8. Bundesverfassungsgericht, 1 BvR 256/08. Accesibil în engleză: www.bverfg.de/pressemitteilungen/bvg10-011en.html
9. Hotărârea Curţii Constituţionale a Cehiei din 22 martie privind Legea nr.127/2005 şi Decretul nr.485/2005. Accesibil în: www.edri.org/files/Dataretention_judgment_ConstitutionalCourt_CzechRepublic.pdf
10. *A se vedea*: CJUE 9 noiembrie 2010, C-92/09 şi C-93/09, *Volker und Markus Schecke* şi *Eifert*, pct.47.
11. În privinţa art.8 al CEDO *a se vedea*: hot.CEDO din 26 martie 1987, nr.9248/81, *Leander vs /Suedia*, seria A, nr.116, parag.48; 4 mai 2000, nr.28341/95, *Rotaru vs/ România*, parag.46, Culegere CEDO 2000-V; D.2001; precum şi din 29 iunie 2006, nr.54934/00, *Weber şi Saravia vs/Germania*, parag.79, Culegerea CEDO 2006-XI.
12. *A se vedea*: CJUE 3 septembrie 2008, C-402/05 P, *Kadi şi Al Barakaat International Foundation vs/ Consiliul şi Comisia*, pct. 363.
13. *A se vedea*: CJUE 23 noiembrie 2010, C-145/09, *Tsakouridis*, pct. 46 şi 47.
14. *A se vedea*: CJUE 8 iulie 2010, C-343/09, *Afton Chemicals*, pct.45; 9 noiembrie 2010, C-92/09, *Volker und Markus Schecke* şi *Eifert*, pct.47; 23 octombrie 2012 C-581/10 şi C-629/10, *Nelson ş.a*., pct.71; 22 ianuarie 2013, C-283/11, *Sky Osterreich*, pct.50; precum şi 17 octombrie 2013, C-101/12 *Schaible*, pct.29.
15. https://secure.edps.europa.eu/EDPSWEB/webday/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

Prezentat la 11.09.2014