CONSILIUL UNIUNII EUROPENE

Bruxelles, 19 aprilie 2011 (03.05)
(OR. en)

9324/11

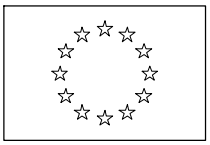
DAPIX 38
TELECOM 47
COPEN 85

NOTĂ DE ÎNSOŢIRE

Sursă:	Secretar General al Comisiei Europene semnat de către dl Jordi AYET PUIGARNAU, director
Data primirii:	18 aprilie 2011
Destinatar:	Dl Pierre de BOISSIEU, Secretar General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2011) 225 final
Subiect:	Raport al Comisiei către Consiliu şi către Parlamentul European - Raport de evaluare referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE)

În anexă, se pune la dispoziţia delegaţiilor documentul Comisiei COM(2011) 225 final.

Anexă: COM(2011) 225 final



COMISIA EUROPEANĂ

Bruxelles, 18.4.2011
COM(2011) 225 final

RAPORT AL COMISIEI CĂTRE CONSILIU ŞI CĂTRE PARLAMENTUL EUROPEAN

Raport de evaluare referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE)

RAPORT AL COMISIEI CĂTRE CONSILIU ŞI CĂTRE PARLAMENTUL EUROPEAN

Raport de evaluare referitor la Directiva privind păstrarea datelor (Directiva 2006/24/CE)

1. INTRODUCERE

Directiva privind păstrarea datelor[1] (denumită în continuare „directiva") prevede că statele membre trebuie să impună furnizorilor de servicii de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii publice (denumiţi în continuare, „operatori") obligaţia de păstrare a datelor privind traficul şi localizarea pe o perioadă cuprinsă între şase luni şi doi ani în scopul cercetării, detectării şi urmăririi penale a infracţiunilor grave.

Prezentul raport al Comisiei evaluează, în conformitate cu articolul 14 din directivă, aplicarea acesteia de către statele membre şi impactul acesteia asupra operatorilor economici şi a consumatorilor, ţinând seama de evoluţiile ulterioare ale tehnologiei comunicaţiilor electronice şi de statisticile furnizate Comisiei, cu scopul de a stabili dacă este necesar să se modifice dispoziţiile sale, în special în ceea ce priveşte datele care intră în sfera sa de aplicare şi perioadele de păstrare. De asemenea, prezentul raport analizează implicaţiile directivei în materie de drepturi fundamentale, având în vedere criticile care au fost formulate, în general, în legătură cu păstrarea datelor şi examinează dacă sunt necesare măsuri pentru a răspunde preocupărilor asociate cu utilizarea de cartele SIM anonime în scopul comiterii de infracţiuni[2].

În general, evaluarea a demonstrat că păstrarea datelor este un instrument valoros pentru sistemele de justiţie penală şi pentru aplicarea legii în UE. Contribuţia directivei la armonizarea păstrării datelor a fost restrânsă în ceea ce priveşte, de exemplu, limitarea scopului şi perioadele de păstrare şi, de asemenea, în ceea ce priveşte domeniul rambursării costurilor suportate de către operatori, care nu intră sub incidenţa sa. Având în vedere implicaţiile şi riscurile pentru piaţa internă şi pentru respectarea dreptului la viaţă privată şi la protecţia datelor cu caracter personal, UE ar trebui să continue să asigure, prin intermediul unor norme comune, că standardele ridicate pentru stocarea, recuperarea şi utilizarea datelor privind traficul şi localizarea sunt menţinute în mod consecvent. Luând în considerare aceste concluzii, Comisia intenţionează să propună modificări la directivă, pe baza unei evaluări a impactului.

---

[1] 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 şi de modificare a Directivei 2002/58/CE, JO L 105, 13.4.2006, p. 54-63.

[2] Concluziile Consiliului privind combaterea folosirii abuzive, în scopuri infracţionale, a comunicaţiilor electronice şi a anonimatului acestora, a 2 908-a reuniune a Consiliului Justiţie şi Afaceri Interne - Bruxelles, 27-28 noiembrie 2008.

2. CONTEXTUL EVALUĂRII

Prezentul raport de evaluare se bazează pe informațiile obținute în urma discuțiilor ample purtate cu statele membre, experți și părți interesate, precum și pe contribuțiile acestora.

În mai 2009, Comisia a găzduit o conferință intitulată „Către evaluarea Directivei privind păstrarea datelor", la care au participat autorități pentru protecția datelor, sectorul privat, societatea civilă și mediul academic. În septembrie 2009, Comisia a trimis un chestionar părților interesate din rândul acestor grupuri, de la care a primit aproximativ 70 de răspunsuri[3]. În decembrie 2010, Comisia a găzduit o a doua conferință intitulată „Asumarea directivei privind păstrarea datelor", la care au participat părți interesate din categorii similare, pentru a efectua un schimb de evaluări preliminare ale directivei și a discuta despre provocările viitoare din acest domeniu.

În perioada octombrie 2009 - martie 2010, Comisia s-a întâlnit cu reprezentanți ai fiecărui stat membru și ai fiecărei țări asociate din Spațiul Economic European pentru a discuta mai amănunțit aspecte legate de aplicarea directivei. Statele membre au început să aplice directiva mai târziu decât s-a prevăzut, în special în ceea ce privește datele referitoare la internet. Ca urmare a întârzierilor în transpunere, nouă state membre au fost în măsură să furnizeze Comisiei statisticile complete prevăzute la articolul 10 din directivă pentru anul 2008 sau 2009, în timp ce, în ansamblu, 19 state membre au furnizat unele statistici (a se vedea secțiunea 4.7). În iulie 2010, Comisia s-a adresat în scris statelor membre, solicitând informații cantitative și calitative suplimentare referitoare la necesitatea de a păstra date pentru a obține rezultate în aplicarea legii. Zece state membre au oferit răspunsuri detaliate privind anumite cazuri în care datele s-au dovedit a fi necesare[4].

Prezentul raport se bazează pe documentele de poziție adoptate de grupul de experți „Platforma pentru păstrarea datelor electronice în vederea investigării, a depistării și a urmăririi penale a infracțiunilor grave", de la înființarea acestuia în 2008[5]. Comisia a luat în considerare rapoartele Grupului de lucru „articolul 29" pentru protecția datelor[6], în special raportul privind a doua acțiune de asigurare a respectării obligațiilor, și anume evaluarea conformității statelor membre în ceea ce privește cerințele prevăzute de directivă în materie de protecție și securitate a datelor[7].

---

3 Răspunsurile au fost publicate pe site-ul Comisiei (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm)

4 Belgia, Republica Cehă, Cipru, Lituania, Ungaria, Țările de Jos, Polonia, Slovenia, Regatul Unit. De asemenea, Suedia a menționat mai multe cazuri de infracțiuni grave specifice în care istoricul datelor privind traficul, care a fost disponibil deși nu exista o obligație în materie de păstrare a datelor, a fost esențial în pronunțarea hotărârilor de condamnare.

5 Acest grup de experți a fost instituit în temeiul Deciziei 2008/324/CE a Comisiei, JO L 111, 23.4.2008, p. 11-14. Comisia a avut întruniri periodice cu grupul. Documentele de poziție ale acestuia sunt publicate la următoarea adresă: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal a fost instituit în temeiul articolului 29 din Directiva privind protecția datelor (Directiva 95/46/CE a Parlamentului European și a Consiliului din 24.10.1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, JO L 281, 23.11.1995, p. 31).

7 Raportul nr. 1/2010 privind a doua acțiune comună de asigurare a respectării obligațiilor: respectarea, la nivel național, de către furnizorii de telecomunicații și de servicii de internet a obligațiilor prevăzute de

3. PĂSTRAREA DATELOR ÎN UNIUNEA EUROPEANĂ

3.1. Păstrarea datelor pentru justiția penală și în scopul aplicării legii

În cadrul activității lor, furnizorii de servicii și de rețele (denumiți în continuare „operatori”) prelucrează date cu caracter personal în scopul transmiterii unei comunicații, facturării, efectuării de plăți de interconectare, prestării de servicii de marketing și a altor servicii cu valoare adăugată. Un astfel de proces de prelucrare implică date care indică sursa, destinația, data, ora, durata și tipul comunicației, precum și echipamentele de comunicație ale utilizatorilor și, în cazul telefoniei mobile, date privind localizarea echipamentului. În temeiul Directivei 2002/58/CE asupra confidențialității și comunicațiilor electronice (denumită în continuare „Directiva privind confidențialitatea în mediul electronic”)[8], astfel de date privind traficul generate de utilizarea serviciilor de comunicații electronice trebuie, în principiu, să fie șterse sau trecute în anonimat atunci când nu mai sunt necesare pentru transmiterea unei comunicații, cu excepția cazului în care, și numai atât timp cât, acestea sunt necesare pentru facturare sau atunci când a fost obținut consimțământul abonatului sau al utilizatorului. Datele privind localizarea pot fi prelucrate doar dacă acestea sunt trecute în anonimat sau dacă se obține consimțământul utilizatorului în cauză, în măsura și pentru durata necesară în vederea furnizării unui serviciu cu valoare adăugată.

Înainte de intrarea în vigoare a directivei, sub rezerva unor condiții specifice, autoritățile naționale solicită operatorilor acordarea accesului la astfel de date, de exemplu pentru a identifica abonații care utilizează o adresă IP, pentru a analiza activitățile de comunicații și pentru a localiza un telefon mobil.

La nivelul UE, păstrarea și utilizarea datelor în scopul aplicării legii au fost abordate pentru prima dată de Directiva 97/66/CE privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor. Această directivă a prevăzut pentru prima dată posibilitatea ca statele membre să adopte astfel de măsuri legislative dacă este necesar pentru protecția securității publice, a apărării sau a ordinii publice, inclusiv a bunăstării economice a statului, atunci când activitățile se referă la securitatea statului și la aplicarea dreptului penal[9].

Dispoziția respectivă a fost dezvoltată în continuare în Directiva privind confidențialitatea în mediul electronic, care prevede posibilitatea ca statele membre să adopte măsuri legislative care derogă de la principiul confidențialității comunicațiilor, inclusiv, în anumite condiții, păstrarea, accesul și utilizarea datelor în scopul aplicării legii. În temeiul articolului 15 alineatul (1), statele membre pot restrânge sfera de aplicare a drepturilor și obligațiilor în materie de confidențialitate, inclusiv prin păstrarea datelor pentru o perioadă limitată, atunci

---

legislația națională în materie de păstrare a datelor privind traficul în baza temeiului juridic al articolelor 6 și 9 din Directiva 2002/58/CE asupra confidențialității și comunicațiilor electronice și din Directiva 2006/24/CE privind păstrarea datelor de modificare a Directivei asupra confidențialității și comunicațiilor electronice” (WP 172), 13.7.2010, (a se vedea http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

[8] Directiva Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37-47).

[9] Articolul 14 alineatul (1) din Directiva 97/66/CE a Parlamentului European și a Consiliului din 15 decembrie 1997 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor (JO L 24, 30.1.1998, p. 1–8).

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 sau a folosirii neautorizate a sistemelor de comunicaţii electronice".

Rolul pe care îl au datele păstrate în ceea ce priveşte sistemele de justiţie penală şi aplicarea legii este discutat în detaliu în secţiunea 5.

3.2. Obiectivul şi temeiul juridic al Directivei privind păstrarea datelor

Ca urmare a prevederilor Directivei 97/66/CE şi a Directivei privind confidenţialitatea în mediul electronic, care permit statelor membre să adopte legislaţie în materie de păstrare a datelor, operatorii din unele statele 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. Atacurile teroriste din Madrid, în 2004, şi din Londra, în 2005, au accelerat discuţiile la nivelul UE cu privire la modul de abordare a acestor aspecte.

În acest context, Directiva 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, şi a urmărit să armonizeze în UE anumite aspecte conexe.

Directiva a modificat articolul 15 alineatul (1) din Directiva privind confidenţialitatea în mediul electronic, prin adăugarea unui alineat care prevede că articolul 15 alineatul (1) nu se aplică datelor păstrate în temeiul Directivei privind păstrarea datelor[10]. Prin urmare, statele membre (astfel cum s-a menţionat în considerentul 12 din directivă) pot 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 directivă şi Directiva privind confidenţialitatea în mediul electronic, corelată cu lipsa unei definiţii în cele două directive a noţiunii de „infracţiune gravă", îngreunează diferenţierea, pe de o parte, a măsurilor adoptate de statele membre în vederea transpunerii obligaţiilor în materie de păstrare a datelor prevăzute în

---

[10] Articolul 11 din directivă prevede următoarele: „La articolul 15 din Directiva 2002/58/CE se inserează următorul alineat: «(1a) Alineatul (1) nu se aplică datelor solicitate în mod specific de 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 publice de comunicaţii pentru a fi păstrate în scopurile menţionate la articolul 1 alineatul (1) din această directivă.»"

directivă și, 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 privind confidențialitatea în mediul electronic[11]. Aceste aspecte sunt discutate în continuare în secțiunea 4.

Directiva se bazează pe articolul 95 din Tratatul de instituire a Comunității Europene (înlocuit de articolul 114 din Tratatul privind funcționarea Uniunii Europene) referitor la înființarea și funcționarea pieței interne. După adoptarea directivei, temeiul juridic al acesteia a fost contestat în fața Curții Europene de Justiție, în baza faptului că principalul obiectiv a fost cercetarea, detectarea și urmărirea penală a infracțiunilor grave. Curtea a hotărât că directiva a reglementat operațiuni care erau independente de punerea în aplicare a oricărei cooperări polițienești și judiciare în materie penală și că nu a armonizat nici aspectele legate de accesul la date al autorităților naționale competente, nici utilizarea și schimbul acestor datelor între autoritățile respective. Prin urmare, Curtea a concluzionat că directiva viza, în esență, activitățile operatorilor din sectorul relevant al pieței interne. În consecință, Curtea a confirmat temeiul juridic[12].

3.3. Conservarea datelor

Păstrarea datelor este diferită de conservarea datelor (cunoscută, de asemenea, sub denumirea de „înghețare rapidă"), în cazul căreia, în baza unui ordin judecătoresc, operatorii au obligația de a păstra datele referitoare numai la anumite persoane suspectate de activitate infracțională, cu începere de la data ordinului de conservare. Conservarea datelor este unul dintre instrumentele de cercetare avute în vedere și utilizate de statele participante în temeiul Convenției Consiliului Europei privind criminalitatea informatică[13]. Aproape toate statele participante au stabilit un punct de contact, al cărui rol este de a asigura furnizarea de asistență imediată în cercetările sau procedurile în materie de criminalitate informatică. Cu toate acestea, nu toate părțile la convenție par să fi prevăzut dispoziții privind conservarea datelor și eficacitatea modelului în combaterea criminalității informatice nu a fost încă evaluată[14]. Recent, a fost dezvoltat un tip de conservare a datelor cunoscut sub denumirea de „înghețare rapidă plus". Acest model depășește conservarea datelor, deoarece un judecător poate să autorizeze și accesul la datele care nu au fost încă șterse de operatori. De asemenea, în temeiul legii ar exista o exceptare foarte limitată de la obligația de a șterge, pentru o scurtă perioadă, anumite date de comunicații care nu sunt stocate în mod normal, cum ar fi date privind localizarea, date de conectare la internet și adrese IP dinamice pentru utilizatori care au un abonament forfetar și în cazul cărora nu este nevoie de stocarea datelor în scopul facturării.

Adepții conservării datelor consideră că aceasta este mai puțin invazivă decât păstrarea datelor. Cu toate acestea, majoritatea statelor membre nu sunt de acord că diferitele forme de conservare a datelor ar putea înlocui în mod corespunzător păstrarea datelor, argumentând că, în timp ce aceasta din urmă pune la dispoziție date istorice, conservarea datelor nu garantează capacitatea de a determina urmele probelor anterior emiterii ordinului de conservare, nu

---

11 Grupul de lucru „articolul 29" se întreabă dacă „obiectivul directivei [privind păstrarea datelor] a fost derogarea de la obligația generală [de a] șterge datele privind traficul în momentul încheierii comunicației electronice sau impunerea obligației de păstrare a tuturor datelor pe care furnizorii le puteau deja stoca în scopuri comerciale proprii."

12 CEJ, C-301/6 Irlanda/Parlamentul și Consiliul, Repertoriu 2009, p. I-00593.

13 Articolul 16 din Convenția privind criminalitatea informatică (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Sursă: Consiliul Europei.

permite efectuarea de cercetări în cazul în care nu se cunoaște obiectivul și nici colectarea de probe cu privire la mișcările victimelor unei infracțiuni sau ale martorilor la o infracțiune, de exemplu[15].

4. TRANSPUNEREA DIRECTIVEI PRIVIND PĂSTRAREA DATELOR

Statele membre trebuiau să transpună directiva înainte de 15 septembrie 2007, cu posibilitatea de prelungire a termenului până la 15 martie 2009 în cazul punerii în aplicare a obligațiilor în materie de păstrare a datelor referitoare la accesul la internet, poșta electronică și telefonia prin internet.

Analiza prezentată în continuare se bazează pe notificările de transpunere primite de Comisie de la 25 de state membre, inclusiv Belgia, care a transpus directiva doar parțial[16]. În Austria și Suedia se dezbat proiectele de lege în materie. În aceste două state membre, nu există nicio obligație de păstrare a datelor, dar autoritățile de aplicare a legii pot solicita și obține date privind traficul de la operatori, în măsura în care astfel de date sunt disponibile. După ce Republica Cehă, Germania și România au notificat inițial transpunerea directivei, legislația națională aferentă de transpunere a directivei a fost anulată de Curțile Constituționale din aceste țări[17] și în prezent Republica Cehă, Germania și România analizează modalitățile de retranspunere a directivei.

Prezenta secțiune analizează modul în care statele membre au transpus dispozițiile relevante ale directivei. De asemenea, examinează dacă statele membre au optat pentru rambursarea costurilor suportate de operatori în legătură cu păstrarea datelor și cu posibilitatea de recuperare a datelor, în directivă neexistând nicio dispoziție în acest sens, și abordează relevanța pentru directivă a hotărârilor pronunțate de Curțile Constituționale din Germania, România și Republica Cehă.

4.1. Scopul păstrării datelor (articolul 1)

În temeiul directivei, statele membre au obligația de a adopta măsuri care să asigure că datele sunt păstrate și sunt disponibile în vederea cercetării, detectării și urmăririi penale a infracțiunilor grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern. Cu toate acestea, scopurile indicate în legislația internă pentru păstrarea și/sau accesul la date variază în continuare în UE. Zece state membre (Bulgaria, Estonia, Irlanda, Grecia, Spania,

---

15 Acest fapt a fost recunoscut, de asemenea, de Curtea Constituțională din Germania în hotărârea sa care anula legea germană de transpunere a Directivei (a se vedea secțiunea 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 din 2 martie 2010, punctul 208).

16 Cele douăzeci și cinci de state membre care au notificat Comisia cu privire la transpunerea directivei sunt următoarele: Belgia, Bulgaria, Republica Cehă, Danemarca, Germania, Grecia, Estonia, Irlanda, Spania, Franța, Italia, Cipru, Letonia, Lituania, Luxemburg, Ungaria, Malta, Țările de Jos, Polonia, Portugalia, România, Slovenia, Slovacia, Finlanda și Regatul Unit. Belgia a informat Comisia că proiectele de lege care definitivează transpunerea se află încă în Parlament.

17 Decizia nr. 1 258 din 8 octombrie 2009 a Curții Constituționale a României, Monitorul Oficial al României nr. 789, 23 noiembrie 2009; hotărârea Bundesverfassungsgericht 1 BvR 256/08, 2 martie 2010; Monitorul Oficial din 1 aprilie 2011, hotărârea Curții Constituționale din 22 martie privind dispozițiile secțiunii 97 punctele 3 și 4 din Legea nr. 127/2005 Coll. privind comunicațiile electronice și de modificare a anumitor legi conexe modificate și Decretul nr. 485/2005 Coll. privind păstrarea și transmiterea datelor către autoritățile competente.

Lituania, Luxemburg, Ungaria, Țările de Jos, Finlanda) au definit „infracțiunile grave” prin trimitere la o pedeapsă minimă cu închisoarea, la posibilitatea impunerii unei pedepse privative de libertate sau la o listă a infracțiunilor definite în altă parte în legislația națională. Opt state membre (Belgia, Danemarca, Franța, Italia, Letonia, Polonia, Slovacia, Slovenia) prevăd obligativitatea păstrării datelor nu numai în vederea cercetării, detectării și urmăririi penale în legătură cu infracțiunile grave, ci și în legătură cu toate infracțiunile, precum și pentru prevenirea criminalității sau din motive generale de securitate națională ori de stat și/sau securitate publică. Legislația a patru state membre (Cipru, Malta, Portugalia, Regatul Unit) se referă la „infracțiuni grave” sau la „delicte grave”, fără a le defini. Date detaliate sunt prezentate în tabelul 1.

Tabelul 1: limitarea scopului pentru păstrarea datelor, în legislațiile naționale	
Belgia	Pentru cercetarea și urmărirea penală a infracțiunilor, urmărirea penală a abuzurilor de numere de telefon ale serviciilor de urgență, cercetarea pentru utilizarea abuzivă a rețelei sau a serviciului de comunicații electronice, în scopul misiunilor de culegere de informații întreprinse de serviciile de informații și de securitate[18].
Bulgaria	Pentru „descoperirea și cercetarea infracțiunilor grave și a infracțiunilor prevăzute la articolul 319 literele (a)-(f) din Codul Penal, precum și pentru căutarea persoanelor”[19].
Republica Cehă	Directiva nu a fost transpusă.
Danemarca	Pentru cercetarea și urmărirea în justiție a faptelor penale[20].
Germania	Directiva nu a fost transpusă.
Estonia	Poate fi utilizată în cazul în care colectarea probelor în temeiul altor acte procedurale este exclusă sau deosebit de complicată și în cazul în care obiectul unei proceduri penale este o infracțiune [de gradul întâi sau o infracțiune de gradul al doilea comisă cu intenție și sancționată cu o pedeapsă cu închisoarea de cel puțin trei ani][21].
Irlanda	Pentru prevenirea infracțiunilor grave [și anume infracțiunile care sunt pasibile de o pedeapsă cu închisoarea de 5 ani sau mai mult sau o infracțiune menționată în anexa la legea de transpunere], apărarea securității statului, salvarea de vieți omenești[22].
Grecia	În scopul detectării infracțiunilor deosebit de grave[23].
Spania	Pentru detectarea, cercetarea și urmărirea penală a infracțiunilor grave prevăzute în Codul Penal sau în legile penale speciale[24].

18 Articolul 126 alineatul (1) din Legea privind comunicațiile electronice, 13 iunie 2005.
19 Articolul 250a alineatul (2) din Legea comunicațiilor electronice (modificată), 2010.
20 Articolul 1 din Ordinul privind păstrarea datelor.
21 Subsecțiunea 110 punctul 1 din Codul de procedură penală.
22 Articolul 6 din Legea comunicațiilor (Legea privind păstrarea datelor), 2011.
23 Astfel de infracțiuni sunt definite la articolul 4 din Legea 2 225/1994 și articolul 1 din Legea 3 917/2011.
24 Articolul 1 alineatul (1) din Legea 25/2007.

Tabelul 1: limitarea scopului pentru păstrarea datelor, în legislațiile naționale	
Franța	Pentru detectarea, cercetarea și urmărirea penală a infracțiunilor, în scopul unic de a oferi autorităților judiciare informațiile necesare, precum și pentru prevenirea actelor de terorism și protejarea proprietății intelectuale[25].
Italia	Pentru detectarea și reprimarea infracțiunilor[26].
Cipru	Pentru cercetarea unei infracțiuni grave[27].
Letonia	Pentru protejarea securității de stat și a securității publice sau pentru a asigura cercetarea infracțiunilor, urmărirea penală și procedurile penale[28].
Lituania	Pentru cercetarea, detectarea și urmărirea penală a infracțiunilor grave și foarte grave, astfel cum sunt definite în Codul Penal lituanian[29].
Luxemburg	Pentru detectarea, cercetarea și urmărirea penală a infracțiunilor pasibile de o pedeapsă penală de maximum un an sau mai mult[30].
Ungaria	Pentru a permite organismelor de cercetare, procurorului, instanțelor și agențiilor naționale de securitate să își îndeplinească atribuțiile și pentru a permite poliției și Oficiului Național al Impozitelor și Vămilor să cerceteze infracțiunile comise cu premeditare, pasibile de o pedeapsă cu închisoarea de cel puțin doi ani[31].
Malta	Pentru cercetarea, detectarea sau urmărirea penală a infracțiunilor grave[32].
Țările de Jos	Pentru cercetarea și urmărirea penală a infracțiunilor grave, pasibile de pedeapsă privativă de libertate[33].
Austria	Directiva nu a fost transpusă.
Polonia	Pentru prevenirea sau detectarea infracțiunilor, pentru prevenirea și detectarea delictelor fiscale, pentru utilizarea de către procurori și instanțe dacă sunt relevante pentru procedurile judiciare în curs, pentru executarea îndatoririlor care revin Agenției Interne de Securitate, Agenției Externe de Informații, Biroului Central Anticorupție, serviciilor militare de contraspionaj și serviciilor militare de informații[34].

25 Legile care reglementează utilizarea datelor păstrate, respectiv, pentru infracțiuni, pentru prevenirea actelor de terorism și pentru protejarea proprietății intelectuale sunt următoarele: articolul L.34-1(II) din CPCE, Legea nr. 2006-64, 23 ianuarie 2006 și Legea nr. 2009-669, 12 iunie 2009.

26 Articolul 132 alineatul (1) din Codul privind protecția datelor.

27 Articolul 4 alineatul (1) din Legea 183(I)/2007.

28 Articolul 71 alineatul (1) din Legea comunicațiilor electronice.

29 Articolul 65 din Legea X-1835.

30 Articolul 1 alineatul (1) din legea din 24 iulie 2010.

31 Pentru scopul general de păstrare a datelor - articolul 159/A din Legea C/2003, modificată de Legea CLXXIV/2007; în ceea ce privește scopul de acces al poliției - articolul 68 din Legea XXXIV/1994; în ceea ce privește scopul de acces al Oficiului Național al Impozitelor și Vămilor, articolul 59 din Legea CXXII/2010.

32 Articolul 20 alineatul (1) din Avizul juridic nr. 198/2008.

33 Articolul 126 din Codul de procedură penală.

34 Articolul 180a din Legea telecomunicațiilor din 16 iulie 2004, modificată prin articolul 1 din legea din 24 aprilie 2009.

Tabelul 1: limitarea scopului pentru păstrarea datelor, în legislațiile naționale	
Portugalia	Pentru cercetarea, detectarea și urmărirea penală a infracțiunilor grave[35].
România	Directiva nu a fost transpusă.
Slovenia	Pentru asigurarea securității naționale, reglementare constituțională, pentru interesele în materie de securitate, interesele politice și economice ale statului ... precum și în scopul apărării naționale[36].
Slovacia	Pentru prevenirea, cercetarea, detectarea și urmărirea penală a infracțiunilor[37].
Finlanda	Pentru cercetarea, detectarea și urmărirea penală a infracțiunilor grave, conform capitolului 5a, articolul 3 alineatul (1) din Legea privind măsurile coercitive[38].
Suedia	Directiva nu a fost transpusă.
Regatul Unit	Pentru cercetarea, detectarea și urmărirea penală a infracțiunilor grave[39].

Majoritatea statelor membre care au transpus directiva, în conformitate cu legislația națională, permit accesul la datele păstrate și utilizarea acestora în scopuri care depășesc cadrul directivei, inclusiv prevenirea și combaterea criminalității, în general, și a riscurilor la adresa vieții și integrității corporale. Deși acest lucru este permis în temeiul Directivei privind confidențialitatea în mediul electronic, gradul de armonizare realizat de legislația UE în acest domeniu rămâne limitat. Este probabil ca diferențele în ceea e privește scopurile păstrării datelor să afecteze volumul și frecvența cererilor și, în consecință, costurile suportate pentru respectarea obligațiilor prevăzute în directivă. În plus, această situație poate să nu furnizeze în suficientă măsură un caracter previzibil, acesta fiind o cerință a oricărei măsuri legislative care restrânge dreptul la viață privată[40]. Comisia va evalua necesitatea atingerii unui grad mai ridicat de armonizare în acest domeniu, precum și opțiunile pentru realizarea acestuia[41].

35 Articolul 1 și articolul 3 alineatul (1) din Legea 32/2008.

36 Articolul 170a alineatul (1) din Legea comunicațiilor electronice.

37 Articolul 59a alineatul (6) din Legea comunicațiilor electronice.

38 Articolul 14a alineatul (1) din Legea comunicațiilor electronice.

39 Reglementările privind păstrarea datelor (Directiva CE) din 2009 (2009 nr. 859).

40 Hotărârea Curții Europene de Justiție din 20 mai 2003 în cauzele conexate C-465/00, C-138/01 și C-139/01 (referință pentru o hotărâre preliminară a Verfassungsgerichtshof și a Oberster Gerichtshof): Rechnungshof (C-465/00)/Österreichischer Rundfunk și alții, precum și Christa Neukomm/Österreichischer Rundfunk (C-138/01) și Joseph Lauermann/Österreichischer Rundfunk (C-139/01) (Protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal — Directiva 95/46/CE — Protecția vieții private — Divulgarea datelor privind veniturile angajaților unor organisme care fac obiectul controlului Rechnungshof).

41 Cu privire la adoptarea directivei, Comisia a publicat o declarație care sugerează că ar trebui luată în considerare lista infracțiunilor care face obiectul mandatului european de arestare. (Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre).

4.2. Operatorii care au obligația de a respecta cerințele în materie de păstrare a datelor (articolul 1)

Directiva se aplică în cazul „furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice” [articolul 1 alineatul (1)]. Două state membre (Finlanda, Regatul Unit) nu impun operatorilor mici obligația de păstrare a datelor, deoarece, în opinia lor, atât furnizorul, cât și statul ar trebui să suporte costurile care depășesc beneficiile generate pentru sistemele de justiție penală și pentru aplicarea legii. Patru state membre (Letonia, Luxemburg, Țările de Jos, Polonia) menționează că au pus în aplicare măsuri administrative alternative. În timp ce marii operatori prezenți în mai multe state membre beneficiază de economii de scară în ceea ce privește costurile, operatorii mai mici din unele state membre tind să creeze întreprinderi comune sau să externalizeze funcțiile de păstrare și recuperare a datelor către societăți specializate, în scopul reducerii costurilor. O astfel de externalizare a funcțiilor tehnice în acest mod nu afectează obligația furnizorilor de a supraveghea în mod corespunzător operațiunile de prelucrare și de a asigura instituirea măsurilor de securitate necesare, care poate ridica probleme, în special, operatorilor mai mici. Comisia va analiza aspectele referitoare la securitatea datelor și impactul asupra întreprinderilor mici și mijlocii, în ceea ce privește opțiunile de modificare a cadrului privind păstrarea datelor.

4.3. Accesul la date: autorități, proceduri și condiții (articolul 4)

Statele membre au obligația de „a se asigura că [datele păstrate] sunt furnizate numai autorităților naționale competente în cazuri specifice și în conformitate cu dreptul intern.” Statele membre sunt cele care definesc în legislația lor națională „procedurile care trebuie să fie urmate și condițiile care trebuie să fie îndeplinite pentru a obține acces la datele păstrate în conformitate cu cerințele de necesitate și proporționalitate, sub rezerva dispozițiilor relevante ale dreptului Uniunii Europene sau ale dreptului internațional public, și, în special, a dispozițiilor CEDO, astfel cum au fost interpretate de către Curtea Europeană pentru Drepturile Omului”.

În toate statele membre, forțele naționale de poliție și, cu excepția jurisdicțiilor de drept cutumiar (Irlanda și Regatul Unit), procurorii pot avea acces la datele păstrate. Paisprezece state membre citează serviciile de securitate, serviciile de informații sau serviciile militare printre autoritățile competente. Șase state membre menționează autorități fiscale și/sau vamale, iar trei citează autorități de frontieră. Un stat membru permite altor autorități publice să aibă acces la date, în cazul în care acestea sunt autorizate în scopuri specifice în temeiul legislației secundare. În unsprezece state membre este necesară autorizarea judiciară pentru fiecare cerere de acces la datele păstrate. În trei state membre este necesară autorizarea judiciară în majoritatea cazurilor. Alte patru state membre solicită ca autorizarea să fie acordată de o autoritate de înalt nivel, dar nu de un judecător. În două state membre, singura condiție pare a fi ca cererea să fie formulată în scris.

Tabelul 2: acces la datele privind telecomunicațiile care au fost păstrate		
	Autorități naționale competente	*Proceduri și condiții*
Belgia	Unitatea judiciară de coordonare, judecătorii de instrucție, procurorul, poliția judiciară.	Accesul trebuie autorizat de un magistrat sau un procuror. La cerere, operatorii trebuie să furnizeze „în timp real” datele referitoare la abonat și datele privind traficul și localizarea pentru apelurile telefonice efectuate în ultima lună. Datele privind apelurile telefonice mai vechi

Tabelul 2: acces la datele privind telecomunicațiile care au fost păstrate		
	Autorități naționale competente	*Proceduri și condiții*
		trebuie să fie furnizate cât mai curând posibil.
Bulgaria[42]	Direcțiile și departamentele specifice din cadrul Agenției de Stat pentru Securitate Națională, Ministerului de Interne, Serviciului de Informații Militare, Serviciului Poliției Militare, Ministrului Apărării, Agenției Naționale de Cercetări; autoritățile judiciare și cele care își desfășoară activitatea în etapa de precontencios, cu anumite condiții.	Accesul este posibil doar în baza ordinului emis de președintele unei instanțe regionale.
Republica Cehă	Directiva nu a fost transpusă.	
Danemarca[43]	Poliția.	Accesul necesită autorizare judiciară; ordinele judecătorești se emit în cazul în care cererea îndeplinește criterii stricte în materie de suspiciune, necesitate și proporționalitate.
Germania	Directiva nu a fost transpusă.	
Estonia[44]	Poliția și Direcția Poliției de Frontieră, Direcția Poliției de Securitate, iar pentru obiecte și comunicații electronice, Direcția Impozite și Vămi.	Accesul necesită autorizare din partea unui judecător de instrucție. Operatorii trebuie să „furnizeze [datele păstrate] în cazurile urgente în cel mult 10 ore și în celelalte cazuri în termen de 10 zile lucrătoare [de la primirea cererii]”.
Irlanda[45]	Membrii ai poliției *(Garda Síochána)*, cu grad de comisar-șef sau cu grad superior; ofițeri din cadrul Forțelor Permanente de Apărare, cu grad de colonel sau cu grad superior; ofițeri din cadrul Administrației Fiscale, cu grad de ofițer principal sau cu grad superior.	Cererile trebuie formulate în scris.
Grecia[46]	Autoritățile publice judiciare, militare sau de poliție.	Accesul necesită o hotărâre judecătorească prin care se declară că efectuarea cercetărilor prin alte mijloace este imposibilă sau extrem de dificilă.
Spania[47]	Forțele de poliție responsabile de detectarea, cercetarea și urmărirea penală a infracțiunilor grave, Centrul Național de Informații și Agenția Vămilor.	Pentru a avea acces la aceste date, autoritățile naționale competente trebuie să primească în prealabil o autorizare judiciară.
Franța[48]	Procurorul, ofițeri de poliție desemnați și jandarmi desemnați.	Poliția trebuie să furnizeze o justificare pentru fiecare cerere de acces la datele păstrate și trebuie să solicite autorizare din partea persoanei din cadrul Ministerului de Interne care a fost desemnată de *Commission nationale de contrôle des interceptions de sécurité*. Cererile de acces sunt gestionate de un ofițer desemnat care lucrează pentru operator.

42 Articolul 250b alineatul (1) din Legea privind comunicațiile electronice (modificată), 2010 (autorități); articolul 250b alineatul (1) și articolul 250c alineatul (1) din Legea privind comunicațiile electronice (modificată), 2010 (acces).

43 Capitolul 71 din Legea privind administrarea actului de justiție.

44 Subsecțiunea 112 punctele 2 și 3 din Codul de procedură penală (cu privire la autorități și procedură); subsecțiunea 111 punctul 9 din Legea comunicațiilor electronice.

45 Articolul 6 din Legea comunicațiilor (păstrarea datelor), 2009.

46 Articolele 3 și 4 din Legea 2 225/94.

47 Articolele 6 - 7 din Legea 25/2007.

Tabelul 2: acces la datele privind telecomunicațiile care au fost păstrate		
	Autorități naționale competente	*Proceduri și condiții*
Italia[49]	Procurorul; poliția; avocatul apărării fie pentru pârât, fie pentru persoana care face obiectul cercetării.	Accesul necesită o „ordonanță motivată”, emisă de procuror.
Cipru[50]	Instanțele, procurorul, poliția.	Accesul trebuie aprobat de un procuror, dacă acesta consideră că astfel pot fi furnizate probe cu privire la săvârșirea unei infracțiuni grave. Un judecător poate emite un ordin de acest tip în cazul în care există o suspiciune rezonabilă cu privire la o infracțiune gravă și în cazul în care datele pot fi asociate cu aceasta.
Letonia[51]	Ofițerii autorizați din cadrul instituțiilor de cercetare în etapa de precontencios; persoanele care desfășoară o activitate de cercetare; ofițerii autorizați din cadrul instituțiilor de securitate de stat; Ministerul Public; instanțele.	Ofițerii autorizați, Ministerul Public și instanțele trebuie să evalueze „caracterul adecvat și relevanța” cererii, să înregistreze cererea și să asigure protecția datelor obținute. Organismele autorizate pot semna un acord cu un operator, de exemplu, pentru criptarea datelor furnizate.
Lituania[52]	Organismele de cercetare în etapa de precontencios, procurorul, instanța de judecată (judecătorii) și ofițerii de informații.	Autoritățile publice autorizate trebuie să solicite în scris furnizarea datelor păstrate. Pentru a obține accesul în cadrul cercetărilor din etapa de precontencios, este necesar un mandat judiciar.
Luxemburg[53]	Autoritățile judiciare (judecătorii de instrucție, procurorul), autoritățile responsabile de garantarea securității statului, de apărare, de siguranța publică, precum și de prevenirea, cercetarea, detectarea și urmărirea penală a infracțiunilor.	Accesul necesită autorizare judiciară.
Ungaria[54]	Poliția, Oficiul Național al Impozitelor și Vămilor, serviciile de naționale de securitate, procurorul, instanțele.	Poliția și Oficiul Național al Impozitelor și Vămilor trebuie să aibă autorizare din partea procurorului. Procurorul și agențiile naționale de securitate pot accesa astfel de date fără un ordin judecătoresc.
Malta[55]	Forța de poliție din Malta; Serviciul de securitate.	Cererile trebuie formulate în scris.
Țările de Jos[56]	Ofițerul de poliție care cercetează.	Accesul trebuie să fie acordat printr-un ordin al unui procuror sau al unui judecător de instrucție.
Austria	Directiva nu a fost transpusă.	

48 Articolele 60-1 și 60-2 din Codul de procedură penală (autorități); articolul L.31-1-1 (condiții).

49 Articolul 132 alineatul (3) din Codul privind protecția datelor.

50 Articolul 4 alineatul (2) și articolul 4 alineatul (4) din Legea 183 (I)/2007 .

51 Articolul 71 alineatul (1) din Legea comunicațiilor electronice (autorități); Regulamentul Cabinetului nr. 820 (proceduri).

52 Articolul 77 alineatele (1) și (2) din Legea X-1 835; raport verbal prezentat Comisiei.

53 Articolul 5-2 alineatul (1) și articolul 9 alineatul (2) din legea din 24 iulie 2010 (autorități); articolul 67 – 1 din Codul de instrucție penală (condiții).

54 Articolul 68 alineatul (1) și articolul 69 alineatul (1) literele (c) și (d) din Legea XXXIV, 1994; articolul 9/A alineatul (1) din Legea V, 1972; articolul 71 alineatele (1), (3), (4), articolul 178/A alineatul (4), articolul 200, articolul 201 și articolul 268 alineatul (2) din Legea XIX, 1998; articolul 40 alineatele (1) și (2), articolul 53 alineatul (1) și articolul 54 alineatul (1) litera (j) din Legea CXXV, 1995.

55 Articolul 20 alineatul (1), articolul 20 alineatul (3) din Avizul juridic nr. 198/2008.

56 Articolul 126ni din Codul de procedură penală.

Tabelul 2: acces la datele privind telecomunicațiile care au fost păstrate		
	Autorități naționale competente	*Proceduri și condiții*
Polonia[57]	Poliția, polițiștii de frontieră, inspectorii fiscali, Agenția de Securitate Internă, Agenția de Informații Externe, Biroul Central Anticorupție, serviciile militare de contrainformații, serviciile militare de informații, instanțele și procurorul.	Cererile trebuie să fie formulate în scris, iar în cazul poliției, al polițiștilor de frontieră și al inspectorilor fiscali, cererile trebuie autorizate de un înalt funcționar din cadrul organizației.
Portugalia[58]	Poliția judiciară, Garda Republicană Națională, Oficiul de Securitate Publică, poliția judiciară militară, Serviciul pentru imigrație și frontiere, poliția maritimă.	Transmiterea datelor necesită autorizare judiciară prin care se constată că accesul este esențial pentru descoperirea adevărului sau că probele ar fi, în orice alt mod, imposibil sau foarte greu de obținut. Autorizarea judiciară este eliberată sub rezerva îndeplinirii unor cerințe în materie de necesitate și proporționalitate.
România	Directiva nu a fost transpusă.	
Slovenia[59]	Poliția, agențiile de informații și securitate, agențiile de apărare responsabile de informații și contrainformații, precum și de misiuni de securitate.	Accesul necesită autorizare judiciară.
Slovacia[60]	Autoritățile de aplicare a legii, instanțele.	Cererile trebuie formulate în scris.
Finlanda[61]	Poliția, polițiștii de frontieră, autoritățile vamale (pentru datele privind abonații, traficul și localizarea care au fost păstrate). Centrul pentru Situații de Urgență, Centrul pentru operațiuni de salvare marină, Subcentrul pentru operațiuni de salvare marină (pentru datele privind identificarea și localizarea în situații de urgență).	Datele privind abonații pot fi accesate de toate autoritățile competente fără autorizare judiciară. Pentru alte categorii de date este necesar un ordin judecătoresc.
Suedia	Directiva nu a fost transpusă.	
Regatul Unit[62]	Poliția, serviciile de informații, autoritățile fiscale și vamale, alte autorități publice desemnate în legislația secundară.	Se acordă acces la date sub rezerva autorizării de către o „persoană desemnată” și a respectării condițiilor privind necesitatea și proporționalitatea, în cazuri specifice și în condițiile în care divulgarea datelor este permisă sau impusă prin lege. Împreună cu operatorii s-a convenit asupra unor proceduri specifice.

Comisia va evalua necesitatea atingerii unui grad mai ridicat de armonizare, precum și opțiunile pentru realizarea acestuia, în ceea ce privește autoritățile care au acces la datele păstrate și procedurile pentru obținerea accesului la datele păstrate. Printre opțiuni s-ar putea

---

57 Articolul 179 alineatul (3) din Legea telecomunicațiilor din 16 iulie 2004, modificată prin articolul 1 din legea din 24 aprilie 2009.

58 Articolul 2 alineatul (1), articolul 3 alineatul (2) și articolul 9 din Legea 32/2008.

59 Articolul 107c din Legea comunicațiilor electronice; articolul 149b din Codul de procedură penală; articolul 24 litera (b) din Legea privind Agenția de Informații și Securitate; articolul 32 din Legea apărării.

60 Articolul 59a alineatul (8) din Legea comunicațiilor electronice.

61 Articolul 35 alineatul (1), articolul 36 din Legea comunicațiilor electronice; articolul 31-33 din Legea Poliției; Articolul 41 din Legea poliției de frontieră.

62 Articolul 25 din anexa 1 la Legea privind reglementarea atribuțiilor de cercetare, 2000; articolul 7 din Regulamentul privind păstrarea datelor; articolul 22 alineatul (2) din Legea privind reglementarea atribuțiilor de cercetare prevede scopurile în care aceste autorități pot obține datele.

număra liste care să definească mai clar autoritățile competente, supravegherea independentă și/sau judiciară a cererilor de date și un standard minim al procedurilor care trebuie respectate de operatori pentru a acorda acces autorităților competente.

4.4. Domeniul de aplicare al păstrării datelor și categoriile de date vizate [articolul 1 alineatul (2), articolul 3 alineatul (2) și articolul 5]

Directiva se aplică rețelei de telefonie fixă, telefoniei mobile, accesului la internet, poștei electronice și telefoniei prin internet. Directiva menționează (la articolul 5) categoriile de date care trebuie păstrate, în principal date necesare pentru a identifica:

(a) sursa unei comunicații;

(b) destinația unei comunicații;

(c) data, ora și durata unei comunicații;

(d) tipul unei comunicații;

(e) echipamentul de comunicație al utilizatorilor sau la ce servește echipamentul acestora și

(f) locația echipamentului de comunicație mobilă.

Directiva reglementează, de asemenea, [articolul 3 alineatul (2)] încercările nereușite de apeluri telefonice, respectiv o comunicație în care un apel telefonic a fost conectat cu succes, dar nu a primit răspuns sau o comunicație în care a avut loc o intervenție a sistemului de gestionare a rețelei, precum și situațiile în care datele privind aceste încercări sunt generate sau prelucrate și păstrate sau înregistrate în jurnalul electronic de către operatori. În temeiul directivei, nu se pot păstra date care dezvăluie conținutul comunicației. De asemenea, s-a precizat ulterior că nici solicitările de căutare, respectiv jurnalele electronice ale serverelor generate prin furnizarea unui serviciu de motor de căutare, nu se încadrează în domeniul de aplicare al directivei, deoarece acestea sunt considerate mai degrabă date privind conținutul, decât date privind traficul[63].

Douăzeci și unu de state membre prevăd păstrarea fiecăreia dintre aceste categorii de date în legislația lor de transpunere. Belgia nu a precizat tipurile de date de telefonie care trebuie păstrate și nici nu a prevăzut dispoziții în materie de date referitoare la internet. Persoanele care au răspuns la chestionarul Comisiei nu au considerat că este necesar să se modifice categoriile de date care trebuie păstrate, deși Parlamentul European a adresat Comisiei o declarație scrisă, prin care lansa apelul de extindere a domeniului de aplicare a directivei în vederea includerii motoarelor de căutare „pentru a putea combate rapid și eficace pornografia infantilă și hărțuirea sexuală online”[64]. În raportul său privind a doua acțiune de asigurare a respectării obligațiilor, Grupul de lucru „articolul 29” pentru protecția datelor a susținut că

---

63 Avizul Grupului de lucru „articolul 29” pentru protecția datelor privind motoarele de căutare, 4 aprilie 2008.

64 Declarație scrisă depusă în conformitate cu articolul 123 din Regulamentul de procedură privind crearea unui sistem european de alertă rapidă (SEAR) împotriva pedofililor și a autorilor actelor de hărțuire sexuală, 19.4.2010, 29/2010.

acele categorii stabilite în directivă ar trebui considerate exhaustive, fără a impune operatorilor obligații suplimentare în materie de păstrare a datelor. Comisia va evalua necesitatea tuturor acestor categorii de date.

4.5. Perioade de păstrare (articolul 6 și articolul 12)

Statele membre au obligația de a se asigura că acele categorii de date precizate la articolul 5 sunt păstrate pe perioade de cel puțin șase luni și de cel mult doi ani. Perioada maximă de păstrare poate fi prelungită de un stat membru care „se confruntă cu situații specifice care justifică extinderea pe o perioadă limitată”; o astfel de prelungire trebuie comunicată Comisiei care, în termen de șase luni de la data notificării, poate decide să o aprobe sau să o respingă. Dacă perioada maximă de păstrare poate fi prelungită, nicio dispoziție nu prevede reducerea duratei de păstrare la mai puțin de șase luni. Toate statele membre care au transpus directiva, cu excepția unuia, aplică o perioadă de păstrare sau perioade de păstrare în aceste limite și Comisia nu a primit nicio notificare de prelungire. Cu toate acestea, nu există o abordare consecventă în UE.

Cincisprezece state membre prevăd o perioadă unică pentru toate categoriile de date: un stat membru (Polonia) prevede o perioadă de păstrare de doi ani, un stat membru prevede 1,5 ani (Letonia), zece state membre prevăd un an (Bulgaria, Danemarca, Estonia, Grecia, Spania, Franța, Țările de Jos, Portugalia, Finlanda, Regatul Unit) și trei state membre prevăd șase luni (Cipru, Luxemburg, Lituania). Cinci state membre au definit perioade diferite de păstrare în funcție de categoriile de date: două state membre (Irlanda, Italia) prevăd doi ani pentru datele de telefonie fixă și mobilă și un an pentru datele privind accesul la internet, poșta electronică și telefonia prin internet; un stat membru (Slovenia) indică 14 luni pentru datele de telefonie și opt luni pentru datele referitoare la internet; un stat membru (Slovacia) prevede un an pentru telefonia fixă și mobilă și șase luni pentru datele referitoare la internet; un stat membru (Malta) prevede un an pentru datele privind telefonia fixă, mobilă și prin internet și șase luni pentru accesul la internet și poșta electronică. Un stat membru (Ungaria) păstrează toate datele timp de un an, cu excepția datelor privind încercările nereușite de apeluri telefonice care sunt păstrate doar șase luni. Un stat membru (Belgia) nu a prevăzut nicio perioadă de păstrare a datelor pentru categoriile de date precizate în directivă. În tabelul 3 sunt prezentate detalii.

Tabelul 3: perioade de păstrare prevăzute în legislația națională	
Belgia[65]	Între 1 an și 36 de luni pentru serviciile de telefonie „accesibile publicului”. Nu există dispoziții în materie de date referitoare la internet.
Bulgaria	1 an. Datele pentru care s-a acordat accesul pot fi păstrate încă 6 luni, în baza unei cereri.
Republica Cehă	Directiva nu a fost transpusă.
Danemarca	1 an
Germania	Directiva nu a fost transpusă.
Estonia	1 an
Irlanda	2 ani pentru datele privind telefonia fixă și mobilă, 1 an pentru datele privind accesul la internet, poșta electronică și telefonia prin internet
Grecia	1 an
Spania	1 an
Franța	1 an

[65] Articolul 126 alineatul (2) din Legea privind comunicațiile electronice, 13 iunie 2005.

Tabelul 3: perioade de păstrare prevăzute în legislația națională	
Italia	2 ani pentru datele privind telefonia fixă și mobilă, 1 an pentru datele privind accesul la internet, poșta electronică și telefonia prin internet
Cipru	6 luni
Letonia	18 luni
Lituania	6 luni
Luxemburg	6 luni
Ungaria	6 luni pentru apelurile telefonice nereușite și 1 an pentru toate celelalte date
Malta	1 an pentru datele privind telefonia fixă, mobilă și telefonia prin internet, 6 luni pentru datele privind accesul la internet și poșta electronică
Țările de Jos	1 an
Austria	Directiva nu a fost transpusă.
Polonia	2 ani
Portugalia	1 an
România	Directiva nu a fost transpusă (6 luni în conformitate cu legislația de transpunere anterioară care a fost anulată)
Slovenia	14 luni pentru datele de telefonie și 8 luni pentru datele referitoare la internet
Slovacia	1 an pentru datele de telefonie fixă și mobilă, 6 luni pentru datele privind accesul la internet, poșta electronică și telefonia prin internet
Finlanda	1 an
Suedia	Directiva nu a fost transpusă
Regatul Unit	1 an

Deși această diversitate de abordare este permisă de directivă, rezultatul este că directiva oferă doar un nivel restrâns de securitate juridică și un caracter previzibil limitat în UE pentru operatorii care își desfășoară activitatea în mai multe state membre și pentru cetățenii ale căror date privind comunicațiile pot fi stocate în state membre diferite. Luând în considerare gradul tot mai ridicat de internaționalizare a prelucrării datelor și externalizarea stocării datelor, ar trebui avute în vedere opțiuni pentru armonizarea suplimentară a perioadelor de păstrare a datelor în UE. În vederea respectării principiului proporționalității, luând în considerare probele cantitative și calitative privind importanța datelor păstrate în statele membre și ținând cont de tendințele înregistrate în materie de comunicații și tehnologie, precum și în materie de criminalitate și terorism, Comisia va avea în vedere stabilirea de perioade diferite în funcție de categoriile de date sau infracțiuni grave sau pentru o combinație a acestor două criterii[66]. Probele cantitative furnizate până în prezent de statele membre cu privire la vechimea datelor păstrate sugerează că aproximativ 90 % din date au o vechime de cel mult șase luni și aproximativ 70 % au o vechime de cel mult trei luni atunci când cererea (inițială) de acces a fost depusă de autoritățile de aplicare a legii (a se vedea secțiunea 5.2).

4.6. Protecția și securitatea datelor și autoritățile de supraveghere (articolele 7 și 9)

În temeiul directivei, statele membre au obligația de a se asigura că operatorii respectă, cel puțin la nivel minim, patru principii de securitate a datelor, și anume, că datele păstrate:

(a) sunt de aceeași calitate și sunt supuse aceleiași securități și protecții ca și datele din rețeaua [publică de comunicații];

[66] Propunerea de directivă a Comisiei privind păstrarea datelor, din 2005, prevedea o perioadă de păstrare de un an pentru datele de telefonie și de șase luni pentru datele referitoare la internet.

(b) sunt supuse măsurilor tehnice și organizaționale 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 și organizaționale adecvate pentru a se asigura că accesarea acestora poate fi făcută numai de către personal special autorizat; și

(d) sunt distruse la finalul perioadei de păstrare, cu excepția celor care au fost accesate și reținute [în scopul stabilit în directivă].

În conformitate cu Directiva privind protecția datelor și cu Directiva privind confidențialitatea în mediul electronic, este interzis ca operatorii să prelucreze în alte scopuri datele păstrate în temeiul directivei, cu condiția ca datele să nu fi fost altfel păstrate[67]. Statele membre au obligația de a desemna o autoritate publică care să răspundă de monitorizarea, în mod absolut independent, a aplicării acestor principii, această autoritate putând fi aceeași ca cea prevăzută în temeiul Directivei privind protecția datelor[68].

Cincisprezece state membre au transpus toate aceste principii în legislația relevantă. Patru state membre (Belgia, Estonia, Spania, Letonia) au transpus două sau trei dintre aceste principii, dar nu prevăd în mod explicit dispoziții privind distrugerea datelor la expirarea perioadei de păstrare. Două state membre (Italia, Finlanda) prevăd distrugerea datelor. Nu este clar care dintre măsurile de securitate tehnice și organizaționale specifice, cum ar fi autentificarea puternică și gestionarea detaliată a jurnalelor electronice de acces[69], au fost aplicate. Douăzeci și două de state membre au o autoritate de supraveghere care răspunde de monitorizarea aplicării principiilor. În majoritatea cazurilor, aceasta este autoritatea pentru protecția datelor. În tabelul 4 sunt prezentate detalii.

Tabelul 4: protecția și securitatea datelor și autoritățile de supraveghere

Stat membru	*Dispoziții privind protecția și securitatea datelor în legislația națională*	*Autoritatea de supraveghere*
Belgia	Operatorii trebuie să asigure că transmiterea datelor nu poate fi interceptată de un terț și că este conformă cu standardele ETSI pentru securitatea telecomunicațiilor și interceptarea legală[70]. Principiul de distrugere obligatorie a datelor la expirarea perioadei de păstrare nu pare să fie luat în considerare.	Institutul pentru Servicii Poștale și Telecomunicații

67 Articolul 13 alineatul (1) din Directiva 95/46/CE.

68 Articolul 28 din Directiva 95/46/CE.

69 Autentificarea puternică implică mecanisme de autentificare dual, cum ar fi parolă plus date biometrice sau parolă plus cod, pentru a asigura prezența fizică a persoanei însărcinate cu prelucrarea datelor privind traficul. Gestionarea detaliată a jurnalelor electronice de acces implică urmărirea detaliată a accesului și a operațiunilor de prelucrare prin intermediul păstrării jurnalelor electronice care înregistrează identitatea utilizatorului, ora accesării și fișierele accesate.

70 Articolul 6 din Decretul regal, 9 ianuarie 2003.

Tabelul 4: protecția și securitatea datelor și autoritățile de supraveghere		
Stat membru	*Dispoziții privind protecția și securitatea datelor în legislația națională*	*Autoritatea de supraveghere*
Bulgaria	Legea de transpunere include obligația de a pune în aplicare cele patru principii[71].	Comisia pentru protecția datelor cu caracter personal monitorizează prelucrarea și stocarea datelor pentru a asigura îndeplinirea obligațiilor; comisia parlamentară a Adunării Naționale – monitorizează procedurile de autorizare și acces la date.
Republica Cehă[72]	Directiva nu a fost transpusă.	
Danemarca	Cele patru principii sunt prevăzute [73].	Agenția Națională pentru Tehnologia Informației și Telecomunicații monitorizează obligația furnizorilor de rețele și servicii de comunicații electronice de a asigura că echipamentele și sistemele tehnice permit accesul poliției la informații privind traficul telecomunicațiilor.
Germania	Directiva nu a fost transpusă.	
Estonia	Legea de transpunere prevede trei din cele patru principii. Nu există nicio dispoziție explicită privind al patrulea principiu, deși persoanele al căror drept la viață privată a fost încălcat din cauza activităților legate de supraveghere pot solicita distrugerea datelor, sub rezerva obținerii unui ordin judecătoresc[74].	Autoritatea responsabilă este Autoritatea de Supraveghere Tehnică.
Irlanda[75]	Legea de transpunere include obligația de a pune în aplicare cele patru principii.	Judecătorul desemnat are competența de a cerceta și a raporta dacă autoritățile naționale competente respectă dispozițiile legii de transpunere.
Grecia[76]	Legea de transpunere include obligația de a pune în aplicare cele patru principii, prevăzând în plus obligația operatorilor de a pregăti și a aplica un plan pentru asigurarea conformității sub controlul unui gestionar desemnat în materie de securitate a datelor.	Autoritatea pentru Protecția Datelor cu Caracter Personal și Autoritatea pentru Protecția Vieții Private în Domeniul Comunicațiilor.
Spania[77]	Dispozițiile privind securitatea datelor conțin trei din cele patru principii (calitatea și securitatea datelor păstrate, accesarea acestora de către persoanele autorizate și protecția împotriva prelucrării neautorizate).	Agenția pentru Protecția Datelor este autoritatea responsabilă.

71 Articolul 4 alineatul (1) din Legea comunicațiilor electronice (modificată), 2010.

72 Secțiunea 87 punctul 3 și secțiunea 88 din Legea 127/2005 modificată prin Legea 247/2008; secțiunea 2 din Legea 336/2005; secțiunea 3 punctul 4 din Legea 485/2005; secțiunea 28 punctul 1 din Legea 101/2000.

73 Legea privind prelucrarea datelor cu caracter personal; Ordinul executiv nr. 714 din 26 iunie 2008 privind furnizarea de rețele și servicii de comunicații electronice.

74 Subsecțiunea 111 punctul 9 din Legea comunicațiilor electronice; subsecțiunea 122 punctul (2) din Codul de procedură penală.

75 Secțiunile 4, 11 și 12 din Legea comunicațiilor (păstrarea datelor), 2009.

76 Articolul 6 din Legea 3917/2011.

77 Articolul 8 din Legea 25/2007, articolul 38 alineatul (3) din Legea generală privind telecomunicațiile. Legea (articolul 9) se referă la derogarea de la drepturile de acces și de anulare, prevăzute în Legea organică 15/1999 privind protecția datelor cu caracter personal (articolele 22 și 23).

Tabelul 4: protecția și securitatea datelor și autoritățile de supraveghere		
Stat membru	*Dispoziții privind protecția și securitatea datelor în legislația națională*	*Autoritatea de supraveghere*
Franța[78]	Legea de transpunere include obligația de a pune în aplicare cele patru principii.	Comisia națională pentru tehnologia informației și libertăți controlează respectarea acestor obligații.
Italia	Nu există dispoziții explicite privind securitatea datelor păstrate, deși există o cerință generală de distrugere sau de trecere în anonimat a datelor privind traficul și de prelucrare consensuală a datelor privind localizarea[79].	Autoritatea pentru Protecția Datelor monitorizează respectarea directivei de către operatori.
Cipru[80]	Legea de transpunere conține dispoziții privind fiecare dintre cele patru principii.	Comisarul pentru protecția datelor cu caracter personal monitorizează aplicarea legii de transpunere.
Letonia[81]	Legea de transpunere conține dispoziții cu privire la două principii: confidențialitatea datelor păstrate și accesul autorizat la datele păstrate, precum și distrugerea datelor la expirarea perioadei de păstrare.	Inspectoratul de Stat privind Datele supraveghează protecția datelor cu caracter personal în sectorul comunicațiilor electronice, dar nu și accesul la datele păstrate și prelucrarea acestora.
Lituania[82]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Inspectoratul de Stat privind Protecția Datelor supraveghează punerea în aplicare a legii de transpunere și răspunde de furnizarea de statistici pentru Comisia Europeană.
Luxemburg[83]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Autoritatea pentru Protecția Datelor
Ungaria[84]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Comisia parlamentară pentru protecția datelor și libertatea de informare
Malta[85]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Comisarul pentru protecția datelor
Țările de Jos[86]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Agenția privind Comunicațiile Radio supraveghează îndeplinirea obligațiilor furnizorilor de acces la internet și a furnizorilor de telecomunicații; Autoritatea pentru Protecția Datelor supraveghează procesul general de prelucrare a datelor cu caracter personal; detaliile cu privire la colaborarea între cele două autorități sunt incluse într-un protocol.
Austria	Directiva nu a fost transpusă.	
Polonia	Legea de transpunere cuprinde dispoziții privind cele patru principii[87].	Autoritatea pentru Protecția Datelor.

78 Articolul D.98-5 din CPCE; articolul L-34-1 (V) din CPCE; articolul 34 din Legea nr. 78-17; articolul 34-1 din CPCE; articolul 11 din Legea nr. 78-17, 6 ianuarie 1978.

79 Articolele 123 și 126 din Codul privind protecția datelor.

80 Articolele 14 și 15 din Legea 183 (I)/2007.

81 Articolul 4 alineatul (4) și articolul 71 alineatele (6)-(8) din Legea comunicațiilor electronice.

82 Articolul 12 alineatul (5), articolul 66 alineatele (8) și (9) din Legea comunicațiilor electronice, modificată la 14 noiembrie 2009.

83 Articolul 1 alineatul (5) din legea din 24 iulie 2010.

84 Articolul 157 din Legea C/2003, modificată prin Legea CLXXIV/2007; articolul 2 din Decretul 226/2003 și Legea LXIII/1992 privind protecția datelor.

85 Articolele 24 și 25 din Nota juridică nr. 198/2008; articolul 40 litera (b) din Legea privind protecția datelor (cap. 440).

86 Articolul 13 alineatul (5) din Legea telecomunicațiilor; titlul complet al protocolului de cooperare este următorul: „*Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens*".

87 Articolele 180a și 180e din Legea telecomunicațiilor.

Tabelul 4: protecția și securitatea datelor și autoritățile de supraveghere		
Stat membru	*Dispoziții privind protecția și securitatea datelor în legislația națională*	*Autoritatea de supraveghere*
Portugalia	Legea de transpunere cuprinde dispoziții privind cele patru principii[88].	Autoritatea pentru Protecția Datelor din Portugalia.
România	Directiva nu a fost transpusă.	
Slovenia[89]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Comisarul pe probleme de informare.
Slovacia[90]	Legea de transpunere cuprinde dispoziții privind cele patru principii.	Autoritatea națională de reglementare și de stabilire a prețurilor în domeniul comunicațiilor electronice supraveghează protecția datelor cu caracter personal.
Finlanda	Legea de transpunere cuprinde dispoziții explicite numai în legătură cu obligația de distrugere a datelor la expirarea perioadei de păstrare[91].	Autoritatea de Reglementare a Comunicațiilor din Finlanda supraveghează respectarea de către operatori a reglementărilor în materie de păstrare a datelor. Ombudsmanul pentru protecția datelor supraveghează legalitatea generală a prelucrării datelor cu caracter personal.
Suedia	Directiva nu a fost transpusă.	
Regatul Unit	Legea de transpunere cuprinde dispoziții privind cele patru principii[92].	Comisarul pe probleme de informare supraveghează păstrarea și/sau prelucrarea datelor privind comunicațiile (și orice alte date cu caracter personal) și efectuează controale corespunzătoare în materie de protecție a datelor. Comisarul pe probleme de interceptare (un înalt judecător în funcție sau la pensie) supraveghează modul în care autoritățile publice dobândesc datele privind comunicațiile în temeiul Legii privind reglementarea competențelor de cercetare. Tribunalul privind Competențele de Cercetare a fost creat pentru investigarea plângerilor în legătură cu utilizarea abuzivă a datelor care au fost dobândite în temeiul legislației de transpunere (Legea privind reglementarea competențelor de cercetare).

Transpunerea articolului 7 este inconsecventă. Deoarece datele păstrate pot avea un caracter extrem de personal și de sensibil, este necesar să se aplice, în mod consecvent și vizibil, standarde ridicate în materie de protecție și securitate a datelor de-a lungul întregului proces, în ceea ce privește stocarea, recuperarea și utilizarea, pentru a reduce la minimum riscul de încălcare a dreptului la viață privată și pentru a menține încrederea cetățenilor. Comisia va analiza opțiunile de consolidare a securității datelor și a standardelor în materie de protecție a datelor, inclusiv prin introducerea unor soluții care iau în considerare viața privată începând cu momentul conceperii, pentru a asigura respectarea acestor standarde atât în cadrul stocării, cât și al transmiterii. De asemenea, aceasta va ține seama de recomandările referitoare la garanțiile minime și măsurile de securitate tehnice și organizaționale formulate în raportul

88 Articolul 7 alineatele (1) și (5) și articolul 11 din Legea 32/2008; articolele 53 și 54 din Legea privind protecția datelor cu caracter personal.

89 Articolul 107a alineatul (6) și articolul 107c din Legea comunicațiilor electronice.

90 Articolul 59a din Legea comunicațiilor electronice; articolul S33 din Legea nr 428/2002 privind protecția datelor cu caracter personal.

91 Articolul 16 alineatul (3) din Legea comunicațiilor electronice.

92 Articolul 6 din Regulamentul privind păstrarea datelor.

Grupului de lucru „articolul 29” pentru protecția datelor privind a doua acțiune de asigurare a respectării obligațiilor[93].

4.7. Statistici (articolul 10)

Statele membre au obligația de a furniza Comisiei statistici anuale privind păstrarea datelor, inclusiv:

– cazurile în care informațiile au fost furnizate autorităților competente în conformitate cu legislația internă aplicabilă;

– timpul scurs între data la care au fost păstrate datele și data la care autoritatea competentă a solicitat transmiterea acestora (și anume vechimea datelor) și

– cazurile în care solicitările de date nu au putut fi îndeplinite.

În momentul solicitării de statistici în temeiul acestei dispoziții, Comisia a cerut statelor membre să furnizeze detalii cu privire la cazuri de „cereri” individuale de date. Cu toate acestea, în statisticile furnizate au existat diferențe în ceea ce privește domeniul de aplicare și gradul de detaliu: în răspunsurile lor, unele state membre au făcut distincție între diferitele tipuri de comunicații, unele au indicat vechimea datelor la momentul depunerii cererii, în timp ce alte state membre au prezentat numai statistici anuale, fără o defalcare detaliată. Nouăsprezece state membre[94] au furnizat statistici privind numărul de cereri de date pentru 2009 și/sau 2008; printre acestea s-au numărat Irlanda, Grecia și Austria, în care au fost formulate cereri de obținere de date, deși nu exista legislație de transpunere la momentul respectiv, precum și Republica Cehă și Germania, în care legislația în materie de păstrare a datelor a fost anulată. Șapte state membre care au transpus directiva nu au furnizat statistici, deși Belgia a comunicat o estimare a volumului de cereri anuale de date de telefonie (300 000).

Datele cantitative și calitative fiabile sunt esențiale pentru a demonstra necesitatea și importanța măsurilor de securitate, cum ar fi păstrarea datelor. Acest fapt a fost recunoscut în planul de acțiune din 2006 privind stabilirea statisticilor în materie de criminalitate și justiție penală[95], care a inclus obiectivul elaborării de metodologii pentru colectarea periodică a datelor, în conformitate cu directiva și introducerii statisticilor în baza de date Eurostat (cu condiția ca acestea să îndeplinească standardele de calitate). Acest obiectiv nu a putut fi atins din cauză că majoritatea statelor membre au transpus integral directiva numai în ultimii doi ani și din cauză că acestea au utilizat interpretări diferite pentru sursa statisticilor. În viitoarea sa propunere de revizuire a cadrului privind păstrarea datelor, precum și în planul revizuit de acțiune privind statisticile, Comisia va avea drept obiectiv elaborarea de indici de cuantificare fezabili și de proceduri de raportare care să permită monitorizarea transparentă și relevantă a păstrării datelor și care să nu genereze sarcini nejustificate pentru sistemele de justiție penală și autoritățile de aplicare a legii.

---

93 Avizul nr. 3/2006 al Grupul de lucru „articolul 29” pentru protecția datelor (WP119); raportul nr. 1/2010.

94 Republica Cehă, Danemarca, Germania, Estonia, Irlanda, Grecia, Spania, Franța, Cipru, Letonia, Litania, Malta, Țările de Jos, Austria, Polonia, Slovenia, Slovacia, Finlanda, Regatul Unit.

95 Comunicarea (2006) 437 a Comisiei, „Elaborarea unei strategii a UE globale și coerente în vederea stabilirii de statistici în materie de criminalitate și justiție penală: Plan de acțiune al UE 2006 – 2010”.

4.8. Transpunerea în țările SEE

Legislația în materie de păstrare a datelor a fost adoptată în Islanda, Liechtenstein și Norvegia[96].

4.9. Deciziile Curților Constituționale cu privire la legile de transpunere

Curtea Constituțională din România, Curtea Constituțională din Germania și Curtea Constituțională din Republica Cehă au anulat în octombrie 2009, martie 2010 și, respectiv, martie 2011, legile de transpunere a directivei în dreptul intern pe motiv că erau neconstituționale. Curtea Constituțională a României[97] a acceptat că se poate permite un amestec în exercitarea drepturilor fundamentale în condițiile în care se respectă anumite norme și se oferă garanții adecvate și suficiente de protejare împotriva unei eventuale acțiuni arbitrare a statului. Cu toate acestea, bazându-se pe jurisprudența Curții Europene a Drepturilor Omului[98], Curtea a constatat că domeniul de aplicare și scopul legii de transpunere erau ambigue și că garanțiile erau insuficiente și a hotărât că o „obligație legală care impune reținerea în mod continuu" a tuturor datelor privind traficul pe o perioadă de șase luni era incompatibilă cu dreptul la respectarea vieții private și libertatea de expresie, prevăzute la articolul 8 din Convenția europeană a drepturilor omului.

Curtea Constituțională germană[99] 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 condiții de securitate a datelor suficient de ridicate, nu ar încălca în mod necesar legea fundamentală a Germaniei. Cu toate acestea, Curtea a subliniat că păstrarea unor astfel de date constituie o restricționare gravă a dreptului la viață privată și, în consecință, aceasta ar trebui să fie permisă doar în anumite circumstanțe extrem de limitate și că o perioadă de păstrare de șase luni este limita maximă („*an der Obergrenze*") a ceea ce ar putea fi considerat drept proporțional (punctul 125). Datele ar trebui solicitate numai în cazul în care există deja o suspiciune privind săvârșirea unei infracțiuni grave sau dovada unui pericol la adresa securității publice, iar recuperarea datelor ar trebui să fie interzisă pentru anumite comunicații privilegiate (și anume, cele legate de o necesitate emoțională sau socială) care au la bază principiul confidențialității. De asemenea, datele ar trebui codate, cu o supraveghere transparentă a utilizării lor.

Curtea Constituțională cehă[100] a anulat legislația de transpunere pe motiv că, fiind o măsură care afecta exercitarea drepturilor fundamentale, aceasta nu era formulată suficient de precis și de clar. Curtea a criticat caracterul insuficient de restrictiv al limitării scopului, luând în considerare amploarea și domeniul de aplicare ale obligației de păstrare a datelor. Aceasta a apreciat că autoritățile cu competențe în materie de acces și utilizare a datelor păstrate, precum și procedurile aferente nu erau definite suficient de clar în legislația de transpunere

---

96 În Islanda, legea de transpunere este Legea 81/2003 privind telecomunicațiile (modificată în aprilie 2005); în Liechtenstein, aceasta este Legea privind telecomunicațiile din 2006. În Norvegia, legea de transpunere a fost aprobată la 5 aprilie 2011 și aceasta urmează să fie aprobată de rege.

97 Decizia nr. 1 258 din 8 octombrie 2009 a Curții Constituționale a României.

98 CEDO, Rotaru/România, 2000; Sunday Times/Regatul Unit, 1979 și Prințul Hans-Adam of Liechtenstein/România, 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, punctele 1 – 345.

100 Hotărârea Curții Constituționale cehe din 22 martie privind Legea nr. 127/2005 și Decretul nr. 485/2005; a se vedea, în special, punctele 45-48, 50-51 și 56.

pentru a asigura integritatea și confidențialitatea datelor. Prin urmare, cetățenii dispuneau de garanții insuficiente împotriva eventualelor abuzuri de putere ale autorităților publice. Curtea nu a criticat directiva în sine și a apreciat că Republica Cehă dispunea de o marjă suficientă pentru a o transpune conform Constituției sale. Cu toate acestea, printr-un *obiter dictum*, Curtea și-a exprimat îndoielile cu privire la necesitatea, eficacitatea și caracterul adecvat al păstrării datelor privind traficul, luând în considerare apariția noilor metode infracționale, cum ar fi utilizarea de cartele SIM anonime.

Aceste trei state membre analizează în prezent modalitățile de retranspunere a directivei. De asemenea, cauze referitoare la păstrarea datelor au fost înaintate Curții Constituționale din Bulgaria, care a hotărât revizuirea legii de transpunere, celei din Cipru, care a statuat că ordinele judecătorești pronunțate în temeiul legii de transpunere erau neconstituționale, și celei din Ungaria, în fața căreia este pendinte o cauză privind omiterea menționării în legea de transpunere a scopurilor legale de prelucrare a datelor[101].

În viitoarea sa propunere de revizuire a cadrului privind păstrarea datelor, Comisia va analiza aspectele evidențiate de jurisprudența națională.

4.10. Asigurarea aplicării directivei

Comisia se așteaptă ca statele membre care nu au transpus încă pe deplin directiva, sau care nu au adoptat încă legislația de înlocuire a actelor normative anulate de instanțele naționale, să facă acest lucru în cel mai scurt timp. În caz contrar, Comisia își rezervă dreptul de a-și exercita competențele de care dispune în temeiul tratatelor UE. În prezent, două state membre care nu au transpus directiva (Austria și Suedia) au fost declarate de Curtea de Justiție vinovate de încălcarea obligațiilor care le revin temeiul dreptului UE[102]. În aprilie 2011, Comisia a decis ca, pentru a doua oară, să trimită în judecată Suedia în fața Curții din cauza nerespectării hotărârii pronunțate în cauza C-185/09, care cerea impunerea de penalități financiare în temeiul articolului 260 din Tratatul privind funcționarea Uniunii Europene, în urma deciziei Parlamentului suedez de a amâna cu 12 luni adoptarea legislației de transpunere. Comisia continuă să monitorizeze îndeaproape situația din Austria, care a comunicat un calendar pentru adoptarea iminentă a legislației de transpunere.

5. ROLUL DATELOR PĂSTRATE ÎN JUSTIȚIA PENALĂ ȘI ÎN ASIGURAREA RESPECTĂRII LEGII

Prezenta secțiune rezumă funcțiile datelor păstrate, astfel cum au fost descrise de statele membre în contribuțiile lor la evaluare.

---

101 Curtea Administrativă Supremă bulgară, decizia nr. 13 627, 11 decembrie 2008; Curtea Supremă a Ciprului, cauzele de recurs nr. 65/2009, 78/2009, 82/2009 și 15/2010-22/2010, 1 februarie 2011; plângerea maghiară constituțională a fost înaintată de Uniunea maghiară pentru libertăți civile la 2 iunie 2008.

102 Cauza C-189/09 și, respectiv, cauza C-185/09.

5.1. Volumul datelor păstrate care au fost accesate de autoritățile naționale competente

Atât volumul traficului de telecomunicații, cât și volumul cererilor de acces la date privind traficul înregistrează o creștere. Statisticile furnizate de 19 state membre pentru 2008 și/sau 2009 evidențiază că, în ansamblu, în UE, în fiecare an au fost depuse peste 2 milioane de cereri de date, cu diferențe semnificative între statele membre, de la mai puțin de 100 pe an (Cipru), la peste 1 milion (Polonia). Conform informațiilor privind tipul de date solicitate care au fost furnizate de douăsprezece state membre pentru 2008 sau 2009, tipul de date solicitate cel mai frecvent avea legătură cu telefonia mobilă (a se vedea tabelele 5, 8 și 12). Statisticile nu indică scopul precis pentru care a fost depusă fiecare cerere. Republica Cehă, Letonia și Polonia au menționat că, în cazul datelor de telefonie mobilă, autoritățile competente au trebuit să depună aceeași cerere la fiecare dintre principalii operatori de telefonie mobilă și că, prin urmare, numărul efectiv al cererilor pe caz era considerabil mai mic decât sugerau statisticile.

Nu există nicio explicație evidentă pentru aceste diferențe, deși mărimea populației, tendințele infracționale dominante, limitările în materie de scop și condiții de acces, precum și costurile pentru dobândirea datelor constituie factori relevanți.

5.2. Vechimea datelor păstrate care au fost accesate

Pe baza defalcărilor statistice furnizate de nouă state membre[103] pentru 2008 (a se vedea rezumatul în tabelul 5 și detalii suplimentare în anexă), aproximativ 90 % din datele accesate de autoritățile competente în anul respectiv aveau o vechime de cel mult șase luni și aproximativ 70 % aveau o vechime de cel mult trei luni atunci când a fost depusă cererea (inițială) de acces.

Tabelul 5: prezentare generală a datelor păstrate care au fost accesate în nouă state membre care au furnizat defalcări pe tipuri de date în 2008

Vechime	*Telefonie fixă*	*Telefonie mobilă*	*Date referitoare la internet*	*Cumulat*
Sub șase luni	61 %	70 %	56 %	67 %
Între 3-6 luni	28 %	18 %	19 %	19 %
Între 6-12 luni	8 %	11 %	18 %	12 %
Peste un an	3 %	1 %	7 %	2 %

Majoritatea statelor membre consideră că utilizarea datelor păstrate, cu o vechime mai mare de trei sau chiar șase luni, este mai puțin frecventă, dar aceasta poate fi esențială; utilizarea acestor date tinde să se încadreze în trei categorii. 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 rețeaua de telefonie fixă și a datelor de telefonie mobilă duce, adesea, la potențiale piste, ceea ce generează cereri suplimentare de date mai vechi. De exemplu, dacă în timpul unei anchete s-a identificat un nume pe baza datelor privind rețeaua de telefonie fixă sau a datelor de telefonie mobilă, anchetatorii ar putea dori să identifice adresa Internet Protocol (IP) pe care a folosit-o această persoană și ar putea dori să identifice persoanele

[103] Republica Cehă, Danemarca, Estonia, Irlanda, Spania, Cipru, Letonia, Malta, Regatul Unit.

contactate într-o anumită perioadă de la această adresă IP. Într-o situație de acest tip, anchetatorii vor solicita probabil date care să permită, de asemenea, urmărirea comunicațiilor cu alte adrese IP și identificarea persoanelor care au utilizat acele adrese IP.

În al doilea rând, investigarea infracțiunilor deosebit de grave, a unei serii de infracțiuni, a criminalității organizate și a incidentelor teroriste tinde să se bazeze pe date păstrate mai vechi, care reflectă timpul necesar pentru a planifica aceste infracțiuni, pentru a identifica modelele de comportament infracțional și relațiile dintre complicii la o infracțiune și pentru a stabili intenția de a săvârși o infracțiune. Adesea, activitățile care au legătură cu infracțiuni financiare complexe sunt detectate doar după câteva luni. În al treilea rând, și în mod excepțional, statele membre au solicitat date privind traficul deținute 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. Acest tip de asistență judiciară reciprocă poate fi un proces îndelungat, ceea ce explică motivele pentru care, în aceste cazuri, unele datele solicitate aveau o vechime de peste șase luni.

5.3. Cereri transfrontaliere de date păstrate

Cercetările și urmăririle penale pot implica probe sau martori din mai multe state membre ori evenimente care s-au desfășurat în mai multe state membre. Conform statisticilor furnizate de statele membre, mai puțin de 1 % din totalul cererilor de date păstrate au avut ca obiect datele deținute în alt stat membru. Autoritățile de aplicare a legii au indicat că preferă să solicite date de la operatorii de pe piața internă, care ar fi putut stoca datele relevante, mai degrabă decât să lanseze procedura de asistență judiciară reciprocă, care poate necesita timp, fără a avea garanția acordării accesului la date. Decizia-cadru 2006/960/JAI privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre[104], care stabilește termene pentru furnizarea de informații în baza cererii formulate de un alt stat membru, nu este aplicabilă, deoarece datele păstrate sunt considerate a fi informații obținute prin mijloace coercitive, care nu intră în sfera de aplicare a instrumentului. Cu toate acestea, niciun stat membru și nicio autoritate de aplicare a legii nu a solicitat facilitarea în continuare a schimbului transfrontalier.

5.4. Importanța datelor păstrate în cadrul cercetărilor și urmăririlor penale

Deși numărul absolut al cerilor de date comunicate nu reflectă în mod necesar importanța datelor în cadrul cercetărilor penale individuale, statele membre au menționat, în general, că păstrarea datelor a avut cel puțin un rol important și, în unele cazuri, indispensabil[105] în prevenirea și combaterea infracțiunilor, inclusiv în protecția victimelor și achitarea unor persoane nevinovate implicate în proceduri penale. Recunoașterea vinovăției, declarațiile martorilor sau probele medicolegale stau la baza pronunțării unei condamnări. Conform celor semnalate, datele păstrate privind traficul s-au dovedit necesare în contactarea martorilor la

---

104 Decizia-cadru 2006/960/JAI a Consiliului din 18 decembrie 2006 privind simplificarea schimbului de informații și date operative între autoritățile de aplicare a legii ale statelor membre ale Uniunii Europene, JO L 386, 29.12.2006, p. 89-100 și JO L 200 din 1.8.2007, p. 637-648.

105 Republica Cehă a apreciat păstrarea datelor „absolut indispensabilă într-un mare număr de cazuri”; Ungaria a declarat că aceasta a fost „indispensabilă în activitățile obișnuite ale [agențiilor de aplicare a legii]”; Slovenia a afirmat că lipsa datelor păstrate ar „paraliza funcționarea agențiilor de aplicare a legii”; o agenție de poliție din Regatul Unit descria disponibilitatea datelor privind traficul ca fiind „absolut esențială … pentru cercetarea amenințărilor teroriste și a infracțiunilor grave.”

incidente, care altfel nu ar fi putut fi identificați, precum și în furnizarea de probe sau indicii pentru a stabili complicitatea în săvârșirea unei infracțiuni. Unele state membre[106] au susținut, de asemenea, că utilizarea datelor păstrate a contribuit la stabilirea nevinovăției persoanelor suspectate de săvârșirea unor infracțiuni, fără a fi nevoie să se recurgă la alte metode de supraveghere, cum ar fi interceptările și perchezițiile la domiciliu, care ar putea fi considerate mai invazive.

Nu există o definiție generală a „infracțiunii grave" în UE, și, în consecință, nu există statistici la nivelul UE privind incidența infracțiunilor grave sau privind cercetarea și urmărirea penală a infracțiunilor grave, deși se publică periodic date privind criminalitatea și justiția. Volumul cumulat de cereri de date păstrate, conform rapoartelor a 19 state membre care au furnizat unele date pentru 2009 și/sau 2008, a fost de aproximativ 2,6 milioane. Comparativ cu ultimele statistici disponibile privind criminalitatea și justiția penală pentru aceste 19 state membre - care se referă la toate infracțiunile raportate, nu numai la infracțiunile grave - se poate spune că, anual, au existat puțin peste două cereri pe ofițer de poliție pe an sau aproximativ 11 cereri pentru fiecare 100 de infracțiuni înregistrate[107].

Pe baza statisticilor și a exemplelor furnizate, care corelează utilizarea datelor istorice de comunicații păstrate cu numărul de condamnări, achitări, cauze suspendate și infracțiuni prevenite, se pot desprinde o serie de concluzii în ceea ce privește rolul și importanța datelor păstrate pentru cercetările penale.

Stabilirea urmelor probelor

În primul rând, datele păstrate permit stabilirea de urme ale probelor care conduc la o infracțiune. Datele sunt utilizate pentru a distinge sau pentru a corobora alte mijloace de probă privind activitățile și legăturile dintre suspecți. În special, datele privind localizarea au fost folosite atât de autoritățile de aplicare a legii, cât și de învinuiți, pentru a exclude suspecții de la locul crimei și pentru a verifica alibiurile. Prin urmare, prin acest tip de probe persoanele pot fi excluse din cadrul anchetelor penale, eliminând astfel necesitatea efectuării unor cercetări mai invazive, sau se pot obține achitări în procese. Belgia a citat condamnarea, în 2008, a autorilor răpirii și sechestrării unui angajat al tribunalului din Anvers, când datele privind localizarea care stabileau legătura între activitățile acestora în trei orașe diferite au avut un rol decisiv în convingerea completului de judecată cu privire la complicitatea lor. În alt caz, cel al crimei comise în 2007, în care a fost implicată o bandă de motocicliști, datele privind localizarea stocate pe telefoanele mobile ale infractorilor au dovedit că aceștia se aflau în zonă la ora comiterii crimei și au dus la o mărturisire parțială[108]. Belgia, Irlanda și Regatul Unit au declarat că anumite infracțiuni care implică o comunicație prin internet pot fi cercetate *numai* prin intermediul datelor păstrate: de exemplu, amenințările cu violența formulate în camere de chat nu lăsa, de multe ori, nicio urmă, cu excepția datelor privind traficul în spațiul informatic. O situație similară este valabilă în cazul infracțiunilor comise pe

---

106 Germania, Polonia, Slovenia și Regatul Unit.

107 În 2007 în UE-27 erau 1,7 milioane de ofițeri de poliție, din care 1,2 milioane în cele 19 state membre care au furnizat statistici privind cererile de date păstrate; în 2007, poliția a consemnat 29,2 milioane de infracțiuni în UE, din care 24 de milioane au fost înregistrate în cele 19 state membre care au furnizat statistici. (Sursa: Eurostat 2009).

108 National Policing Improvement Agency (Regatul Unit), *The Journal of Homicide and Major Incident Investigation*, volumul 5, numărul 1, primăvara 2009, p. 39-51.

cale telefonică. Ungaria și Polonia au citat un caz de fraudă împotriva persoanelor în vârstă de la sfârșitul anului 2009/începutul anului 2010, comis prin intermediul unor apeluri telefonice prin care autorii pretindeau a fi membri de familie care aveau nevoie de un împrumut; persoanele vinovate au putut fi identificate doar datorită datelor de telefonie păstrate.

Începerea cercetărilor penale

În al doilea rând, au existat cazuri în care, în lipsa unor probe medicolegale sau a martorilor oculari, singura modalitate de începere a unei cercetări penale a fost consultarea datelor păstrate. Germania a dat ca exemplu cazul uciderii unui ofițer de poliție, când agresorul a fugit cu autovehiculul victimei, pe care ulterior l-a abandonat. A fost posibil să se stabilească că făptuitorul a telefonat pentru a procura un alt mijloc de transport. Nu existau probe medicolegale sau martori oculari pentru stabilirea identității asasinului, iar autoritățile s-au bazat pe disponibilitatea acestor date privind traficul pentru a-și putea continua cercetările. În cazurile de abuz sexual asupra copiilor săvârșite prin intermediul internetului, păstrarea datelor a fost indispensabilă pentru reușita cercetărilor. În paralel cu alte tehnici de cercetare, datele păstrate permit identificarea consumatorilor de conținut cu abuzuri asupra copiilor[109] și contribuie la identificarea și salvarea copiilor-victimă. Republica Cehă a comunicat că, fără acces la datele referitoare la internet care au fost păstrate, ar fi fost imposibil să înceapă cercetările în cadrul „Operațiunii Vilma” care viza o rețea de persoane care utilizau și transmiteau pornografie infantilă. La nivelul UE, eficacitatea operațiunii „Rescue” (care este facilitată de Europol) în ceea ce privește protejarea copiilor împotriva abuzurilor a fost diminuată din cauza că netranspunerea legislației în materie de păstrare a datelor a împiedicat anumite state membre să efectueze cercetări cu privire la membrii unei extinse rețele pedofile internaționale care utilizau adrese IP cu o vechime de până la un an.

În cercetările privind infracțiuni informatice, adresa IP este, adesea, primul indiciu. Autoritățile de aplicare a legii, prin recuperarea datelor privind traficul, pot identifica abonatul din spatele adresei IP, înainte de a stabili dacă pot fi începute cercetări penale. De asemenea, poate permite poliției să avertizeze potențialele victime ale atacurilor informatice: în cazul în care poliția reușește să confiște un server de comandă și control utilizat de către operatorii de botnet, ei pot vedea numai adresele IP legate de acest server; dar, prin accesarea datelor păstrate, poliția poate identifica și preveni potențialele victime care dețin aceste adrese IP.

Datele păstrate fac parte integrantă din cercetarea penală

În al treilea rând, deși autoritățile de aplicare a legii și instanțele din majoritatea statelor membre nu păstrează statistici privind tipul de probe care s-au dovedit cruciale în pronunțarea de condamnări sau de achitări, datele păstrate fac parte integrantă din cercetarea și urmărirea penală în UE. Unele state membre au declarat că nu au putut să izoleze întotdeauna impactul datelor păstrate asupra încheierii cu succes a cercetărilor și urmăririlor penale, din cauză că instanțele iau în considerare toate probele care le sunt prezentate și apreciază foarte rar că un anumit element de probă a fost concludent[110]. Țările de Jos au comunicat că, în perioada

---

109 Proiectul intitulat „*Measurement and analysis of p2p activity against paedophile content*”, finanțat de Programul pentru un internet mai sigur, a furnizat informații precise privind activitatea pedofilă în sistemul *eDonkey peer-to-peer*, care au permis identificarea a 178 000 de utilizatori (din 89 de milioane de utilizatori verificați) care au solicitat conținut cu caracter pedofil.

110 Belgia, Republica Cehă, Lituania.

ianuarie-iulie 2010, datele istorice privind traficul au fost un factor decisiv în 24 de hotărâri judecătorești. Finlanda a raportat că în 56 % din cele 3 405 de cereri, datele păstrate s-au dovedit a fi „importante” sau „esențiale” pentru detectarea și/sau instrumentarea cazurilor penale. Regatul Unit a furnizat date prin care se urmărea cuantificarea impactului păstrării datelor asupra urmăririi penale; acesta a comunicat că, pentru trei dintre agențiile sale de aplicare a legii, datele păstrate au fost necesare în majoritatea, dacă nu în toate cercetările care au avut ca rezultat începerea urmăririi penale sau pronunțarea unei hotărâri de condamnare.

5.5. Evoluțiile tehnologice și utilizarea cartelelor SIM preplătite

Autoritățile de aplicare a legii trebuie să țină pasul cu evoluțiile tehnologice care sunt utilizate pentru săvârșirea sau încurajarea infracțiunilor. Păstrarea datelor este unul dintre instrumentele de cercetare penală care trebuie puse la dispoziția autorităților de aplicare a legii pentru a aborda, în mod flexibil și eficient, provocările criminalității contemporane sub aspectul diversității, volumului și vitezei. O serie de forme de comunicații din ce în ce mai comune nu intră sub incidența directivei. Rețelele private virtuale (VPN), de exemplu, din cadrul universităților sau marilor corporații, permit mai multor utilizatori să acceseze internetul prin intermediul unui singur portal utilizând aceeași adresă IP. Cu toate acestea, în prezent este în curs de elaborare o nouă tehnologie care să permită atribuirea de adrese utilizatorilor individuali de VPN.

Ponderea utilizatorilor de telefonie mobilă care folosesc servicii preplătite variază în UE. Unele state membre au susținut că, în special atunci când sunt achiziționate într-un alt stat membru, cartelele SIM preplătite, ai căror posesori nu sunt identificați, ar putea fi, de asemenea, utilizate de persoane implicate în activități infracționale ca mijloc de evitare a identificării în cursul cercetării penale[111]. Șase state membre (Danemarca, Spania, Italia, Grecia, Slovacia și Bulgaria) au adoptat măsuri care necesită înregistrarea cartelor SIM preplătite. Acestea și alte state membre (Polonia, Cipru, Lituania) au susținut opțiunea adoptării de măsuri la nivelul UE pentru înregistrarea obligatorie a identității utilizatorilor de servicii preplătite. Eficacitatea acestor măsuri naționale nu a fost dovedită. Au fost evidențiate limitări potențiale, de exemplu, în cazurile de furt de identitate sau atunci când cartela SIM este achiziționată de un terț ori atunci când un utilizator activează serviciul de roaming prin conectarea cu o cartelă cumpărată într-o țară terță. În general, Comisia nu este convinsă de necesitatea de a acționa în acest domeniu la nivelul UE în acest stadiu.

6. IMPACTUL PĂSTRĂRII DATELOR ASUPRA OPERATORILOR ȘI CONSUMATORILOR

6.1. Operatori și consumatori

Într-o declarație comună adresată Comisiei, cinci mari asociații din sectorul industrial au afirmat că impactul economic al directivei a fost „substanțial” sau „enorm” pentru „furnizorii de servicii mai mici”, deoarece directiva lasă „o marjă largă de manevră”[112]. Opt operatori au prezentat estimări foarte divergente ale costului, în ceea ce privește cheltuielile de capital și cheltuielile operaționale pe care le implică respectarea directivei. Aceste afirmații pot fi

---

111 Concluziile Consiliului privind combaterea folosirii abuzive, în scopuri infracționale, a comunicațiilor electronice și a anonimatului acestora.

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

susținute prin indicarea nivelurilor de rambursare a costurilor operatorilor, astfel cum au fost raportate de patru state membre (a se vedea tabelul 6).

Un studiu efectuat anterior transpunerii directivei în majoritatea statelor membre a estimat costul de instituire a unui sistem de păstrare a datelor pentru un furnizor de servicii de internet care deservește o jumătate de milion de clienți la aproximativ 375 240 EUR în primul an și, ulterior, costurile operaționale lunare la 9 870 EUR[113], costurile de instituire a unui sistem de recuperare a datelor au fost estimate la 131 190 EUR, iar costurile operaționale la 28 960 EUR pe lună. Cu toate acestea, Curtea Constituțională germană, în hotărârea sa din 2 martie 2010, a apreciat că impunerea unei obligații de stocare „nu este excesiv de împovărătoare pentru furnizorii de servicii afectați [sau] disproporționată în raport cu sarcina financiară suportată de întreprinderi ca urmare a obligației de stocare”[114]. Costurile unitare de păstrare a datelor sunt invers proporționale cu dimensiunea operatorului și cu nivelul de standardizare adoptat de un stat membru în raporturile cu operatorii[115].

În răspunsurile lor la chestionarul Comisiei, majoritatea operatorilor nu au putut să cuantifice impactul directivei asupra concurenței, a prețurilor cu amănuntul pentru consumatori sau a investițiilor în infrastructuri și servicii noi.

Nu există nicio dovadă cu privire la vreun efect cuantificabil sau considerabil al directivei asupra prețurilor de consum pentru serviciile de comunicații electronice; în cadrul consultării publice din 2009 nu s-au primit contribuții din partea reprezentanților consumatorilor. Un sondaj efectuat în Germania în numele unei organizații a societății civile a arătat că, în anumite circumstanțe, consumatorii intenționau să își modifice comportamentul în materie de comunicații și să evite să utilizeze serviciile de comunicații electronice, cu toate că nu există nicio dovadă care să indice că a avut loc o modificare de comportament într-unul din statele membre vizate sau în UE, în general[116].

Comisia intenționează să evalueze impactul viitoarelor modificări aduse directivei asupra industriei și a consumatorilor, inclusiv, eventual, prin intermediul unui sondaj Eurobarometru specific pentru măsurarea percepției publice.

6.2. Rambursarea costurilor

Directiva nu reglementează rambursarea costurilor suportate de operatori, ca urmare a obligației de păstrare a datelor. Aceste costuri pot fi considerate drept:

(a) *cheltuieli operaționale*, respectiv costuri de operare sau cheltuieli recurente, care sunt legate de desfășurarea activității, de un dispozitiv, de o componentă, de un echipament sau de o instalație; și

---

113 Wilfried Gansterer & Michael Ilger, Păstrarea datelor – Directiva UE 2006/24/CE dintr-o perspectivă tehnologică *(Data retention – The EU Directive 2006/24/EC from a Technological Perspective)*, Viena: *Verlag Recht und Medien*, 2008.

114 Bundesverfassungsgericht, 1 BvR 256/08, 2 martie 2010, punctul 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

116 Sondajul a fost efectuat de Forsa și comandat de AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

(b) *cheltuieli de capital*, respectiv, cheltuieli care generează beneficii viitoare sau costul dezvoltării ori furnizării componentelor neconsumabile necesare pentru produs sau sistem, care pot include costul cu forța de muncă și cheltuielile aferente instalației, cum ar fi chiria și utilitățile.

Toate statele membre asigură o formă de rambursare în cazul în care datele sunt solicitate în contextul unei proceduri penale în instanță. Două state membre au menționat că rambursează atât cheltuieli operaționale, cât și de capital. Șase state rambursează numai cheltuieli operaționale. Nicio altă schemă de rambursare nu a fost notificată Comisiei. În tabelul 6 sunt prezentate detalii.

Tabelul 6: state membre care rambursează costurile

Stat membru	**Cheltuieli operaționale**	**Cheltuieli de capital**	**Costurile anuale cu rambursarea (milioane EUR)**
Belgia	Da	Nu	22 (2008)
Bulgaria	Nu	Nu	-
Republica Cehă	Directiva nu a fost transpusă[117].		
Danemarca	Da	Nu	-
Germania	Directiva nu a fost transpusă.		
Estonia	Da	Nu	-
Irlanda	Nu	Nu	-
Grecia	Nu	Nu	-
Spania	Nu	Nu	-
Franța	Da	Nu	-
Italia	-	-	-
Cipru	Nu	Nu	-
Letonia	Nu	Nu	-
Lituania	Da, dacă se solicită și se justifică rambursarea.	Nu	-
Luxemburg	Nu	Nu	-
Ungaria	Nu	Nu	-
Malta	Nu	Nu	-
Țările de Jos	Da	Nu	-
Austria	Directiva nu a fost transpusă.		
Polonia	Nu	Nu	-
Portugalia	Nu	Nu	-
România	Directiva nu a fost transpusă.		
Slovenia	Nu	Nu	-
Slovacia	Nu	Nu	-
Finlanda	Da	Da	1
Suedia	Directiva nu a fost transpusă.		
Regatul Unit	Da	Da	55 (rambursate în total pentru costurile suportate în trei ani)

[117] Înainte de anularea legii de transpunere din Republica Cehă, aceasta a rambursat atât cheltuieli operaționale, cât și cheltuieli de capital și a raportat costuri de rambursare în valoare de 6, 8 milioane EUR pentru 2009.

Pe baza celor de mai sus, se poate concluziona că directiva nu și-a atins pe deplin obiectivul de a crea condiții de concurență echitabile pentru operatorii din UE. Comisia va analiza opțiunile de reducere la minimum a obstacolelor din calea funcționării pieței interne prin asigurarea faptului că operatorii beneficiază, în mod mai consecvent, de rambursarea costurilor pe care le suportă pentru a se conforma cerințelor în materie de păstrare a datelor, acordând o atenție deosebită operatorilor mici și mijlocii.

7. IMPLICAȚIILE PĂSTRĂRII DATELOR DIN PERSPECTIVA DREPTURILOR FUNDAMENTALE

7.1. Drepturile fundamentale la viață privată și la protecția datelor cu caracter personal

Păstrarea datelor constituie o limitare a dreptului la viață privată și a dreptului la protecția datelor cu caracter personal, care sunt drepturi fundamentale în UE[118]. O astfel de limitare trebuie să fie, în conformitate cu articolul 52 alineatul (1) din Carta drepturilor fundamentale, „prevăzută de lege și să respecte substanța acestor drepturi, sub rezerva principiului proporționalității", trebuie să fie justificată ca necesară și să răspundă obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți. În practică, aceasta înseamnă că orice limitare trebuie[119]:

(a) să fie formulată în mod precis și previzibil;

(b) să fi necesară pentru realizarea unui obiectiv de interes general sau pentru protejarea drepturilor și libertăților celorlalți;

(c) să fie proporțională cu obiectivul urmărit și

(d) să respecte conținutul esențial al drepturilor fundamentale vizate.

Articolul 8 alineatul (2) din Convenția europeană pentru apărarea drepturilor omului recunoaște, de asemenea, că amestecul unei autorități publice în exercitarea dreptului unei persoane la viață privată poate fi justificat ca fiind necesar în interesul securității naționale, siguranței publice sau al prevenirii criminalității[120]. Articolul 15 alineatul (1) din Directiva privind confidențialitatea în mediul electronic și considerentele directivei privind păstrarea datelor reiterează aceste principii care stau la baza abordării UE în materie de păstrare a datelor.

Ulterior, jurisprudența Curții de Justiție a Uniunii Europene și a Curții Europene a Drepturilor Omului a dezvoltat condițiile pe care trebuie să le îndeplinească orice limitare a dreptului la

---

118 Articolul 7 și articolul 8 din Carta drepturilor fundamentale a Uniunii Europene (JO C 83, 30.3.2010, p. 389) garantează dreptul oricărei persoane la „protecția datelor cu caracter personal care o privesc." Articolul 16 din Tratatul privind funcționarea Uniunii Europene (JO C 83, 30.3.2010, p. 1) consacră, de asemenea, dreptul oricărei persoane la „protecția datelor cu caracter personal care o privesc."

119 A se vedea lista de verificare a Comisiei privind drepturile fundamentale pentru toate propunerile legislative în Comunicarea COM(2010) 573/4 a Comisiei, „Strategie pentru punerea în aplicare efectivă a Cartei drepturilor fundamentale de către Uniunea Europeană".

120 Articolul 8 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (ETS nr. 5), Consiliul Europei, 4.11.1950.

viață privată. Aceste hotărâri sunt relevante din perspectiva eventualei modificări a directivei, în special în ceea ce privește condițiile de acces și utilizare a datelor păstrate.

Orice limitare a dreptului la viață privată trebuie să fie precisă și să aibă un caracter previzibil

În cauza Österreichischer Rundfunk, Curtea Europeană de Justiție a hotărât că orice amestec în exercitarea dreptului la viață privată prevăzut de lege trebuie să fie „formulat suficient de precis pentru a permite cetățenilor să își modifice comportamentul în consecință ….[astfel încât] să se conformeze cerinței privind caracterul previzibil".

Orice limitare a dreptului la viață privată trebuie să fie strict necesară și să asigure un minimum de garanții

În cauza Copland/Regatul Unit, referitoare la monitorizarea de către stat a apelurilor telefonice, a corespondenței electronice și a utilizării internetului de către o persoană, Curtea Europeană a Drepturilor Omului a hotărât că o astfel de restricționare a dreptului la viață privată ar putea fi considerată necesară numai în cazul în care se bazează pe legislația internă relevantă[121]. În cauza S. și Marper/Regatul Unit, referitoare la păstrarea profilurilor ADN sau a amprentelor digitale ale oricărei persoane achitate de săvârșirea unei infracțiuni sau în cazul căreia procedurile sunt retrase înainte de pronunțarea unei hotărâri de condamnare, Curtea a hotărât că o astfel de limitare a dreptului la viață privată ar putea fi justificată numai dacă răspunde unei nevoi sociale urgente, dacă este proporțională cu obiectivul urmărit și dacă motivele invocate de autoritatea publică pentru a justifica această limitare au fost relevante și suficiente[122]. Principiile de bază ale protecției datelor prevedeau ca păstrarea datelor să fie proporțională în raport cu scopul colectării și ca perioada de stocare să fie limitată[123]. Pentru interceptarea convorbirilor telefonice, supravegherea secretă și culegerea de informații sub acoperire „[era] esențial ... să existe norme clare, detaliate care să reglementeze incidența și aplicarea măsurilor, precum și garanții minime privind, *inter alia*, durata, stocarea, utilizarea, accesul terților, procedurile pentru conservarea integrității și confidențialității datelor și procedurile pentru distrugerea acestora, oferind astfel garanții suficiente împotriva riscului de abuz și arbitrarietate."

Orice limitare a dreptului la viață privată trebuie să fie proporțională cu interesul general

În mod similar, Curtea Europeană de Justiție, în hotărârea pronunțată în cauza Schecke & Eifert privind publicarea numelui tuturor beneficiarilor de subvenții agricole pe internet[124], a apreciat că legislatorul UE pare a nu fi luat măsurile corespunzătoare pentru a găsi un echilibru între respectarea substanței dreptului la viață privată și interesul general (transparența), astfel cum este recunoscut de UE. În special, Curtea a constatat că legislatorii nu au luat în considerare alte metode care ar fi fost consecvente cu obiectivul și care ar fi avut ca rezultat o interferență mai redusă cu dreptul beneficiarilor subvențiilor la respectarea vieții lor private și la protecția datelor lor cu caracter personal. În consecință, Curtea a hotărât că

---

121 Copland/Regatul Unit, hotărârea Curții Europene a Drepturilor Omului, Strasbourg, 3.4.2007, p. 9.

122 Marper/Regatul Unit, hotărârea Curții Europene a Drepturilor Omului, Strasbourg, 4.12.2008, p. 31.

123 Marper, p. 30.

124 Cauza C-92/09 Volker și Markus Schecke GbR/Land Hessen și cauza C-93/09 Eifert/Land Hessen și Bundesanstalt für Landwirtschaft und Ernahrung, 9.11.2010.

legislatorii au depăşit limitele proporţionalităţii, întrucât „limitările în legătură cu protecţia datelor cu caracter personal trebuie să se aplice numai în măsura în care este strict necesar”.

7.2. Critici aduse principiului păstrării datelor

Mai multe organizaţii ale societăţii civile s-au adresat Comisiei susţinând că păstrarea datelor este, în principiu, o restrângere nejustificată şi inutilă a dreptului persoanelor la viaţă privată. Acestea consideră că păstrarea „generală şi nediferenţiată”, în lipsa consimţământului persoanei, a datelor privind traficul de telecomunicaţii, localizarea şi abonatul constituie o restricţionare ilegală a drepturilor fundamentale. Ca urmare a introducerii unei cauze în faţa instanţelor dintr-un stat membru (Irlanda), de către un grup pentru apărarea drepturilor civile, se preconizează că problema legalităţii directivei va fi înaintată Curţii Europene de Justiţie[125]. De asemenea, Autoritatea Europeană pentru Protecţia Datelor şi-a exprimat îndoiala cu privire la necesitatea măsurii.

7.3. Apeluri în favoarea unor norme mai stricte în materie de securitate şi protecţie a datelor

Raportul Grupului de lucru „articolul 29” privind a doua acţiune de asigurare a respectării obligaţiilor a susţinut că riscurile de încălcare a confidenţialităţii comunicaţiilor şi a libertăţii de exprimare erau inerente stocării datelor privind traficul. Raportul a criticat anumite aspecte ale punerii în aplicare la nivel naţional, în special înregistrarea datelor în jurnalul electronic, perioadele de păstrare, tipul de date păstrate şi măsurile în materie de securitate a datelor. Grupul de lucru a menţionat cazuri în care detalii ale *conţinutului* comunicaţiilor legate de internet, care nu se încadrează în domeniul de aplicare al directivei, au fost reţinute, inclusiv adrese IP de destinaţie şi URL-uri ale site-urilor internet, obiectul emailurilor şi lista destinatarilor menţionaţi în copia mesajului. Prin urmare, acesta a solicitat clarificarea caracterului exhaustiv al categoriilor şi a faptului că nu trebuie să se impună operatorilor nicio obligaţie suplimentară în materie de păstrare a datelor.

Autoritatea Europeană pentru Protecţia Datelor a afirmat că directiva „nu a reuşit să armonizeze legislaţia naţională” şi că utilizarea datelor păstrate nu este strict limitată la combaterea infracţiunilor grave[126]. Autoritatea a declarat că un instrument al UE care conţine norme privind obligaţia de păstrare a datelor ar trebui, în cazul în care se demonstrează necesitatea, să conţină şi norme privind accesul autorităţilor de aplicare a legii la aceste date şi utilizarea ulterioară a acestora. Autoritatea a invitat UE să adopte un cadru legislativ cuprinzător, care nu numai să impună obligaţii de păstrare a datelor pentru operatori, ci şi să reglementeze modul în care statele membre utilizează datele în scopul aplicării legii, astfel încât să se obţină „securitate juridică pentru cetăţeni”.

În general, autorităţile pentru protecţia datelor au susţinut că păstrarea datelor în sine implică un risc de încălcare eventuală a vieţii private, aspect neabordat de directivă la nivelul UE, în schimb fiind prevăzută cerinţa ca statele membre să garanteze respectarea normelor naţionale în materie de protecţie a datelor. Deşi nu există exemple concrete de încălcări grave ale vieţii private, riscul de încălcare a securităţii datelor se va menţine şi acesta ar putea creşte odată cu

---

125 La 5 mai 2010, Înalta Curte din Irlanda a autorizat Digital Rights Ireland Limited să se adreseze Curţii Europene de Justiţie în temeiul articolului 267 din Tratatul privind funcţionarea Uniunii Europene.

126 Discursul lui Peter Hustinx la conferinţa „Asumarea directivei privind păstrarea datelor”, 3 decembrie 2010.

evoluțiile tehnologice și cu tendințele înregistrate la nivelul formelor de comunicații, indiferent dacă datele sunt stocate în scop comercial sau de securitate, în interiorul sau în afara UE, cu excepția cazului în care se instituie garanții suplimentare.

8. CONCLUZII ȘI RECOMANDĂRI

Prezentul raport a evidențiat o serie de beneficii și de domenii care trebuie îmbunătățite în contextul regimului actual de păstrare a datelor în UE. Uniunea Europeană a adoptat directiva într-un moment în care gradul de alertă în ceea ce privește atacurile teroriste iminente era ridicat. Evaluarea impactului, pe care Comisia intenționează să o efectueze, oferă o oportunitate pentru analizarea păstrării datelor în UE în raport cu criteriile de necesitate și proporționalitate, luând în considerare securitatea internă, buna funcționare a pieței interne și consolidarea respectării dreptului la viață privată și al dreptului la protecția datelor cu caracter personal, precum și în interesul acestora. Propunerea Comisiei de revizuire a cadrului privind păstrarea datelor ar trebui să se bazeze pe următoarele concluzii și recomandări.

8.1. UE ar trebui să sprijine și să reglementeze păstrarea datelor ca o măsură de securitate

Majoritatea statelor membre sunt de părere că normele UE privind păstrarea datelor rămân necesare în calitate de instrument utilizat în aplicarea legii, protecția victimelor și sistemele de justiție penală. Probele furnizate de statele membre, sub formă de statistici și exemple, au un caracter limitat în anumite privințe, dar, cu toate acestea, atestă rolul foarte important pe care îl au datele păstrate în cadrul cercetării penale. Aceste date oferă indicii și probe importante în prevenirea și urmărirea penală a infracțiunilor și în asigurarea justiției penale. Utilizarea acestora a dus la pronunțarea de condamnări pentru infracțiuni care, dacă datele nu ar fi fost păstrate, nu ar fi fost niciodată soluționate. De asemenea, utilizarea acestora a dus la achitarea unor persoane nevinovate. Armonizarea normelor în acest domeniu ar trebui să garanteze că păstrarea datelor este un instrument eficient în combaterea criminalității, că industria beneficiază de securitate juridică într-o piață internă care funcționează bine și că în întreaga Uniune Europeană este asigurat în mod consecvent un nivel ridicat de respectare a dreptului la viață privată și de protecție a datelor cu caracter personal.

8.2. Transpunerea a fost inegală

Legislația de transpunere este în vigoare în 22 de state membre. Evaluarea Directivei privind păstrarea datelor este foarte problematică din cauza marjei considerabile de care dispun statele membre pentru a adopta măsuri privind păstrarea datelor în temeiul articolului 15 alineatul (1) din Directiva privind confidențialitatea în mediul electronic. Există diferențe considerabile între legislațiile de transpunere în domeniile care reglementează limitarea scopului, accesul la date, perioadele de păstrare, protecția și securitatea datelor, precum și statisticile. Trei state membre au încălcat directiva, întrucât legislația națională de transpunere a fost anulată de Curtea Constituțională. Alte două state membre nu au transpus încă directiva. Comisia va continua să colaboreze cu toate statele membre pentru a contribui la punerea în aplicare efectivă a directivei. De asemenea, Comisia va continua să își îndeplinească rolul care îi revine în materie de aplicare a dreptului UE, utilizând în ultimă instanță procedurile de încălcare a dreptului UE, dacă este cazul.

8.3. Directiva nu a armonizat pe deplin abordarea în materie de păstrare a datelor și nu a creat condiții de concurență echitabile pentru operatori

Directiva a asigurat faptul că, în prezent, datele sunt păstrate în majoritatea statelor membre. Directiva nu garantează în sine faptul că stocarea, recuperarea și utilizarea datelor respectă pe deplin dreptul la viață privată și la protecția datelor cu caracter personal. Responsabilitatea pentru garantarea acestor drepturi aparține statelor membre. Obiectivul directivei era numai armonizarea parțială a abordărilor în materie de păstrare a datelor; prin urmare, nu este surprinzător faptul că nu există o abordare comună, nici în ceea ce privește dispozițiile specifice ale directivei, ca de exemplu limitarea scopului sau perioadele de păstrare, nici în ceea ce privește aspectele care nu fac obiectul domeniului său de aplicare, ca de exemplu rambursarea costurilor. Cu toate acestea, dincolo de gradul de variație prevăzut în mod explicit de directivă, diferențele în ceea ce privește aplicarea la nivel național a dispozițiilor în materie de păstrare a datelor au generat dificultăți considerabile pentru operatori.

8.4. Costurile suportate de operatori ar trebui rambursate în mod consecvent

În continuare nu există siguranță juridică pentru industrie. Obligația păstrării și recuperării datelor reprezintă un cost semnificativ pentru operatori, în special pentru operatorii mai mici, iar operatorii sunt afectați și rambursați în mod diferit în funcție de statele membre, deși nu există dovezi potrivit cărora sectorul telecomunicațiilor în ansamblul său a fost afectat negativ din cauza directivei. Comisia va lua în considerare modalități de rambursare consecventă a costurilor suportate de operatori.

8.5. Asigurarea proporționalității în procesul integrat de stocare, recuperare și utilizare a datelor

Comisia se va asigura că orice propunere viitoare în materie de păstrare a datelor respectă principiul proporționalității și că este adecvată pentru atingerea obiectivului de combatere a infracțiunilor grave și a terorismului și că nu depășește ceea ce este necesar pentru îndeplinirea acestuia. Comisia va recunoaște că orice exceptări sau limitări care vizează protecția datelor cu caracter personal ar trebui să se aplice doar în măsura în care sunt necesare. Comisia va evalua în mod aprofundat implicațiile unei reglementări mai stricte în materie de stocare, acces și utilizare a datelor privind traficul pentru eficacitatea și eficiența sistemului de justiție penală și a aplicării legii. În evaluarea impactului, ar trebui să fie analizate, în special, următoarele domenii:

- consecvența în limitarea scopului de păstrare al datelor și tipurile de infracțiuni pentru care datele păstrate pot fi accesate și utilizate;
- armonizarea în mai mare măsură și, dacă este posibil, scurtarea perioadelor de păstrare obligatorie a datelor;
- asigurarea supravegherii independente a cererilor de acces și a regimului general de păstrare a datelor și de acces la date aplicat în toate statele membre;
- limitarea numărului autorităților autorizate să aibă acces la date;
- reducerea categoriilor de date care trebuie păstrate;

- orientări privind măsurile de securitate tehnice și organizaționale aferente accesului la date, inclusiv procedurile de transfer;

- orientări privind utilizarea datelor, inclusiv prevenirea extragerii datelor și

- dezvoltarea de indici de cuantificare fezabili și de proceduri de raportare pentru a facilita compararea aplicării și evaluării unui viitor instrument.

Comisia va analiza, de asemenea, dacă o abordare la nivelul UE în materie de conservare a datelor ar putea completa aspectele legate de păstrarea datelor.

În ceea ce privește „lista de verificare" privind drepturile fundamentale și abordarea gestionării informațiilor în spațiul de libertate, securitate și justiție[127], Comisia va analiza fiecare dintre aceste domenii conform principiului proporționalității și cerinței privind caracterul previzibil. De asemenea, Comisia va asigura coerența cu revizuirea în curs a cadrului UE privind protecția datelor[128].

8.6. Etapele următoare

Luând în considerare prezenta evaluare, Comisia va propune o revizuire a cadrului actual privind păstrarea datelor. Comisia va elabora mai multe opțiuni, în consultare cu autoritățile de aplicare a legii, autoritățile judiciare, grupurile care reprezintă industria și consumatorii, autoritățile pentru protecția datelor și organizațiile societății civile. Comisia va analiza în continuare percepția publicului cu privire la păstrarea datelor și impactul său asupra comportamentului. Aceste concluzii se vor regăsi într-o analiză a impactului opțiunilor de politică identificate, care va sta la baza propunerii Comisiei.

---

127 A se vedea mai sus referința la comunicarea privind punerea în aplicare a Cartei drepturilor fundamentale; „Prezentare generală asupra modului de gestionare a informațiilor în spațiul de libertate, securitate și justiție", COM(2010)385, 20.7.2010.

128 COM(2010) 609, 4.11.2010.

Anexă: statistici suplimentare referitoare la păstrarea datelor privind traficul

Note privind anexa

1. Vechimea datelor înseamnă timpul scurs între data la care au fost păstrate datele și data la care autoritatea competentă a solicitat transmiterea acestora.

2. Date referitoare la internet înseamnă datele care privesc accesul la internet, poșta electronică și telefonia prin internet.

3. Statisticile pentru Republica Cehă, Letonia și Polonia fac obiectul unor rezerve (a se vedea secțiunea 5.1).

Statistici transmise de statele membre pentru 2008

Tabelul 7: cereri de date privind traficul care au fost păstrate, în funcție de vechime, în 2008									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	102 691	18 440	10 110	319	0	0	0	0	131 560
Danemarca	2 669	672	185	37	23	2	7	4	3 599
Germania	9 363	2 336	985	0	0	0	0	0	12 684
Estonia	2 773	733	157	827	0	0	0	0	4 490
Irlanda	8 981	2 016	936	1 855	90	85	78	54	14 095
Grecia	Nu au fost furnizate defalcări în funcție de vechime.								584
Spania	22 629	15 868	10 298	4 783	0	0	0	0	53 578
Franța	Nu au fost furnizate defalcări în funcție de vechime.								50 3437
Italia	Nu au fost furnizate.								
Cipru	30	4	0	0	0	0	0	0	34
Letonia	10 539	2 739	1 368	1 211	597	438	0	0	16 892
Lituania	55 735	23 817	5 251	512	0	0	0	0	85 315
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	810	59	0	0	0	0	0	0	869
Țările de Jos	Nu au fost furnizate defalcări în funcție de vechime.								85 000
Austria	Nu au fost furnizate defalcări în funcție de vechime.								3 093
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate defalcări în funcție de vechime.								2 821
Slovacia	Nu au fost furnizate.								
Finlanda	9 134	1 144	448	214	268				4 008
Suedia	Nu au fost furnizate.								
Regatul Unit	315 350	88 339	34 665	19 398	6 385	2 973	1 536	1 576	470 222
Total	**533 504**	**15 6167**	**64 403**	**29 156**	**7 095 ***	**3 230 ***	**1 353 ***	**1 366 ***	**1 392 281**

* Exclusiv Finlanda

Tabelul 8: cereri de date privind traficul care au fost păstrate, pe tipuri de date, în 2008 (în paranteză numărul de cazuri în care cererile de date nu au putut fi satisfăcute – dacă au fost furnizate)				
Tip de date/ stat membru	**Date privind rețeaua de telefonie fixă**	**Date privind telefonia mobilă**	**Date referitoare la internet**	**Total**
Belgia	Nu au fost furnizate.			
Bulgaria	Nu au fost furnizate.			
Republica Cehă	4 983 (131)	12 5040 (2 276)	1 537 (83)	131 560 (2 490)
Danemarca	192 (0)	3 273 (5)	134 (0)	3 599 (5)
Germania	Nu au fost furnizate defalcări pe tipuri de date.			12684 (931)
Estonia	4 114 (1 519)	376 (7)	Nu au fost furnizate.	4 490 (1 526)
Irlanda	5 317 (16)	5 873 (48)	2 905 (33)	14 095 (97)
Grecia	Nu au fost furnizate defalcări pe tipuri de date.			584
Spania	4 448 (0)	40 013 (0)	9 117 (0)	53 578 (0)
Franța	Nu au fost furnizate defalcări pe tipuri de date.			503 437
Italia	Nu au fost furnizate.			
Cipru	3 (0)	31 (5)	0 (0)	34 (5)
Letonia	1 602 (90)	14 238 (530)	1 052 (76)	16 892 (696)
Lituania	765 (72)	84 550 (5 657)	Nu au fost furnizate.	85 315 (5 729)
Luxemburg	Nu au fost furnizate.			
Ungaria	Nu au fost furnizate.			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Țările de Jos	Nu au fost furnizate defalcări pe tipuri de date.			85 000
Austria	Nu au fost furnizate defalcări pe tipuri de date.			3 093
Polonia	Nu au fost furnizate.			
Portugalia	Nu au fost furnizate.			
România	Nu au fost furnizate.			
Slovenia	Nu au fost furnizate defalcări pe tipuri de date.			2 821
Slovacia	Nu au fost furnizate.			
Finlanda	Nu au fost furnizate defalcări pe tipuri de date.			4 008
Suedia	Nu au fost furnizate.			
Regatul Unit	90 747 (0)	329 421 (0)	50 054 (0)	470 222 (0)
Total				**1 392 281**

Tabelul 9: cereri de date privind traficul aferente *rețelei de telefonie fixă* care au fost păstrate și transmise, în funcție de vechime, în 2008									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	3 669	916	143	124	0	0	0	0	4 852
Danemarca	133	28	31	0	0	0	0	0	192
Germania	Nu au fost furnizate.								
Estonia	1 876	161	74	484	0	0	0	0	2 595
Irlanda	4 118	712	197	182	32	21	23	16	5 301
Grecia	Nu au fost furnizate.								
Spania	1 948	1 431	741	328	0	0	0	0	4 448
Franța	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	3	0	0	0	0	0	0	0	3
Letonia	698	213	167	193	104	137	0	0	1 512
Lituania	251	442	0	0	0	0	0	0	693
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	28	1	0	0	0	0	0	0	29
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	54 805	27 052	5 340	753	1 135	437	1 050	175	9 0747
Total	**67 529**	**30 956**	**6 693**	**2 064**	**1 271**	**595**	**1 073**	**191**	**110 372**

Tabelul 10: cereri de date privind traficul aferente *telefoniei mobile* care au fost păstrate şi transmise, în funcţie de vechime, în 2008									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	98 232	17 013	7 518	1	0	0	0	0	122 764
Danemarca	2 433	628	143	33	20	1	7	3	3 268
Germania	Nu au fost furnizate.								
Estonia	248	58	35	28	0	0	0	0	369
Irlanda	4 326	820	230	240	57	63	52	37	5 825
Grecia	Nu au fost furnizate.								
Spania	17 403	12 114	7 444	3 052	0	0	0	0	40 013
Franţa	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	23	3	0	0	0	0	0	0	26
Letonia	8 928	2 298	1 085	746	394	257	0	0	13 708
Lituania	55 484	23 375	14	20	0	0	0	0	78 893
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	575	53	0	0	0	0	0	0	628
Ţările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	229 375	52 241	26 228	16 040	3 333	521	339	1 344	329 421
Total	**417 027**	**108 603**	**42 697**	**20 160**	**3 804**	**842**	**398**	**1 384**	**594 915**

Tabelul 11: cereri de date privind traficul *referitoare la internet* care au fost păstrate și transmise, în funcție de vechime, în 2008									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	737	412	137	168	0	0	0	0	1 454
Danemarca	102	14	11	2	3	1	0	1	134
Germania	Nu au fost furnizate.								
Estonia	Nu au fost furnizate.								
Irlanda	492	460	498	1 422	0	0	0	0	2 872
Grecia	Nu au fost furnizate.								
Spania	3 278	2 323	2 113	1403	0	0	0	0	9 117
Franța	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	0	0	0	0	0	0	0	0	0
Letonia	424	150	75	219	74	34	0	0	976
Lituania	Nu au fost furnizate.								
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	76	3	0	0	0	0	0	0	79
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	31 170	9 046	3 097	2 605	1 917	2 015	147	57	50 054
Total	**36 279**	**12 408**	**5 931**	**5 819**	**1 994**	**2 050**	**147**	**58**	**64 686**

Statistici transmise de statele membre pentru 2009

Tabelul 12: cereri de date păstrate, în funcție de vechime, în 2009									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	210 975	56 623	11 620	1 053	0	0	0	0	280 271
Danemarca	2 980	685	179	104	54	38	12	14	4 066
Germania	Nu au fost furnizate.								
Estonia	4 299	1 836	1 210	1 065	0	0	0	0	8 410
Irlanda	8 117	1 652	805	297	168	134	69	41	11 283
Grecia	Nu au fost furnizate.								
Spania	29 775	19 346	13 999	6 970	0	0	0	0	70 090
Franța	Nu au fost furnizate defalcări în funcție de vechime.								514 813
Italia	Nu au fost furnizate.								
Cipru	31	8	1	0	0	0	0	0	40
Letonia	20 758	2 414	1 088	796	565	475	0	0	26 096
Lituania	30 247	35 456	5 886	884	0	0	0	0	72 473
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	3 336	362	151	174	0	0	0	0	4 023
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Polonia	642 327	178 306	75 525	52 526	27 098	23 924	13 984	34 628	1 048 318
Slovenia	Nu au fost furnizate defalcări în funcție de vechime.								1 918
Slovacia	Nu au fost furnizate defalcări în funcție de vechime.								5 214
Finlanda	2 000	1 310	532	152	76	0	0	0	4 070
Suedia	Nu au fost furnizate.								
Regatul Unit	Nu au fost furnizate.								
Total	**954 845**	**297 998**	**110 996**	**64 021**	**27 961**	**24 571**	**14 065**	**34 683**	**2 051 085**

Tabelul 13: cereri de date păstrate, pe tipuri de date, în 2009 (în paranteză numărul de cazuri în care cererile de date nu au putut fi satisfăcute – dacă au fost furnizate)				
Tip de date/ stat membru	**Date privind rețeaua de telefonie fixă**	**Date privind telefonia mobilă**	**Date referitoare la internet**	**Total**
Belgia	Nu au fost furnizate.			
Bulgaria	Nu au fost furnizate.			
Republica Cehă	13 843 (934)	256 074 (9 141)	10 354 (371)	280 271 (10 446)
Danemarca	133 (0)	3 771 (10)	162 (1)	4066 (11)
Germania	Nu au fost furnizate.			
Estonia	6 422 (2 279)	902 (21)	1 086 (468)	8 410 (2 768)
Irlanda	4 542 (16)	5 239 (20)	1 502 (56)	11 283 (92)
Grecia	Nu au fost furnizate.			
Spania	5 055 (0)	56 133 (0)	8 902 (0)	70 090 (0)
Franța	Nu au fost furnizate defalcări pe tipuri de date.			514 813
Italia	Nu au fost furnizate.			
Cipru	0 (0)	23 (3)	14 (0)	40 (3)
Letonia	1 672 (218)	22 796 (102)	1 628 (240)	26 096 (560)
Lituania	1 321 (0)	51 573 (6 237)	19 579 (343)	72 473 (6 580)
Luxemburg	Nu au fost furnizate.			
Ungaria	Nu au fost furnizate.			
Malta	156 (10)	3 693 (882)	174 (10)	4 023 (902)
Țările de Jos	Nu au fost furnizate.			
Austria	Nu au fost furnizate.			
Polonia	Nu au fost furnizate defalcări pe tipuri de date.			1 048 318
Portugalia	Nu au fost furnizate.			
România	Nu au fost furnizate.			
Slovenia	Nu au fost furnizate defalcări pe tipuri de date.			1 918 (48)
Slovacia	Nu au fost furnizate defalcări pe tipuri de date.			5 214 (157)
Finlanda	Nu au fost furnizate defalcări pe tipuri de date.			4 070
Suedia	Nu au fost furnizate.			
Regatul Unit	Nu au fost furnizate.			
Total				**2 051 082 (1069 885)**

Tabelul 14: cereri de date privind *rețeaua de telefonie fixă* care au fost păstrate și transmise, în funcție de vechime, în 2009									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	9 919	2 907	47	36	0	0	0	0	12 909
Danemarca	105	19	7	2	0	0	0	0	133
Germania	Nu au fost furnizate.								
Estonia	2 254	866	599	424	0	0	0	0	4 143
Irlanda	3 934	337	69	70	50	39	16	11	4 526
Grecia	Nu au fost furnizate.								
Spania	2 371	1 492	844	348	0	0	0	0	5 055
Franța	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	0	0	0	0	0	0	0	0	0
Letonia	744	253	157	143	68	89	0	0	1 454
Lituania	469	773	73	6	0	0	0	0	1 321
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	83	25	18	20	0	0	0	0	146
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	Nu au fost furnizate.								
Total	**19 879**	**6 672**	**1 814**	**1 049**	**118**	**128**	**16**	**11**	**29 687**

Tabelul 15: cereri de date privind *telefonia mobilă* care au fost păstrate și transmise, în funcție de vechime, în 2009									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	197 620	48 841	472	0	0	0	0	0	246 933
Danemarca	2 777	639	162	98	47	19	12	7	3 761
Germania	Nu au fost furnizate.								
Estonia	318	397	96	70	0	0	0	0	881
Irlanda	3 669	835	220	210	115	92	50	28	5 219
Grecia	Nu au fost furnizate.								
Spania	24 065	15 648	11 147	5 273	0	0	0	0	56 133
Franța	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	17	16	0	0	0	0	0	0	23
Letonia	18 832	1 912	778	515	394	263	0	0	22 694
Lituania	25 713	19 595	28	0	0	0	0	0	45 336
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	2 332	246	111	122	0	0	0	0	2 811
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	Nu au fost furnizate.								
Total	**275 343**	**88 119**	**13 014**	**6 288**	**556**	**374**	**62**	**35**	**383 791**

Tabelul 16: cereri de date *referitoare la internet* care au fost păstrate și transmise, în funcție de vechime, în 2009									
Vechimea datelor solicitate (luni)/stat membru	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgia	Nu au fost furnizate.								
Bulgaria	Nu au fost furnizate.								
Republica Cehă	3 369	4 811	861	942	0	0	0	0	9 983
Danemarca	98	27	10	4	4	7	0	1	151
Germania	Nu au fost furnizate.								
Estonia	315	145	56	102	0	0	0	0	618
Irlanda	489	455	502	0	0	0	0	0	1 446
Grecia	Nu au fost furnizate.								
Spania	3 339	2 206	2 008	1 349	0	0	0	0	8 902
Franța	Nu au fost furnizate.								
Italia	Nu au fost furnizate.								
Cipru	12	2	0	0	0	0	0	0	14
Letonia	852	198	74	90	88	86	0	0	1 388
Lituania	4 060	15 087	1	88	0	0	0	0	19 236
Luxemburg	Nu au fost furnizate.								
Ungaria	Nu au fost furnizate.								
Malta	150	14	0	0	0	0	0	0	164
Țările de Jos	Nu au fost furnizate.								
Austria	Nu au fost furnizate.								
Polonia	Nu au fost furnizate.								
Portugalia	Nu au fost furnizate.								
România	Nu au fost furnizate.								
Slovenia	Nu au fost furnizate.								
Slovacia	Nu au fost furnizate.								
Finlanda	Nu au fost furnizate.								
Suedia	Nu au fost furnizate.								
Regatul Unit	Nu au fost furnizate.								
Total	**12 684**	**22 945**	**3 512**	**2 575**	**92**	**93**	**0**	**1**	**41 902**