



**SVET  
EVROPSKE UNIJE**

**Bruselj, 19. april 2011 (02.05)  
(OR. en)**

**9324/11**

**DAPIX 38  
TELECOM 47  
COPEN 85**

**SPREMNI DOPIS**

---

Pošiljatelj:	za generalnega sekretarja Evropske komisije: direktor Jordi AYET PUIGARNAU
Datum prejema:	18. april 2011
Prejemnik:	generalni sekretar Sveta Evropske unije Pierre de BOISSIEU
Št. dok. Kom.:	COM(2011) 225 konč.
Zadeva:	Poročilo Komisije Svetu in Evropskemu parlamentu Ocenjevalno poročilo o Direktivi o hrambi podatkov (Direktiva 2006/24/ES)

---

Delegacije prejmejo priloženi dokument Komisije COM(2011) 225 konč.

Priloga: COM(2011) 225 konč.



EVROPSKA KOMISIJA

Bruselj, 18.4.2011  
COM(2011) 225 konč.

**POROČILO KOMISIJE SVETU IN EVROPSKEMU PARLAMENTU**

**Ocenjevalno poročilo o Direktivi o hrambi podatkov (Direktiva 2006/24/ES)**

# POROČILO KOMISIJE SVETU IN EVROPSKEMU PARLAMENTU

## Ocenjevalno poročilo o Direktivi o hrambi podatkov (Direktiva 2006/24/ES)

### 1. UVOD

Direktiva o hrambi podatkov<sup>1</sup> (v nadaljnjem besedilu: Direktiva) določa, da morajo države članice ponudnikom javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij (v nadaljnjem besedilu: ponudniki) naložiti obveznost, da podatke o prometu in lokaciji hranijo od šestih mesecev do dveh let za namene preiskovanja, odkrivanja in pregona hudih kaznivih dejanj.

To poročilo Komisije v skladu s členom 14 Direktive ocenjuje njeno uporabo v državah članicah in njen vpliv na gospodarske subjekte in potrošnike ob upoštevanju nadaljnega razvoja v tehnologiji elektronskih komunikacij in statistike, ki jih prejme Komisija, da se ugotovi, ali je potrebna sprememba določb te direktive, zlasti glede zajetja podatkov in obdobja hrambe. To poročilo preučuje tudi posledice uporabe Direktive za temeljne pravice in sicer zaradi kritik, ki jih je bila hramba podatkov na splošno deležna, in proučuje, ali so potrebni ukrepi za obravnavanje pomislekov, povezanih z uporabo anonimnih kartic SIM za kriminalne namene<sup>2</sup>.

Na splošno je ocena pokazala, da je hramba podatkov dragoceno orodje kazenskopravnih sistemov in organov pregona v EU. Prispevek Direktive k usklajevanju hrambe podatkov je na primer omejen glede omejitve namena, obdobja hrambe in tudi na področju povračila stroškov, ki jih imajo ponudniki, kar je zunaj področja uporabe Direktive. Zaradi posledic in nevarnosti za notranji trg in za spoštovanje pravice do zasebnosti ter varstva osebnih podatkov bi morala EU prek skupnih predpisov še naprej zagotavljati, da se dosledno ohranjajo visoki standardi za shranjevanje, pridobivanje in uporabo podatkov o prometu in lokaciji. Ob upoštevanju teh ugotovitev bo Komisija na podlagi ocene učinka predlagala spremembe Direktive.

### 2. OZADJE TE OCENE

To ocenjevalno poročilo je bilo pripravljeno na podlagi obsežnih razprav z državami članicami, strokovnjaki in zainteresiranimi stranmi ter z njihovimi prispevki.

Maja 2009 je Komisija organizirala konferenco z naslovom „K oceni Direktive o hrambi podatkov“, ki so se je udeležili organi za varstvo podatkov ter predstavniki zasebnega

---

<sup>1</sup> Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, UL L 105, 13.4.2006, str. 54-63

<sup>2</sup> Sklepi Sveta o boju proti kaznivim zlorabi in anonimni uporabi elektronskih komunikacij, 2908. zasedanje Sveta za pravosodje in notranje zadeve, Bruselj, 27.-28. november 2008.

sektorja, civilne družbe in akademskih krogov. Komisija je septembra 2009 zainteresiranim stranem iz teh skupin poslala vprašalnik in prejela okrog 70 odgovorov<sup>3</sup>. Decembra 2010 je Komisija priredila drugo konferenco z naslovom „Prevzem Direktive o hrambi podatkov“, ki so se je udeležile podobne zainteresirane strani in izmenjale predhodne ocene Direktive in razpravljale o prihodnjih izzivih na tem področju.

Od oktobra 2009 do marca 2010 se je Komisija srečala s predstavniki vsake države članice in pridružene države ekonomskega gospodarskega prostora, da so razpravljali o nadaljnjih podrobnostih vprašanj glede uporabe Direktive. Države članice so začele Direktivo uporabljati pozneje, kot je bilo pričakovano, zlasti v zvezi s podatki, povezanimi z internetom. Zamude pri prenosu so pomenile, da je devet držav članic Komisiji lahko posredovalo popolne statistične podatke bodisi za leto 2008 bodisi za leto 2009, ki jih zahteva člen 10 Direktive, čeprav je sicer 19 držav članic posredovalo nekaj statističnih podatkov (glej oddelek 4.7). Komisija je julija 2010 pisala državam članicam in zahtevala nadaljnje kvantitativne in kvalitativne informacije, ki se nanašajo na nujnost hranjenja podatkov, ki organom pregona omogočajo doseganje rezultatov. Deset držav članic je posredovalo podrobnosti o posebnih primerih, v katerih se je izkazalo, da so bili podatki potrebni<sup>4</sup>.

To poročilo se opira na dokumente o stališčih, ki jih je od svoje ustanovitve leta 2008 sprejela „platforma za hrambo elektronskih podatkov za preiskovanje, odkrivanje in pregon težjih kaznivih dejanj“<sup>5</sup>. Komisija je upoštevala poročila delovne skupine za varstvo podatkov<sup>6</sup> iz člena 29 in zlasti poročilo o drugem izvršilnem ukrepu, to je oceno izpolnjevanja zahtev Direktive glede varstva podatkov in varnosti podatkov v državah članicah<sup>7</sup>.

### **3. HRAMBA PODATKOV V EVROPSKI UNIJI**

#### **3.1. Hramba podatkov za namene pregona in kazenskih postopkov**

Ponudniki storitev in omrežij (v nadaljnjem besedilu: ponudniki) med opravljanjem svojih dejavnosti obdelujejo osebne podatke z namenom pošiljanja sporočila, zaračunavanja, plačil medomrežnega povezovanja, trženja in nekaterih drugih storitev z dodano vrednostjo. Taka obdelava vključuje navedbo vira, cilja, datuma, časa, trajanja in vrste komunikacije ter

---

<sup>3</sup> Odgovori so bili objavljeni na spletišču Komisije ([http://ec.europa.eu/home-affairs/news/consulting\\_public/consulting\\_0008\\_en.htm](http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm)).

<sup>4</sup> Belgija, Češka, Ciper, Litva, Madžarska, Nizozemska, Poljska, Slovenija, Združeno kraljestvo. Tudi Švedska je poročala o več primerih posebnih hudih kaznivih dejanj, v katerih so bili za obsodbe odločilni podatki o preteklem prometu, ki so bili na voljo kljub temu, da ni bilo obveznosti hrambe podatkov.

<sup>5</sup> Ta strokovna skupina je bila ustanovljena s Sklepom Komisije 2008/324/ES, UL L 111, 23.4.2008, str. 11–14. Komisija se redno srečuje s skupino. Njeni dokumenti o stališčih so objavljeni na strani [http://ec.europa.eu/justice\\_home/doc\\_centre/police/doc\\_police\\_intro\\_en.htm](http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm).

<sup>6</sup> Delovna skupina za varstvo posameznikov pri obdelavi osebnih podatkov je bila ustanovljena na podlagi člena 29 Direktive o varstvu podatkov (Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).

<sup>7</sup> Poročilo 01/2010 o drugem skupnem izvršilnem ukrepu: Izpolnjevanje obveznosti ponudnikov telekomunikacij in ponudnikov internetnega dostopa na nacionalni ravni, ki jih zahteva nacionalna zakonodaja o hrambi podatkov o prometu na pravni podlagi členov 6 in 9 Direktive o e-zasebnosti 2002/58/ES in Direktive o hrambi podatkov 2006/24/ES, ki spreminja Direktivo o e-zasebnosti (WP 172), 13.7.2010 (glej [http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm)).

komunikacijske opreme uporabnikov in v primeru mobilne telefonije podatke o lokaciji opreme. V skladu z Direktivo 2002/58/ES o zasebnosti na področju elektronskih komunikacij (v nadaljnjem besedilu: Direktiva o e-zasebnosti)<sup>8</sup> je treba take podatke o prometu, ki se pridobijo pri uporabi elektronskih komunikacijskih storitev, načeloma izbrisati ali predelati v anonimne, potem ko niso več potrebni za namen prenosa komunikacije, razen kadar so potrebni za namene zaračunavanja in le tako dolgo, kot so za to potrebni, ali če je bila pridobljena privolitev naročnika ali uporabnika. Podatki o lokaciji se smejo obdelati šele potem, ko postanejo anonimni, ali s privolitvijo zadevnega uporabnika, in sicer v obsegu in trajanju, ki sta potrebna za izvedbo storitve z dodano vrednostjo.

Pred začetkom veljavnosti Direktive so nacionalni organi pod posebnimi pogoji od ponudnikov zahtevali dostop do teh podatkov, da so na primer lahko določili naročnika, ki uporablja naslov IP, analizirali komunikacijske dejavnosti ali določili lokacijo mobilnega telefona.

Na ravni EU je hrambo in uporabo podatkov za namene kazenskega pregona prva obravnavala Direktiva 97/66/ES o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju. Navedena direktiva je prva omogočala državam članicam, da sprejmejo tovrstne zakonodajne ukrepe, kadar je to potrebno za zaščito javne varnosti, obrambe ali javnega reda, vključno z gospodarsko blaginjo države, če se dejavnosti nanašajo na zadeve državne varnosti in izvajanje kazenske zakonodaje<sup>9</sup>.

To določbo je še bolj razvila Direktiva o e-zasebnosti, ki državam članicam omogoča, da sprejmejo zakonodajne ukrepe, ki odstopajo od načela zaupnosti komunikacij ter pod določenimi pogoji določajo tudi hrambo in dostop do podatkov in njihovo uporabo za namene kazenskega pregona. Člen 15(1) dovoljuje državam članicam, da omejijo pravice in obveznosti do zasebnosti, vključno s hrambo podatkov za omejeno obdobje, kadar „takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito nacionalne varnosti (to je državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema“.

Vloga hranjenih podatkov v kazenskopравnih sistemih in kazenskem pregonu je dodatno obravnavana v oddelku 5.

### **3.2. Cilj in pravna podlaga Direktive o hrambi podatkov**

Zaradi določb Direktive 97/66/ES in Direktive o e-zasebnosti, ki državam članicam dovoljujejo, da sprejmejo zakonodajo o hrambi podatkov, so ponudniki v nekaterih državah članicah morali kupiti opremo za hrambo podatkov in zaposliti osebje za pridobivanje podatkov v imenu organov pregona, ponudniki v drugih državah članicah pa ne, kar je povzročilo izkrivljanje na notranjem trgu. Poleg tega so gibanja v poslovnih modelih in ponudbi storitev, kot je rast pavšalnih cen, predplačniških in brezplačnih elektronskih

---

<sup>8</sup> Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 0037-0047).

<sup>9</sup> Člen 14(1) Direktive 97/66/ES Evropskega parlamenta in Sveta z dne 15. decembra 1997 o obdelavi osebnih podatkov in varstvu zasebnosti v telekomunikacijskem sektorju (UL L 24, 30.1.1998, str. 1–8).

komunikacijskih storitev, povzročila, da so ponudniki postopno prenehali shranjevati podatke o prometu in lokaciji za namene zaračunavanja in s tem zmanjšali razpoložljivost takih podatkov za namene pregona in kazenskih postopkov. Zaradi terorističnih napadov v Madridu leta 2004 in v Londonu leta 2005 je razprava na ravni EU o načinu obravnave teh vprašanj postala še bolj nujna.

Ob upoštevanju navedenega Direktiva o hrambi podatkov od držav članic zahteva, da ponudnikom javno dostopnih elektronskih komunikacijskih storitev in javnih komunikacijskih omrežij naložijo obveznost, da hranijo podatke o komunikaciji za namene preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih države članice opredeljujejo v svojih nacionalnih zakonodajah, in zahteva uskladitev nekaterih s tem povezanih vprašanj v EU.

Direktiva spreminja člen 15(1) Direktive o e-zasebnosti tako, da mu dodaja odstavek, ki določa, da se člen 15(1) ne uporablja za podatke, hranjene v skladu z Direktivo o hrambi podatkov<sup>10</sup>. Zato je državam članicam (kakor je navedeno v uvodni izjavi 12) še naprej dovoljeno odstopanje od načela zaupnosti komunikacij. Direktiva (o hrambi podatkov) ureja hrambo podatkov samo za bolj omejen namen preiskovanja, odkrivanja in pregona hudih kaznivih dejanj.

Zaradi tega zapletenega pravnega razmerja med Direktivo in Direktivo o e-zasebnosti in ker v nobeni od teh dveh direktiv ni opredeljen pojem „hudo kaznivo dejanje“, je po eni strani težko razlikovati med ukrepi, ki so jih države članice sprejele za prenos obveznosti glede hrambe podatkov iz Direktive, in po drugi strani bolj splošno prakso hrambe podatkov v državah članicah, ki jo dovoljuje člen 15(1) Direktive o e-zasebnosti<sup>11</sup>. To je dodatno obravnavano v oddelku 4.

Direktiva temelji na členu 95 Pogodbe o ustanovitvi Evropske skupnosti (ki ga je nadomestil člen 114 Pogodbe o delovanju Evropske unije) o vzpostavitvi in delovanju notranjega trga. Po sprejetju Direktive je bila njena pravna podlaga izpodbijana pred Sodiščem Evropske unije na podlagi dejstva, da je bil glavni cilj preiskovanje, odkrivanje in pregon hudih kaznivih dejanj. Sodišče Evropske unije je odločilo, da Direktiva ureja postopke, ki so neodvisni od izvajanja vsakega morebitnega policijskega in sodnega ukrepa sodelovanja na kazenskem področju in z direktivo niso poenoteni niti dostop pristojnih nacionalnih organov do podatkov niti uporaba in izmenjava teh podatkov med temi organi. Zato je ugotovilo, da se Direktiva v bistvu nanaša na dejavnosti ponudnikov v zadevnem sektorju notranjega trga. Skladno s tem je potrdilo pravno podlago<sup>12</sup>.

---

<sup>10</sup> Člen 11 Direktive določa: „V člen 15 Direktive 2002/58/ES se vstavi naslednji odstavek: ‚1a. Odstavek 1 se ne uporablja za podatke, katerih hramba je posebej zahtevana v Direktivi 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij za namene iz člena 1(1) navedene direktive.‘“

<sup>11</sup> Delovna skupina iz člena 29 se sprašuje, ali „je bila direktiva [o hrambi podatkov] mišljena kot odstopanje od splošne obveznosti, da se podatki o prometu po zaključku elektronske komunikacije izbrišejo ali da se določi hramba vseh navedenih ponudnikov podatkov, ki so že pooblaščen za shranjevanje za svoje poslovne namene.“

<sup>12</sup> Sodba Sodišča z dne 10. februarja 2009 v zadevi Irska proti Evropskemu parlamentu in Svetu Evropske unije (C-301/06), ZOdl., str. I-00593.

### 3.3. Ohranitev podatkov

Hramba podatkov se razlikuje od ohranitve podatkov (poznane tudi kot „hitra zamrznitev“), na podlagi katere so ponudniki, ki jim je vročena odločba sodišča, dolžni od datuma odločbe o ohranitvi podatke hraniti samo za določene posameznike, osumljene kriminalne dejavnosti. Ohranitev podatkov je eno od preiskovalnih orodij, ki jih predvidevajo in uporabljajo sodelujoče države na podlagi Konvencije Sveta Evrope o kibernetiski kriminaliteti<sup>13</sup>. Skoraj vse sodelujoče države so vzpostavile kontaktno točko, katere vloga je zagotavljanje takojšnje pomoči pri preiskavah ali postopkih v zvezi s kibernetisko kriminaliteto. Vendar se zdi, da vse pogodbenice Konvencije niso predvidele ohranitve podatkov in ni še ocene učinkovitosti modela glede boja proti kibernetiski kriminaliteti<sup>14</sup>. Nedavno je bila razvita vrsta ohranitve podatkov, ki se imenuje „hitra zamrznitev plus“. Ta model presega ohranitev podatkov v tem, da lahko sodnik dobi tudi dostop do podatkov, ki jih ponudnik še ni izbrisal. Po zakonodaji bi bila zelo omejena oprostitev obveznosti, da se za kratko obdobje izbrišejo podatki o določeni komunikaciji, ki se običajno ne shranjujejo, kot so podatki o lokaciji, podatki o internetni povezavi in dinamični naslovi IP za uporabnike s pavšalno naročnino in kadar podatkov ni treba shranjevati za namene zaračunavanja.

Zagovorniki ohranitve podatkov menijo, da manj posega v zasebnost kot hramba podatkov. Vendar se večina držav članic ne strinja, da bi katera od različic ohranitve podatkov lahko ustrezno nadomestila hrambo podatkov, in trdi, da hramba podatkov pomeni, da so na voljo pretekli podatki, ohranitev podatkov pa ne zagotavlja možnosti vzpostavljanja dokaznih sledi pred odločbo o ohranitvi, ne omogoča preiskav, v katerih je cilj neznan, in ne omogoča zbiranja dokazov o gibanju na primer žrtev ali prič kaznivega dejanja<sup>15</sup>.

## 4. PRENOS DIREKTIVE O HRAMBI PODATKOV

Države članice so morale Direktivo prenesti do 15. septembra 2007, z možnostjo odložitve izvajanja obveznosti glede hrambe, ki se nanaša na dostop do interneta, internetno elektronsko pošto in internetno telefonijo do 15. marca 2009.

Analiza v nadaljevanju temelji na obvestilih o prenosu, ki jih je Komisija prejela od petindvajsetih držav članic, vključno z Belgijo, ki je Direktivo prenesla samo delno<sup>16</sup>. V Avstriji in na Švedskem poteka razprava o osnutku zakonodaje. V teh dveh državah članicah ni obveznosti hrambe podatkov, vendar organi pregona od ponudnikov lahko zahtevajo in pridobijo podatke o prometu v obsegu, ki je na voljo, in to tudi zahtevajo. Po prvotnem obvestilu Češke, Nemčije in Romunije o prenosu so ustavna sodišča teh treh držav članic

---

<sup>13</sup> Člen 16 Konvencije o kibernetiski kriminaliteti (<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>).

<sup>14</sup> Vir: Svet Evrope.

<sup>15</sup> To je priznalo tudi nemško ustavno sodišče v svoji sodbi, ki razveljavlja nemški zakon o prenosu Direktive (glej oddelek 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 z dne 2. marca 2010, odstavek 208).

<sup>16</sup> O prenosu Direktive je Komisijo uradno obvestilo petindvajset držav članic in sicer Belgija, Bolgarija, Češka, Danska, Nemčija, Grčija, Estonija, Irska, Španija, Francija, Italija, Ciper, Latvija, Litva, Luksemburg, Madžarska, Malta, Nizozemska, Poljska, Portugalska, Romunija, Slovenija, Slovaška, Finska in Združeno kraljestvo. Belgija je Komisijo obvestila, da je osnutek zakonodaje o dokončanju prenosa še vedno v obravnavi v parlamentu.

razveljavila domačo zakonodajo za prenos Direktive<sup>17</sup>, sedaj pa razmišljajo, kako bi ponovno prenesli Direktivo.

Ta oddelek analizira, kako so države članice prenesle ustrezne določbe Direktive. Proučuje tudi, ali so države članice odločile, da ponudnikom povrnejo stroške, ki jih je povzročila hramba podatkov in omogočanje pridobivanja podatkov, za katere v Direktivi ni nobene določbe, obravnava pa tudi pomembnost sodb ustavnih sodišč Nemčije, Romunije in Češke za Direktivo.

#### 4.1. Namen hrambe podatkov (člen 1)

Direktiva obvezuje države članice, da sprejmejo ukrepe za zagotovitev, da se podatki hranijo in so na voljo za namen preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kakor jih opredeljuje nacionalna zakonodaja vsake od držav članic. Vendar se nameni, navedeni za hrambo in/ali dostop do podatkov v domači zakonodaji, v EU še naprej razlikujejo. Deset držav članic (Bolgarija, Estonija, Irska, Grčija, Španija, Litva, Luksemburg, Madžarska, Nizozemska in Finska) je opredelilo „hudo kaznivo dejanje“ s sklicevanjem na najnižjo zaporno kazen, možnost, da se naloži kazen odvzema prostosti, ali na vrsto kaznivih dejanj, ki so opredeljena drugod v nacionalni zakonodaji. Osem držav članic (Belgija, Danska, Francija, Italija, Latvija, Poljska, Slovaška in Slovenija) zahteva, da se podatki ne hranijo samo za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj, ampak za vsa kazniva dejanja in za preprečevanje kaznivih dejanj ali na splošno zaradi nacionalne ali državne in/ali javne varnosti. Zakonodaja štirih držav članic (Cipra, Malte, Portugalske in Združenega kraljestva) navaja „hudo kaznivo dejanje“ ali „hud prekršek“, vendar ju ne opredeljuje. Podrobnosti so navedene v Preglednici 1.

<b>Preglednica 1: Omejitev namena hrambe podatkov, navedena v nacionalni zakonodaji</b>	
Belgija	Za preiskovanje in pregon kaznivih dejanj, pregon zlorabe telefonskih številok za klic v sili, preiskavo zlonamerne zlorabe elektronskega komunikacijskega omrežja ali storitve, za namene nalog zbiranja obveščevalnih podatkov, ki jih opravljajo obveščevalne in varnostne službe <sup>18</sup> .
Bolgarija	Za „odkrivanje in preiskovanje hudih kaznivih dejanj in kaznivih dejanj iz člena 319a-319f Kazenskega zakonika in za iskanje oseb“ <sup>19</sup> .
Češka	Direktiva ni prenesena.
Danska	Za preiskovanje in pregon kaznivih dejanj <sup>20</sup> .
Nemčija	Direktiva ni prenesena.

<sup>17</sup> Odločba romunskega ustavnega sodišča št. 1258 z dne 8. oktobra 2009, Uradni list Republike Romunije št. 789, 23.11.2009; sodba Bundesverfassungsgericht 1 BvR 256/08 z dne 2. marca 2010; Uradni list z dne 1. aprila 2011, sodba ustavnega sodišča z dne 22. marca o odločbah 3. in 4. odstavka oddelka 97 zakona št. 127/2005 Coll. o elektronskih komunikacijah in o spremembi nekaterih povezanih zakonov, kakor so bili spremenjeni, ter Uredba št. 485/2005 Coll. o hrambi podatkov in njihovem prenosu pristojnim organom.

<sup>18</sup> Člen 126(1) Zakona o elektronskih komunikacijah z dne 13. junija 2005.

<sup>19</sup> Člen 250a (2) Zakona o elektronskih komunikacijah (spremenjen) 2010.

<sup>20</sup> Člen 1 Odredbe o hrambi podatkov.

<b>Preglednica 1: Omejitev namena hrambe podatkov, navedena v nacionalni zakonodaji</b>	
Estonija	Lahko se uporablja, če je zbiranje dokazov z drugimi procesnimi dejanji onemogočeno ali posebej zapleteno in je predmet kazenskega postopka kaznivo dejanje [prve stopnje ali naklepno kaznivo dejanje druge stopnje z zaporno kaznijo najmanj tri leta] <sup>21</sup> .
Irska	Za preprečevanje hudih prekrškov [tj. prekrškov, ki se kaznujejo z zaporno kaznijo 5 let ali več, ali prekrškov na seznamu zakona o prenosu], zaščito varnosti države, reševanje človeških življenj <sup>22</sup> .
Grčija	Za odkrivanje posebej hudih kaznivih dejanj <sup>23</sup> .
Španija	Za odkrivanje, preiskovanje in pregon hudih kaznivih dejanj, navedenih v Kazenskem zakoniku ali posebni kazenski zakonodaji <sup>24</sup> .
Francija	Za odkrivanje, preiskovanje in pregon kaznivih dejanj in izključno za potrebe zagotavljanja potrebnih informacij sodnim organom ter za preprečevanje terorističnih dejanj in varovanje intelektualne lastnine <sup>25</sup> .
Italija	Za odkrivanje in zatiranje kaznivih dejanj <sup>26</sup> .
Ciper	Za preiskovanje hudih kaznivih dejanj <sup>27</sup> .
Latvija	Za zaščito državne in javne varnosti ali za zagotovitev preiskave kaznivih dejanj, kazenskega pregona in kazenskih postopkov na sodišču <sup>28</sup> .
Litva	Za preiskovanje, odkrivanje in pregon hudih in zelo hudih kaznivih dejanj, kot so opredeljena v Kazenskem zakoniku Litve <sup>29</sup> .
Luksemburg	Za odkrivanje, preiskovanje in pregon kaznivih dejanj, za katera je najvišja zaporna kazen eno leto ali več <sup>30</sup> .
Madžarska	Da se organom za preiskovanje, državnemu tožilcu, sodiščem in agencijam za nacionalno varnost omogoči, da opravljajo svoje dolžnosti, policiji ter nacionalnemu davčnemu in carinskemu uradu pa da preiskujejo naklepna kazniva dejanja, ki se kaznujejo z zaporno kaznijo dveh ali več let <sup>31</sup> .
Malta	Za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj <sup>32</sup> .
Nizozemska	Za preiskovanje in pregon hudih kaznivih dejanj, za katera se lahko naloži kazen odvzema prostosti <sup>33</sup> .
Avstrija	Direktiva ni prenesena.

<sup>21</sup> Pododdelek 110(1) Zakonika o kazenskem postopku.

<sup>22</sup> Člen 6 Komunikacije (Zakon o hrambi podatkov) 2011.

<sup>23</sup> Taka kazniva dejanja so opredeljena v členu 4 zakona št. 2225/1994; člen 1 zakona št. 3917/2011.

<sup>24</sup> Člen 1(1) zakona št. 25/2007.

<sup>25</sup> Zakoni, ki urejajo uporabo hranjenih podatkov za kazniva dejanja, preprečevanje terorističnih dejanj in varovanje intelektualne lastnine so: člen L.34-1(II), CPCE, zakon št. 2006-64 z dne 23. januarja 2006 in zakon št. 2009-669 z dne 12. junija 2009.

<sup>26</sup> Člen 132(1) Zakonika o varstvu podatkov.

<sup>27</sup> Člen 4(1) zakona št. 183(I)/2007.

<sup>28</sup> Člen 71(1) Zakona o elektronskih komunikacijah.

<sup>29</sup> Člen 65 zakona št. X-1835.

<sup>30</sup> Člen 1(1) zakona z dne 24. julija 2010.

<sup>31</sup> Za splošni namen hrambe podatkov člen 159/A zakona št. C/2003, kakor je bil spremenjen z zakonom št. CLXXIV/2007; namensko za dostop policije člen 68, zakon št. XXXIV/1994; namensko za dostop nacionalnega davčnega in carinskega urada člen 59, zakon št. CXXII/2010.

<sup>32</sup> Člen 20(1) pravnega obvestila št. 198/2008.

<sup>33</sup> Člen 126 Zakonika o kazenskem postopku.

<b>Preglednica 1: Omejitev namena hrambe podatkov, navedena v nacionalni zakonodaji</b>	
Poljska	Za preprečevanje ali odkrivanje kaznivih dejanj, za preprečevanje in odkrivanje fiskalnih kaznivih dejanj, če so primerni za sodne postopke, ki potekajo, jih uporabljajo tožilci in sodišča, za Agencijo za notranjo varnost, Obveščevalno agencijo, Osrednji protikorupcijski urad, Vojaško protiobveščevalno službo in Vojaško obveščevalno službo, da opravljajo svoje dolžnosti <sup>34</sup> .
Portugalska	Za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj <sup>35</sup> .
Romunija	Direktiva ni prenesena.
Slovenija	Za zagotavljanje nacionalne varnosti, ustavne ureditve ter varnostnih, političnih in gospodarskih interesov države ... in za namene obrambe države <sup>36</sup> .
Slovaška	Za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj <sup>37</sup> .
Finska	Za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj, določenih v poglavju 5a člena 3(1) Zakona o prisilnih ukrepih <sup>38</sup> .
Švedska	Direktiva ni prenesena.
Združeno kraljestvo	Za preiskovanje, odkrivanje in pregon hudih kaznivih dejanj <sup>39</sup> .

Večina držav članic, ki so prenesle Direktivo, v skladu s svojo nacionalno zakonodajo omogoča dostop do hranjenih podatkov in njihovo uporabo za namene, ki presegajo namene, zajete v Direktivi, vključno s preprečevanjem kriminala in bojem proti njemu na splošno ter ogrožanjem življenja in fizične integritete. To je dovoljeno v skladu z Direktivo o e-zasebnosti, vendar stopnja usklajenosti v zakonodaji EU na tem področju ostaja omejena. Verjetno je, da razlike v namenih hrambe podatkov vplivajo na količino in pogostost zahtevkov in s tem na stroške, ki nastanejo pri izpolnjevanju obveznosti iz Direktive. Ta položaj morebiti tudi ne zagotavlja zadostne predvidljivosti, ki se zahteva v vsakem zakonodajnem ukrepu, ki omejuje pravico do zasebnosti<sup>40</sup>. Komisija bo ocenila potrebo po višji stopnji usklajenosti na tem področju in možnosti, da se to doseže<sup>41</sup>.

<sup>34</sup> Člen 180a Zakona o telekomunikacijah z dne 16. julija 2004, kakor je bil spremenjen s členom 1 zakona z dne 24. aprila 2009.

<sup>35</sup> Člen 1 in člen 3(1) zakona št. 32/2008.

<sup>36</sup> Člen 170a(1) Zakona o elektronskih komunikacijah.

<sup>37</sup> Člen 59a (6) Zakona o elektronskih komunikacijah.

<sup>38</sup> Člen 14a (1) Zakona o elektronskih komunikacijah.

<sup>39</sup> Predpisi o hrambi podatkov (Direktiva ES) 2009 (2009 št. 859).

<sup>40</sup> Sodba Sodišča z dne 20. maja 2003 v združenih zadevah C-465/00, C-138/01 in C-139/01 (predlog Verfassungsgerichtshof in Oberster Gerichtshof za sprejetje predhodne odločbe): Rechnungshof (C-465/00) proti Österreichischer Rundfunk in drugi in Christa Neukomm (C-138/01) in Joseph Lauer mann (C-139/01) proti Österreichischer Rundfunk (Varstvo posameznikov pri obdelavi osebnih podatkov — Direktiva 95/46/ES — Varstvo zasebnosti— Razkritje podatkov o dohodkih zaposlenih v organih, ki jih Rechnungshof nadzoruje).

<sup>41</sup> Ob sprejetju Direktive je Komisija izdala izjavo, ki nakazuje, da bi bilo treba preučiti seznam kaznivih dejanj v evropskem nalogu za prijetje. (Okvirni Sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami.)

#### **4.2. Ponudniki morajo ravnati v skladu s hrambo podatkov (člen 1)**

Direktiva se uporablja za „ponudnike javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij“ (člen 1(1)). Dve državi članici (Finska in Združeno kraljestvo) od malih ponudnikov ne zahtevata hrambe podatkov, ker trdita, da bi bili stroški za ponudnika in državo večji od koristi za organe pregona in kazenske postopke. Štiri države članice (Latvija, Luksemburg, Nizozemska in Poljska) poročajo, da so vzpostavile drugačne upravne ureditve. Veliki ponudniki, prisotni v več državah članicah, z vidika stroškov uživajo ugodnosti ekonomije obsega, manjši ponudniki v nekaterih državah članicah pa ustanavljajo skupna podjetja ali zaradi zniževanja stroškov oddajo izvajanje gospodarskim družbam, specializiranim za hrambo in pridobivanje. Zunanje izvajanje tehničnih funkcij na tak način ne vpliva na obveznost ponudnikov, da ustrezno nadzirajo postopke obdelave in zagotovijo, da so vzpostavljeni zahtevani varnostni ukrepi. To lahko povzroča težave zlasti manjšim ponudnikom. Komisija bo proučila vprašanja varnosti podatkov ter vpliv na mala in srednje velika podjetja v povezavi z možnostmi za spremembo okvira hrambe podatkov.

#### **4.3. Dostop do podatkov: organi ter postopki in pogoji (člen 4)**

Države članice morajo „zagotoviti, da se [hranjeni podatki] zagotovijo samo pristojnim nacionalnim organom za vsak primer posebej in v skladu z nacionalnim pravom“. Vsaka država članica v nacionalnem pravu določi „postopke in pogoje za pridobitev dostopa do hranjenih podatkov v skladu z zahtevami glede nujnosti in sorazmernosti, in sicer ob upoštevanju ustreznih določb prava Evropske unije ali mednarodnega javnega prava, zlasti pa EKČP, kakor jo razlaga Evropsko sodišče za človekove pravice“.

V vseh državah članicah imajo dostop do hranjenih podatkov nacionalna policija in, razen v anglo-ameriškem pravu (Irska in Združeno kraljestvo), tožilci. Štirinajst držav članic med pristojnimi organi navaja varnostne ali obveščevalne službe ali vojaške službe. Šest držav članic navaja davčne in/ali carinske organe in tri države navajajo mejne organe. Ena država članica dovoljuje dostop do podatkov tudi drugim javnim organom, če imajo so po sekundarni zakonodaji pooblaščen za posebne namene. Enajst držav članic zahteva sodno pooblastilo za vsak zahtevek za dostop do hranjenih podatkov. V treh državah članicah se v večini primerov zahteva sodno pooblastilo. Štiri druge države članice zahtevajo pooblastilo višjega organa, ne pa sodnika. V dveh državah članicah se zdi, da je edini pogoj to, da je zahtevek v pisni obliki.

<b>Preglednica 2: Dostop do hranjenih podatkov o telekomunikacijah</b>		
	<i>Pristojni nacionalni organi</i>	<i>Postopki in pogoji</i>
Belgija	enota za pravosodno usklajevanje, preiskovalni sodniki, državni tožilec, kriminalistična policija	Dostop mora dovoliti sodnik ali tožilec. Ponudniki morajo na zahtevo v „realnem času“ zagotoviti podatke o naročniku in prometu ter lokaciji za klice, opravljene v zadnjem mesecu. Podatke za starejše klice je treba zagotoviti čim prej.
Bolgarija <sup>42</sup>	posebni direktorati in oddelki Državne agencije za nacionalno varnost, Ministrstvo za notranje zadeve, Služba za vojaške informacije, Vojaška policija, Minister za obrambo, Nacionalna preiskovalna agencija; sodišče in predprocesni organi pod pogoji	Dostop je možen samo na podlagi naloga predsednika regionalnega sodišča.
Češka	Direktiva ni prenesena.	
Danska <sup>43</sup>	policija	Za dostop je potrebno sodno pooblastilo; odločba sodišča se izda, če vloga izpolnjuje stroga merila o sumu, nujnosti in sorazmernosti.
Nemčija	Direktiva ni prenesena.	
Estonija <sup>44</sup>	urad policije in mejne straže, varnostna policija, za predmete in elektronske komunikacije pa Davčna in carinska uprava	Za dostop je potrebno dovoljenje preiskovalnega sodnika V nujnih primerih morajo ponudniki [hranjene podatke] „zagotoviti najpozneje v 10 urah, v drugih primerih pa v 10 delovnih dneh [od prejema zahtevka]“.
Irska <sup>45</sup>	člani Garda Síochána (policija) s činom Chief Superintendent ali višjim; častniki stalnih obrambnih sil s činom polkovnik ali višjim; funkcionarji Urada za državne finance na stopnji glavnega funkcionarja ali višje	Zahtevek mora biti v pisni obliki.
Grčija <sup>46</sup>	sodni, vojaški ali policijski javni organ	Za dostop je potrebna sodna odločba, ki navaja, da je preiskava z drugimi sredstvi nemogoča ali izredno težka.
Španija <sup>47</sup>	policijska enota, odgovorna za odkrivanje, preiskovanje in pregon hudih kaznivih dejanj, Nacionalni obveščevalni center in Carinska agencija	Za dostop pristojnih nacionalnih organov do teh podatkov je potrebno predhodno sodno pooblastilo.
Francija <sup>48</sup>	državni tožilec, pooblaščen policisti in orožniki	Policija mora vsak zahtevek za dostop do podatkov utemeljiti in pridobiti dovoljenje od osebe na Ministrstvu za notranje zadeve, ki jo imenuje Commission nationale de contrôle des interceptions de sécurité. Zahtevke za dostop obravnava imenovani

<sup>42</sup> Člen 250a(1) Zakona o elektronskih komunikacijah (spremenjen) 2010 (organi); člen 250b(2), 250c(1) Zakona o elektronskih komunikacijah (spremenjen) 2010 (dostop).

<sup>43</sup> Poglavje 71 Zakona o pravosodju.

<sup>44</sup> Pododdelek 112(2) in (3) Zakonika o kazenskem postopku (o organih in postopku); pododdelek 111(9) (pogoji) Zakona o elektronskih komunikacijah.

<sup>45</sup> Člen 6 Predloga zakona o komunikacijah (hramba podatkov) 2009.

<sup>46</sup> Člena 3 in 4 zakona št. 2225/94.

<sup>47</sup> Člena 6 in 7 zakona št. 25/2007.

Preglednica 2: Dostop do hranjenih podatkov o telekomunikacijah		
	<i>Pristojni nacionalni organi</i>	<i>Postopki in pogoji</i>
		uradnik, ki dela za ponudnika.
Italija <sup>49</sup>	državni tožilec, policija, odvetnik obtoženca ali osebe v preiskavi	Za dostop je potrebna „utemeljena odločba“, ki jo izda državni tožilec.
Ciper <sup>50</sup>	sodišča; državni tožilec, policija	Dostop mora odobriti tožilec, če meni, da lahko zagotovi dokaze, da je bilo storjeno hudo kaznivo dejanje. Sodnik lahko izda tako odločbo, če obstaja utemeljen sum hudega kaznivega dejanja in če je verjetno, da so podatki s takim dejanjem povezani.
Latvija <sup>51</sup>	pooblaščen uradniki v ustanovah za predhodne preiskave, osebe, ki opravljajo preiskovalno delo, pooblaščen uradniki v ustanovah državne varnosti, urad državnega tožilca, sodišča	Pooblaščen uradniki, urad državnega tožilca in sodišča morajo oceniti „primernost in ustreznost“ zahtevka, evidentirati zahtevek in zagotoviti varstvo pridobljenih podatkov. Pooblaščen organi lahko s ponudnikom popišejo sporazum, npr. za šifriranje posredovanih podatkov.
Litva <sup>52</sup>	organi za predhodne preiskave, tožilec, sodišče (sodniki) in pripadniki obveščevalne službe	Pooblaščen javni organi morajo pisno zahtevati hranjene podatke. Za dostop za predhodne preiskave je potreben sodni nalog.
Luksemburg <sup>53</sup>	sodni organi (preiskovalni sodniki, tožilec), organi, odgovorni za zaščito državne varnosti, obrambo, javno varnost in preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj	Za dostop je potrebno sodno pooblastilo.
Madžarska <sup>54</sup>	policija, nacionalni davčni in carinski urad, službe za nacionalno varnost, državni tožilec, sodišča	Policija in nacionalni davčni in carinski urad morata imeti dovoljenje tožilca. Agencije za nacionalno varnost in tožilec imajo lahko dostop do takih podatkov brez odločbe sodišča.
Malta <sup>55</sup>	policija Malte, varnostna služba	Zahtevki morajo biti v pisni obliki.
Nizozemska <sup>56</sup>	preiskovalni policist	Za dostop je potrebna odločba tožilca ali preiskovalnega sodnika.
Avstrija	Direktiva ni prenesena.	
Poljska <sup>57</sup>	policija, mejna straža, davčni inšpektorji, Agencija za notranjo varnost, Obveščevalna agencija, Osrednji protikorupcijski urad, vojaške protiobveščevalne službe in vojaške obveščevalne službe, sodišča in državni tožilec	Zahtevki morajo biti v pisni obliki. Zahtevke policije, mejne straže in davčnih inšpektorjev mora odobriti višji uradnik v organizaciji.

<sup>48</sup> Člena 60-1 in 60-2 Zakonika o kazenskem postopku (organi); člen L.31-1-1 (pogoji).

<sup>49</sup> Člen 132(3) Zakonika o varstvu podatkov.

<sup>50</sup> Člen 4(2) in (4) zakona št. 183(I)/2007.

<sup>51</sup> Člen 71(1) Zakona o elektronskih komunikacijah (organi); vladna uredba št. 820 (postopki).

<sup>52</sup> Člen 77(1) in (2) zakona št. X-1835; ustno poročilo Komisiji.

<sup>53</sup> Člen 5-2(1) in člen 9(2) zakona z dne 24. julija 2010 (organi); člen 67-1 Zakonika o kazenskih navodilih (pogoji).

<sup>54</sup> Člena 68(1) in 69(1)(c)(d) zakona št. XXXIV 1994; člen 9/A(1) zakona št. V 1972; členi 71(1), (3), (4), 178/A (4), 200, 201, 268(2) zakona št. XIX 1998; členi 40(1), 40(2), 53(1), 54(1)(j) zakona št. CXXV 1995.

<sup>55</sup> Člen 20(1) in (3) pravnega obvestila št. 198/2008.

<sup>56</sup> Člen 126ni Zakonika o kazenskem postopku.

<sup>57</sup> Člen 179(3) Zakona o telekomunikacijah z dne 16. julija 2004, kakor je bil spremenjen s členom 1 zakona z dne 24. aprila 2009.

<b>Preglednica 2: Dostop do hranjenih podatkov o telekomunikacijah</b>		
	<i>Pristojni nacionalni organi</i>	<i>Postopki in pogoji</i>
Portugalska <sup>58</sup>	kriminalistična policija, nacionalna republikanska garda, Urad za javno varnost, Vojaška kriminalistična policija, Oddelek za tujce in mejo, Pomorska policija	Za posredovanje podatkov je potrebno sodno pooblastilo, ker je dostop odločilen, da se odkrije resnica ali ker bi bilo na drug način dokaze nemogoče ali zelo težko pridobiti. Sodno pooblastilo mora izpolnjevati zahteve glede nujnosti in sorazmernosti.
Romunija	Direktiva ni prenesena.	
Slovenija <sup>59</sup>	policija, obveščevalne in varnostne agencije, obrambne agencije, odgovorne za obveščevalno in protiobveščevalno dejavnost ter varnostne misije	Za dostop je potrebno sodno pooblastilo.
Slovaška <sup>60</sup>	organi pregona, sodišča	Zahtevki morajo biti v pisni obliki.
Finska <sup>61</sup>	policija, mejna straža, carinski organi (za hranjene podatke o naročnikih, prometu in lokaciji), središče za odzivanje v izrednih razmerah, pomorske reševalne akcije, podsredišče za pomorsko reševanje (za identifikacijske podatke in podatke o lokaciji v izrednih razmerah)	Dostop do podatkov o naročnikih imajo vsi pristojni organi brez sodnega pooblastila. Za druge podatke je potrebna odločba sodišča.
Švedska	Direktiva ni prenesena.	
Združeno kraljestvo <sup>62</sup>	policija, obveščevalne službe, davčni in carinski organi, drugi javni organi, določeni v sekundarni zakonodaji	Dostop je dovoljen na podlagi dovoljenja „pooblaščenih oseb“ in preskusa nujnosti in sorazmernosti v posebnih primerih ter v okoliščinah, v katerih zakonodaja dovoljuje ali zahteva razkritje podatkov. S ponudniki so bili dogovorjeni posebni postopki.

Komisija bo ocenila potrebo po višji stopnji usklajenosti glede organov, ki imajo dostop do hranjenih podatkov, in postopkov za pridobitev dostopa, ter možnosti, da se to doseže. Možnosti lahko vključujejo bolj jasne sezname pristojnih organov, neodvisen in/ali sodni nadzor zahtevkov za podatke in minimalni standard postopkov za ponudnike pri odobritvi dostopa pristojnim organom.

#### **4.4. Področje uporabe hrambe podatkov in kategorije zajetih podatkov (členi 1(2), 3(2) in 5)**

Direktiva se uporablja za področja telefonije v fiksnem omrežju, mobilne telefonije, dostopa do interneta, internetne elektronske pošte in internetne telefonije. Določa (v členu 5) kategorije podatkov, ki jih je treba hraniti, in sicer podatke, potrebne za prepoznavanje:

- (a) vira komunikacije;
- (b) cilja komunikacije;

<sup>58</sup> Členi 2 (1), 3(2) in 9 zakona št. 32/2008.

<sup>59</sup> Člen 107c Zakona o elektronskih komunikacijah; člen 149b Zakonika o kazenskem postopku; člen 24(b) Zakona o Slovenski obveščevalno-varnostni agenciji; člen 32 Zakona o obrambi.

<sup>60</sup> Člen 59a (8) Zakona o elektronskih komunikacijah.

<sup>61</sup> Člen 35(1) in člen 36 Zakona o elektronskih komunikacijah; členi 31-33 Zakona o policiji; člen 41 Zakona o mejni straži.

<sup>62</sup> Člen 25 obrazec 1 Zakona o ureditvi preiskovalnih pooblastil iz leta 2000; člen 7 Uredbe o hrambi podatkov. Člen 22(2) RIPA določa namene, za katere ti organi lahko pridobijo podatke.

- (c) datuma, časa in trajanja komunikacije;
- (d) vrste komunikacije;
- (e) komunikacijske opreme uporabnikov ali kar je domnevno njihova oprema in
- (f) lokacije opreme za mobilno komunikacijo.

Zajema tudi (člen 3(2)) neuspešne klice, to je komunikacijo, pri kateri je bila povezava uspešno vzpostavljena, a ni bilo odgovora, oziroma je prišlo do prekinitve pri upravljanju omrežja in kjer ponudniki podatke o teh neuspešnih klicih pridobivajo ali obdelujejo ter hranijo ali beležijo. Podatki, ki razkrivajo vsebino komunikacije, se v skladu z Direktivo ne smejo hraniti. Naknadno je bilo tudi pojasnjeno, da so iskalne poizvedbe, to so strežniški dnevnik, ki se ustvarijo pri ponujanju storitve iskalnika, tudi zunaj področja uporabe Direktive, ker se šteje, da so podatki o vsebini in ne podatki o prometu<sup>63</sup>.

Enaindvajset držav članic je v svoji zakonodaji za prenos določilo hrambo vsake od teh kategorij podatkov. Belgija ni določila vrst podatkov o telefoniji, ki jih je treba hraniti, niti nima določb glede podatkov, povezanih z internetom. Tisti, ki so izpolnjevali vprašalnik Komisije, so menili, da ni treba spreminjati kategorij podatkov, ki jih je treba hraniti, čeprav je Evropski parlament Komisiji izdal pisno izjavo, v kateri poziva, naj se Direktiva „zaradi hitre obravnave otroške pornografije in spolnih zlorab na spletu“ razširi na iskalnike<sup>64</sup>. Delovna skupina za varstvo podatkov iz člena 29 je v svojem poročilu o drugem izvršilnem ukrepu trdila, da je treba šteti kategorije iz Direktive za izčrpane in da se ponudnikom ne sme naložiti nobenih dodatnih obveznosti glede hrambe podatkov. Komisija bo ocenila nujnost vseh teh kategorij podatkov.

#### **4.5. Obdobja hrambe (člen 6 in člen 12)**

Države članice morajo zagotoviti, da se podatki kategorij, opredeljenih v členu 5, hranijo za obdobje najmanj šestih mesecev in največ dveh let. Država članica lahko „v posebnih okoliščinah, ki upravičujejo podaljšanje najdaljšega obdobja“ najdaljše obdobje hrambe podaljša; o takem podaljšanju je treba uradno obvestiti Komisijo, ki lahko v šestih mesecih po uradnem obvestilu odobri ali zavrne podaljšanje. Čeprav se najdaljše obdobje lahko podaljša, pa ni določbe o skrajšanju hrambe pod šestmesečno obdobje. Vse države članice, razen ene, ki so prenesle Direktivo, uporabljajo obdobje ali obdobja hrambe v okviru teh omejitev in Komisija ni prejela nobenih uradnih obvestil o podaljšanju. Vendar pa v EU ni doslednega pristopa.

Petnajst držav članic določa eno samo obdobje za vse kategorije podatkov: ena država članica (Poljska) določa dveletno obdobje hrambe, ena (Latvija) določa 1,5-letno, deset enoletno (Bolgarija, Danska, Estonija, Grčija, Španija, Francija, Nizozemska, Portugalska, Finska, Združeno kraljestvo) in šest držav članic določa šestmesečno obdobje (Ciper, Luksemburg, Litva). Pet držav članic je opredelilo različna obdobja hrambe za različne kategorije podatkov:

<sup>63</sup> Mnenje delovne skupine iz člena 29 o vprašanih v zvezi z varstvom podatkov, povezanih z iskalniki, 4. april 2008.

<sup>64</sup> Pisna izjava na podlagi pravila 123 Poslovnika o oblikovanju evropskega sistema hitrega obveščanja proti pedofilom in spolnim nadlegovalcem, 19.4.2010, 0029/2010.

dve državi članici (Irska, Italija) določata dveletno obdobje za podatke o fiksni in mobilni telefoniji in eno leto za podatke o dostopu do interneta, internetni elektronski pošti in internetni telefoniji; ena država članica (Slovenija) določa 14 mesecev za podatke o telefoniji in osem mesecev za podatke, povezane z internetom; ena država članica (Slovaška) določa eno leto za fiksno in mobilno telefonijo in šest mesecev za podatke, povezane z internetom; ena država članica (Malta) določa eno leto za podatke o fiksni, mobilni in internetni telefoniji in šest mesecev za podatke o dostopu do interneta in internetni elektronski pošti. Ena država članica (Madžarska) hrani vse podatke eno leto, razen podatkov o neuspešnih klicih, ki jih hrani samo šest mesecev. Ena država članica (Belgija) ni določila nobenega obdobja hrambe za kategorije podatkov, določene v Direktivi. Podrobnosti so v Preglednici 3.

<b>Preglednica 3: Obdobja hrambe, določena v nacionalnem pravu</b>	
Belgija <sup>65</sup>	Med 1 letom in 36 meseci za „javno dostopne“ telefonske storitve. Ni določbe za podatke, povezane z internetom.
Bolgarija	1 leto. Podatki, do katerih se je dostopalo, se lahko na zahtevo hranijo še nadaljnjih 6 mesecev.
Češka	Direktiva ni prenesena.
Danska	1 leto.
Nemčija	Direktiva ni prenesena.
Estonija	1 leto.
Irska	2 leti za podatke o fiksni in mobilni telefoniji, 1 leto za podatke o dostopu do interneta, internetni elektronski pošti in internetni telefoniji.
Grčija	1 leto.
Španija	1 leto.
Francija	1 leto.
Italija	2 leti za podatke o fiksni in mobilni telefoniji, 1 leto za podatke o dostopu do interneta, internetni elektronski pošti in internetni telefoniji.
Ciper	6 mesecev.
Latvija	18 mesecev.
Litva	6 mesecev.
Luksemburg	6 mesecev.
Madžarska	6 mesecev za neuspešne klice in 1 leto za vse druge podatke.
Malta	1 leto za podatke o fiksni, mobilni in internetni telefoniji, 6 mesecev za podatke o dostopu do interneta in internetni elektronski pošti.
Nizozemska	1 leto.
Avstrija	Direktiva ni prenesena.
Poljska	2 leti.
Portugalska	1 leto.
Romunija	Direktiva ni prenesena (6 mesecev v skladu z razveljavljenim zakonom o prenosu).
Slovenija	14 mesecev za podatke o telefoniji in 8 mesecev za podatke, povezane z internetom.
Slovaška	1 leto za podatke o fiksni in mobilni telefoniji, 6 mesecev za podatke o dostopu do interneta, internetni elektronski pošti in internetni telefoniji.
Finska	1 leto.
Švedska	Direktiva ni prenesena.
Združeno kraljestvo	1 leto.

<sup>65</sup> Člen 126(2) Zakona o elektronskih komunikacijah z dne 13. junija 2005.

Direktiva dovoljuje različne pristope, iz česar sledi, da zagotavlja le omejeno pravno varnost in predvidljivost za ponudnike v EU, ki dejavnost opravljajo v več kot eni državi članici in za državljane, katerih komunikacije so lahko shranjene v različnih državah članicah. Ob upoštevanju vse večje internacionalizacije obdelave podatkov in zunanje izvajanja shranjevanja podatkov je treba proučiti možnosti za nadaljnjo uskladitev obdobja hrambe v EU. Zaradi izpolnjevanja načela sorazmernosti in ob upoštevanju kvantitativnih in kvalitativnih dokazov o vrednosti hranjenih podatkov v državah članicah ter trendov na področju komunikacij in tehnologij ter na področju kriminala in terorizma bo Komisija proučila uporabo različnih obdobja za različne kategorije podatkov, različne kategorije hudih kaznivih dejanj ali kombinacije obojega<sup>66</sup>. Kvantitativni dokazi, ki so jih doslej zagotovile države članice glede starosti hranjenih podatkov, kažejo, da je okoli 90 % podatkov starih šest mesecev ali manj, okoli 70 % jih je starih tri mesece ali manj, kadar (prvotni) zahtevki za dostop vložijo organi pregona (glej oddelek 5.2).

#### **4.6. Varovanje in varnost podatkov in nadzorni organi (člena 7 in 9)**

V skladu z Direktivo morajo države članice zagotoviti, da ponudniki spoštujejo vsaj štiri načela varstva podatkov, in sicer:

- (a) da so hranjeni podatki enake kakovosti in zanje veljajo enaka določila o varnosti in zaščiti kot za podatke na [javnem komunikacijskem] omrežju;
- (b) da se v zvezi s podatki sprejmejo primerni tehnični in organizacijski ukrepi, s katerimi se jih zaščiti pred nenamernim ali nezakonitim uničenjem, izgubo ali spremembami in nepooblaščenimi ali nezakonitimi oblikami hrambe, obdelave, dostopa ali razkrivanja;
- (c) da se v zvezi s podatki sprejmejo primerni tehnični in organizacijski ukrepi, s katerimi se zagotovi, da so dostopni samo posebej pooblaščenemu osebu in
- (d) da se ob koncu obdobja hranjenja uničijo vsi podatki, razen tistih, do katerih se je dostopalo in se jih hranilo [za namen, določen v Direktivi].

V skladu z Direktivo o varstvu podatkov in Direktivo o e-zasebnosti ponudniki ne smejo obdelovati podatkov, hranjenih v skladu z Direktivo za druge namene, če se podatki sicer ne bi hranili<sup>67</sup>. Države članice morajo določiti javni organ, ki je popolnoma samostojno odgovoren za spremljanje uporabe teh načel in je lahko isti, kot organi, ki jih zahteva Direktiva o varstvu podatkov<sup>68</sup>.

Petnajst držav članic je v ustrezno zakonodajo preneslo vsa ta načela. Štiri države članice (Belgija, Estonija, Španija, Latvija) so prenesle dve ali tri načela, vendar izrecno ne določajo uničenja podatkov ob koncu obdobja hrambe. Dve državi članici (Italija, Finska) določata uničenje podatkov. Ni jasno, kateri posebni tehnični in organizacijski varnostni ukrepi, kot sta

---

<sup>66</sup> Predlog Komisije iz leta 2005 za direktivo o hrambi podatkov je predvideval enoletno obdobje hrambe za podatke o telefoniji in šest mesecev za podatke o internetu.

<sup>67</sup> Člen 13(1) Direktive 95/46/ES.

<sup>68</sup> Člen 28 Direktive 95/46/ES.

varno preverjanje pristnosti in podrobno upravljanje dnevnika dostopa<sup>69</sup>, so bili uporabljeni. Dvaindvajset držav članic ima nadzorni organ, ki je odgovoren za spremljanje uporabe teh načel. V večini primerov je to organ za varstvo podatkov. Podrobnosti so v Preglednici 4.

<b>Preglednica 4: Varovanje in varnost podatkov in nadzorni organi</b>		
<i>Država članica</i>	<i>Določbe o varovanju in varnosti podatkov v nacionalni zakonodaji</i>	<i>Nadzorni organ</i>
Belgija	Ponudniki morajo zagotoviti, da posredovanja podatkov ne more presteči tretja oseba, ponudniki pa morajo izpolnjevati standarde Evropskega inštituta za telekomunikacijske standarde za varnost telekomunikacij in zakonito prestrezanje <sup>70</sup> . Zdi se, da načelo obveznega uničenja podatkov ob koncu obdobja hrambe ni obravnavano.	Inštitut za poštne storitve in telekomunikacije
Bolgarija	Zakon o prenosu vključuje zahtevo, da se izvajajo vsa štiri načela <sup>71</sup> .	Komisija za varstvo osebnih podatkov spremlja obdelavo in shranjevanje podatkov, da zagotovi izpolnjevanje obveznosti; parlamentarna komisija v državnem zboru spremlja postopke za odobritev in dostop do podatkov.
Češka <sup>72</sup>	Direktiva ni prenesena.	
Danska	Določena so štiri načela <sup>73</sup> .	Nacionalna agencija za IT in telekomunikacije spremlja obveznost ponudnikov elektronskih komunikacijskih omrežij in storitev za zagotovitev, da tehnična oprema in sistemi omogočajo policiji dostop do informacij o telekomunikacijskem prometu.
Nemčija	Direktiva ni prenesena.	
Estonija	Zakon o prenosu določa tri od štirih načel. Ni izrecne določbe za četrto načelo, čeprav lahko oseba, ki ji je bila zaradi dejavnosti, povezanih z nadzorom, kršena zasebnost, s sodbo sodišča zahteva uničenje podatkov <sup>74</sup> .	Odgovorni organ je Organ za tehnični nadzor.
Irska <sup>75</sup>	Zakon o prenosu vključuje zahtevo, da se izvajajo vsa štiri načela.	Pooblaščen sodnik ima pristojnost za preiskovanje in poročanje, ali pristojni nacionalni organi izpolnjujejo določbe zakona o prenosu.

<sup>69</sup> Varno preverjanje pristnosti vključuje mehanizem dvojnega preverjanja pristnosti, kot sta geslo in biometrija ali geslo in žeton, da se zagotovi fizična pristnost osebe, ki je odgovorna za obdelavo podatkov o prometu. Podrobno upravljanje dnevnika dostopa vključuje podrobno sledenje postopkov dostopa in obdelave prek hrambe dnevnika, v katerem je zabeležena identiteta uporabnika, čas dostopa in dokumenti, do katerih se je dostopalo.

<sup>70</sup> Člen 6 kraljevega odloka z dne 9. januarja 2003.

<sup>71</sup> Člen 4 (1) Zakona o elektronskih komunikacijah (spremenjen) 2010

<sup>72</sup> Oddelka 87(3) in 88 zakona št. 127/2005, kakor je bil spremenjen z zakonom št. 247/2008; oddelek 2 zakona št. 336/2005; oddelek 3(4) zakona št. 485/2005; oddelek 28(1) zakona št. 101/2000.

<sup>73</sup> Zakon o obdelavi osebnih podatkov; Odredba št. 714 z dne 26. junija 2008 o zagotavljanju elektronskih komunikacijskih omrežij in storitev.

<sup>74</sup> Pododdelek 111(9) Zakona o elektronskih komunikacijah; Pododdelek 122(2) Zakonika o kazenskem postopku.

<sup>75</sup> Oddelki 4, 11 in 12 Predloga zakona o komunikacijah (hramba podatkov) 2009.

<b>Preglednica 4: Varovanje in varnost podatkov in nadzorni organi</b>		
<i>Država članica</i>	<i>Določbe o varovanju in varnosti podatkov v nacionalni zakonodaji</i>	<i>Nadzorni organ</i>
Grčija <sup>76</sup>	Zakon o prenosu vključuje zahtevo, da se izvajajo vsa štiri načela, in nadaljnjo zahtevo, da ponudniki pripravijo in uporabljajo načrt za zagotavljanje skladnosti pod vodstvom imenovanega vodje za varstvo podatkov.	Organ za varstvo osebnih podatkov in organ za komunikacijsko zasebnost
Španija <sup>77</sup>	Določbe o varnosti podatkov zajemajo tri od štirih načel (kakovost in varnost hranjenih podatkov, dostop pooblaščenim osebam in zaščito pred nepooblaščenimi obdelavo).	Odgovorni organ je Agencija za varstvo podatkov.
Francija <sup>78</sup>	Zakon o prenosu vključuje zahtevo, da se izvajajo vsa štiri načela.	Nacionalna komisija za informacijsko tehnologijo in svobodo izvaja nadzor nad izpolnjevanjem obveznosti.
Italija	Ni izrecne določbe o varnosti hranjenih podatkov, obstaja pa splošna zahteva o uničenju ali anonimiziranju podatkov o prometu in sporazumni obdelavi podatkov o lokaciji <sup>79</sup> .	Organ za varstvo podatkov spremlja, ali ponudniki ravnajo skladno z Direktivo.
Ciper <sup>80</sup>	Zakon o prenosu določa vsa štiri načela.	Komisar za varstvo osebnih podatkov spremlja uporabo zakona o prenosu.
Latvija <sup>81</sup>	Zakon o prenosu določa dve od štirih načel: zaupnost podatkov in pooblaščen dostop do hranjenih podatkov ter uničenje podatkov ob koncu obdobja hrambe.	Državni inšpektorat za podatke nadzira varstvo osebnih podatkov v sektorju elektronskih komunikacij, ne pa tudi dostopa do podatkov in obdelave hranjenih podatkov.
Litva <sup>82</sup>	Zakon o prenosu določa vsa štiri načela.	Državni inšpektorat za varstvo podatkov nadzira izvajanje zakona o prenosu in je odgovoren za posredovanje statističnih podatkov Evropski komisiji.
Luksemburg <sup>83</sup>	Zakon o prenosu določa vsa štiri načela.	Organ za varstvo podatkov
Madžarska <sup>84</sup>	Zakon o prenosu določa vsa štiri načela.	Parlamentarni komisar za varstvo podatkov in svobodo obveščanja.
Malta <sup>85</sup>	Zakon o prenosu določa vsa štiri načela.	Komisar za varstvo podatkov

<sup>76</sup> Člen 6 zakona št. 3917/2011.

<sup>77</sup> Člen 8 zakona št. 25/2007, člen 38(3) Zakona o splošnih telekomunikacijah. Zakon (člen 9) se sklicuje na izjemo od dostopa in pravico do preklica, predpisano v sistemskem zakonu 15/1999 o varstvu osebnih podatkov (člena 22 in 23).

<sup>78</sup> Člen D.98-5, CPCE; člen L-34-1(V), CPCE; člen 34, Zakon št. 78-17; člen 34-1, CPCE; člen 11 zakona št. 78-17 z dne 6. januarja 1978.

<sup>79</sup> Člena 123 in 126 Zakonika o varstvu podatkov.

<sup>80</sup> Člena 14 in 15 zakona št. 183(I)/2007.

<sup>81</sup> Člena 4(4) in 71(6-8) Zakona o elektronskih komunikacijah.

<sup>82</sup> Členi 12(5), 66(8) in (9) Zakona o elektronskih komunikacijah, kot je bil spremenjen 14. novembra 2009.

<sup>83</sup> Člen 1(5) zakona z dne 24. julija 2010.

<sup>84</sup> Člen 157/A zakona št. C/2003, kakor je bil spremenjen z zakonom št. CLXXIV/2007; člen 2 Uredbe 226/2003; in zakon št. LXIII/1992 o varstvu podatkov.

<sup>85</sup> Člena 24 in 25 pravnega obvestila št. 198/2008; člen 40(b) Zakona o varstvu podatkov (poglavje 440).

Preglednica 4: Varovanje in varnost podatkov in nadzorni organi		
Država članica	Določbe o varovanju in varnosti podatkov v nacionalni zakonodaji	Nadzorni organ
Nizozemska <sup>86</sup>	Zakon o prenosu določa vsa štiri načela.	Agencija za radijske zveze nadzira obveznosti ponudnikov dostopa do interneta in telekomunikacij; organ za varstvo podatkov nadzira splošno obdelavo osebnih podatkov; protokol podrobno določa sodelovanje med obema organoma.
Avstrija	Direktiva ni prenesena.	
Poljska	Zakon o prenosu določa vsa štiri načela <sup>87</sup> .	Organ za varstvo podatkov
Portugalska	Zakon o prenosu določa vsa štiri načela <sup>88</sup> .	Portugalski organ za varstvo podatkov
Romunija	Direktiva ni prenesena.	
Slovenija <sup>89</sup>	Zakon o prenosu določa vsa štiri načela.	Informacijski pooblaščenec
Slovaška <sup>90</sup>	Zakon o prenosu določa vsa štiri načela.	Varstvo osebnih podatkov nadzira nacionalni organ, ki izdaja predpise in agencija za določanje cen elektronskih komunikacij.
Finska	Zakon o prenosu izrecno predvideva le zahtevo, da se podatki ob koncu obdobja hrambe uničijo <sup>91</sup> .	Finski regulativni organ za komunikacije nadzira, ali ponudniki ravnajo skladno s predpisi o hrambi podatkov. Pooblaščenec za varstvo osebnih podatkov nadzira splošno zakonitost obdelave osebnih podatkov.
Švedska	Direktiva ni prenesena.	
Združeno kraljestvo	Zakon o prenosu določa vsa štiri načela <sup>92</sup> .	Informacijski pooblaščenec nadzira hrambo in/ali obdelavo podatkov o komunikaciji (in drugih osebnih podatkov) ter ustrezen nadzor varstva podatkov. Pooblaščenec za preprečevanje (vršilec dolžnosti ali upokojeni višji sodnik) nadzoruje pridobivanje podatkov o komunikaciji v skladu z RIPA s strani javnih organov. Sodišče s preiskovalnimi pooblastili preiskuje pritožbe zaradi zlorabe podatkov, če so pridobljeni v skladu z zakonodajo za prenos (RIPA).

Prenos člena 7 je neskladen. Hranjeni podatki so lahko zelo osebni in občutljivi in v celem procesu je pri shranjevanju, pridobivanju in uporabi podatkov treba dosledno in vidno uporabljati visoke standarde varstva podatkov, da se zmanjša nevarnost kršitev zasebnosti in ohranja zaupanje državljanov. Komisija bo preučila možnosti za krepitev standardov varnosti in varstva podatkov, vključno z uvedbo rešitev vgrajene zasebnosti, da se zagotovi izpolnjevanje teh standardov kot del shranjevanja in posredovanja. Upoštevala bo tudi priporočila poročila o drugem skupnem izvršilnem ukrepu Delovne skupine za varstvo podatkov iz člena 29 za minimalne zaščitne ukrepe in za tehnične in organizacijske varnostne ukrepe<sup>93</sup>.

<sup>86</sup> Člen 13(5) Zakona o telekomunikacijah; dolgi naslov protokola sodelovanja je *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*.

<sup>87</sup> Člena 180a in 180e Zakona o telekomunikacijah.

<sup>88</sup> Člen 7(1) in (5) in člen 11 zakona št. 32/2008; člena 53 in 54 Zakona o varstvu osebnih podatkov.

<sup>89</sup> Člen 107a(6) in člen 107c Zakona o elektronskih komunikacijah.

<sup>90</sup> Člen 59a Zakona o elektronskih komunikacijah; člen S33 zakona št. 428/2002 o varstvu osebnih podatkov.

<sup>91</sup> Člen 16(3) Zakona o elektronskih komunikacijah.

<sup>92</sup> Člen 6 Uredbe o hrambi podatkov.

<sup>93</sup> Mnenje Delovne skupine za varstvo podatkov iz člena 29 3/2006 (WP119); Poročilo 01/2010.

#### 4.7. Statistika (člen 10)

Države članice zagotovijo, da vsako leto posredujejo Komisiji statistične podatke o hrambi podatkov, ki vključuje:

- zadeve, v katerih so bile informacije zagotovljene pristojnim organom v skladu z veljavno nacionalno zakonodajo;
- čas med dnevom, ko so bili podatki shranjeni, in dnevom, ko je pristojni organ zahteval prenos podatkov (t.j. starost podatkov) in
- zadeve, v katerih zahtev za podatke ni bilo mogoče izpolniti.

Pri zahtevanju statistike na podlagi te določbe je Komisija države članice prosila, naj posredujejo podrobnosti o posameznih „zahtevkih“ za podatke. Kljub temu so bili obseg in podrobnosti posredovanih statističnih podatkov različni: nekatere države članice so v svojih odgovorih razlikovale različne vrste komunikacij, nekatere so navedle starost podatkov v času zahtevka, druge pa so posredovale samo letno statistiko brez podrobne razčlenitve. Devetnajst držav članic<sup>94</sup> je posredovalo statistiko o številu zahtevkov za podatke za leto 2009 in/ali leto 2008; med njimi so bile Irska, Grčija in Avstrija, v katerih se podatki zahtevajo kljub temu, da ni zakonodaje za prenos, ter Češka in Nemčija, v kateri je bil zakon o hrambi podatkov razveljavljen. Sedem držav članic, ki so prenesle Direktivo, ni posredovalo statistike, čeprav je Belgija poslala oceno obsega letnih zahtevkov za podatke o telefoniji (300 000).

Zanesljivi kvantitativni in kvalitativni podatki so odločilnega pomena pri dokazovanju nujnosti in vrednosti varnostnih ukrepov, kot je hramba podatkov. To je bilo priznано v akcijskem načrtu za leto 2006 za oceno kriminala in kazenskega pravosodja<sup>95</sup>, ki je vključeval cilj za razvoj metod za redno zbiranje podatkov v skladu z Direktivo in za vključitev statistike v podatkovno zbirko Eurostata (če izpolnjujejo standarde kakovosti). Tega cilja ni bilo mogoče doseči, ker je večina držav članic Direktivo v celoti prenesla šele v zadnjih dveh letih, za vir statistike pa so uporabljale različne razlage. Komisija bo v svojem prihodnjem predlogu o reviziji okvira hrambe podatkov skupaj s pregledom akcijskega načrta za statistiko poskušala razviti izvedljive postopke meritev in poročanja, ki bodo omogočili pregledno in smiselno spremljanje hrambe podatkov, ki ne bo prekomerno obremenilo kazenskega pravosodja in organov pregona.

#### 4.8. Prenos v državah EGP

Zakonodaja o hrambi podatkov je bila sprejeta na Islandiji, v Lihtenštajnu in na Norveškem<sup>96</sup>.

---

<sup>94</sup> Češka, Danska, Nemčija, Estonija, Irska, Grčija, Španija, Francija, Ciper, Latvija, Litva, Malta, Nizozemska, Avstrija, Poljska, Slovenija, Slovaška, Finska in Združeno kraljestvo.

<sup>95</sup> Sporočilo Komisije (2006) 437 z naslovom „Razvoj skladne in celovite strategije EU za merjenje kriminala in kazenskega pravosodja: Akcijski načrt EU 2006–2010“.

<sup>96</sup> Zakon o prenosu na Islandiji je Zakon o telekomunikacijah 81/2003 (kakor je bil spremenjen aprila 2005); v Lihtenštajnu je Zakon o telekomunikacijah iz leta 2006. Na Norveškem je bila zakonodaja o prenosu potrjena 5. aprila 2011, zakon pa trenutno čaka na kraljevo potrditev.

#### 4.9. Odločbe ustavnih sodišč o zakonih o prenosu

Romunsko ustavno sodišče, nemško zvezno ustavno sodišče in češko ustavno sodišče so oktobra 2009, marca 2010 oziroma marca 2011 razveljavili zakone o prenosu Direktive v njihove sodne pristojnosti, ker so menili, da so neustavni. Romunsko sodišče<sup>97</sup> se je strinjalo, da se poseg v temeljnje pravice lahko dovoli, če se pri tem spoštuje nekatera pravila ter zagotovi ustrezne in zadostne zaščitne ukrepe za varstvo pred možnim samovoljnim državnim poseganjem. Vendar je Sodišče na podlagi sodne prakse Evropskega sodišča za človekove pravice<sup>98</sup> ugotovilo, da je zakon o prenosu dvoumen glede področja uporabe in namena in ne zagotavlja zadostnih zaščitnih ukrepov. Zato je odločilo, da je „neprestana pravna obveznost“ vse podatke o prometu hraniti šest mesecev nezdržljiva s pravicama do zasebnosti in svobode izražanja iz člena 8 Evropske konvencije o človekovih pravicah.

Nemško ustavno sodišče<sup>99</sup> je povedalo tudi, da je hramba podatkov ustvarila pojmovanje nadzora, ki bi lahko škodovalo svobodnemu uresničevanju temeljnih pravic. Izrecno je priznalo, da hramba podatkov za strogo omejene uporabe z dovolj visoko stopnjo varnosti podatkov ne bi nujno kršila nemške ustave. Vendar je Sodišče poudarilo, da je hramba takih podatkov velika omejitev pravice do zasebnosti in bi zato morala biti dopustna samo v posebej omejenih okoliščinah ter da je šestmesečno obdobje hrambe zgornja omejitev („*an der Obergrenze*“), ki se lahko šteje za sorazmerno (točka 215). Podatki se lahko zahtevajo le, kadar že obstaja sum hudega kaznivega dejanja ali dokaz nevarnosti za javno varnost. Pridobivanje podatkov bi moralo biti prepovedano za nekatere privilegirane komunikacije (t.j. komunikacije, povezane s čustveno ali socialno potrebo), ki se zanašajo na zaupnost. Podatki bi morali biti tudi kodirani s preglednim nadzorom uporabe podatkov.

Češko ustavno sodišče<sup>100</sup> je zakonodajo za prenos razveljavilo na podlagi ugotovitve, da kot ukrep, ki posega v temeljne pravice, zakonodaja za prenos ni dovolj natančno in jasno oblikovana. Sodišče je v kritiki izrazilo, da omejitev namena ni dovolj ozka glede na težo in obseg zahteve o hrambi podatkov. Trdilo je, da opredelitev organov, pristojnih za dostopanje do hranjenih podatkov in za njihovo obdelavo, ter postopkov za tovrsten dostop in obdelavo v zakonodaji za prenos ni dovolj jasna, da bi se zagotovili celovitost in zaupnost podatkov. Posamezen državljani zato ni imel zadostnih jamstev in zaščitnih ukrepov za preprečitev morebitnih zlorab moči javnih organov. Sodišče ni kritiziralo Direktive same in je navedlo, da je Češki pustilo dovolj prostora za njen prenos v skladu z ustavo. Vendar je Sodišče v obliki *obiter dictum* izrazilo dvom glede nujnosti, učinkovitosti in ustreznosti hrambe podatkov o prometu ob upoštevanju pojava novih metod kriminala, na primer prek uporabe anonimnih kartic SIM.

Te tri države članice zdaj proučujejo načine za ponoven prenos Direktive. Zadeve v zvezi s hrambo podatkov so bile predložene tudi ustavnim sodiščem Bolgarije, kar je povzročilo revizijo zakona o prenosu, Cipra, kjer je bilo odločeno, da so odločbe sodišča, izdane v skladu

---

<sup>97</sup> Odločba romunskega ustavnega sodišča št. 1258 z dne 8. oktobra 2009.

<sup>98</sup> ESČP, Rotaru proti Romuniji 2000, Sunday Times proti Združenemu kraljestvu 1979 in lihtenštajnski princ Hans-Adam proti Romuniji 2001.

<sup>99</sup> Bundesverfassungsgericht, 1 BvR 256/08, točke 1–345.

<sup>100</sup> Sodba češkega ustavnega sodišča z dne 22. marca o zakonu št. 127/2005 in Uredba št. 485/2005; glej zlasti točke 45–48, 50–51 in 56.

z zakonom o prenosu, neustavne, in Madžarske, kjer zadeva v zvezi s tem, da v zakonu o prenosu niso navedeni pravni nameni obdelave podatkov, še ni rešena<sup>101</sup>.

Komisija bo v svojem prihodnjem predlogu o reviziji okvira hrambe podatkov proučila vprašanja, ki jih je sprožila nacionalna sodna praksa.

#### **4.10. Izvrševanje Direktive**

Komisija od držav članic, ki še niso v celoti prenesle Direktive, ali ki še niso sprejele zakonodaje, ki nadomešča zakonodajo o prenosu, ki so jo razveljavila nacionalna sodišča, pričakuje, da to storijo čim je mogoče. V nasprotnem primeru si Komisija pridržuje pravico do izvršitve svojih pooblastil po Pogodbah EU. Do zdaj je Sodišče za dve državi članici, ki nista prenesli Direktive (Avstrija in Švedska), ugotovilo, da sta kršili svoje obveznosti na podlagi prava EU<sup>102</sup>. Komisija je aprila 2011 sklenila, da Švedsko še drugič napoti na Sodišče zaradi neizpolnjevanja sodbe v zadevi C-185/09, ter po sklepu švedskega parlamenta, da odloži sprejetje zakonodaje za prenos za 12 mesecev, zahtevala, da se ji naloži denarna kazen v skladu s členom 260 Pogodbe o delovanju Evropske unije. Komisija še naprej pozorno spremlja položaj v Avstriji. Slednja je predložila časovni načrt takojšnjega sprejetja zakonodaje za prenos.

### **5. VLOGA HRANJENIH PODATKOV V KAZENSKEM PRAVOSODJU IN KAZENSKEM PREGONU**

Ta oddelek povzema funkcije hranjenih podatkov, kakor jih opisujejo države članice v svojih prispevkih k oceni.

#### **5.1. Obseg hranjenih podatkov, do katerih dostopajo pristojni nacionalni organi**

Povečuje se obseg telekomunikacijskega prometa in zahtevkov za dostop do podatkov o prometu. Statistični podatki, ki jih je za leto 2008 in/ali 2009 posredovalo devetnajst držav članic kaže, da je bilo v EU skupaj vsako leto vloženi več kot dva milijona zahtevkov za dostop in da so med državami članicami znatne razlike – od manj kot sto na leto (Ciper) do več kot 1 milijon (Poljska). Glede na podatke o vrsti zahtevanih podatkov, ki jih je za leto 2008 oziroma leto 2009 predložilo dvanajst držav članic, so se najpogosteje zahtevane vrste podatkov nanašale na mobilno telefonijo (glej preglednice 5, 8 in 12). Statistični podatki ne navajajo natančnega namena vložitve zahtevkov. Češka, Latvija in Poljska so navedle, da so pri podatkih o mobilni telefoniji pristojni organi morali isti zahtevek posredovati vsakemu od glavnih operaterjev mobilne telefonije in je zato dejansko število zahtevkov na zadevo znatno manjše, kot navaja statistika.

Nobenega očitnega pojasnila ni za te razlike, čeprav med pomembne dejavnike spadajo številčnost prebivalstva, prevladujoči trendi kriminala, omejitve namena in pogoji za dostop ter stroški pridobivanja podatkov.

---

<sup>101</sup> Bolgarsko vrhovno upravno sodišče, odločba št. 13627, 11. december 2008; pritožbeni primer ciprskega vrhovnega sodišča št. 65/2009, 78/2009, 82/2009 in 15/2010-22/2010, 1. februar 2011; madžarska Zveza za državljanske svoboščine je 2. junija 2008 vložila madžarsko ustavno pritožbo.

<sup>102</sup> Zadeva C-189/09 oziroma zadeva C-185/09.

## 5.2. Starost hranjenih podatkov, do katerih se je dostopalo

Na podlagi statistične razčlenitve, ki jo je za leto 2008 predložilo devet držav članic<sup>103</sup> (glej povzetek v Preglednici 5 in nadaljnje podrobnosti v Prilogi), je bilo ob vložitvi (prvotnega) zahtevka za dostop okoli 90 % podatkov, do katerih so dostopali pristojni organi v navedenem letu, starih šest mesecev ali manj, okoli 70 % pa tri mesece ali manj.

<b>Preglednica 5: Pregled starosti hranjenih podatkov, do katerih se je dostopalo v devetih državah članicah, ki so predložile razčlenitev po vrsti podatkov v letu 2008</b>				
<i>Starost</i>	<i>Fiksna telefonija</i>	<i>Mobilna telefonija</i>	<i>Podatki o internetu</i>	<i>Skupaj</i>
Do 3 mesece	61 %	70 %	56 %	67 %
3–6 mesecev	28 %	18 %	19 %	19 %
6–12 mesecev	8 %	11 %	18 %	12 %
Več kot 1 leto	3 %	1 %	7 %	2 %

Po navedbah držav članic je uporaba hranjenih podatkov, starejših od treh in celo šestih mesecev, manj pogosta, vendar je lahko odločilna; njena uporaba se deli na tri kategorije. Prvič, podatki, povezani z internetom, se v kazenskih preiskavah pogosto zahtevajo pozneje kot druge vrste dokazov. Analiza podatkov o fiksnem omrežju in mobilni telefoniji pogosto ustvari nove možne sledi, kar povzroči nadaljnje zahtevke za starejše podatke. Če se na primer med preiskavo ugotovi ime na podlagi podatkov o fiksnem omrežju ali mobilni telefoniji, preiskovalci morda želijo določiti naslov internetnega protokola (IP), ki ga je ta oseba uporabljala ali morda želijo ugotoviti, s katerimi osebami je bila ta oseba v danem obdobju prek tega naslova IP v stiku. V takem scenariju je verjetno, da preiskovalci zahtevajo podatke, ki omogočajo tudi sledenje komunikaciji z drugimi naslovi IP, in identiteto oseb, ki so uporabljale te naslove IP.

Drugič, preiskovanje posebej hudega kaznivega dejanja, vrste kaznivih dejanj, organiziranega kriminala in terorističnih dogodkov se običajno opira na starejše hranjene podatke, ki odražajo dolžino časa, potrebnega za načrtovanje takih dejanj, da se ugotovijo vzorci kaznivih ravnanj ter odnosi med sokrivci in da se ugotovi naklep. Dejavnosti, povezane z zapletenimi finančnimi kaznivimi dejanji, se pogosto odkrijejo šele po več mesecih. Tretjič in izjemoma, so države članice zahtevale podatke o prometu iz druge države članice, ki običajno te podatke lahko izroči samo na podlagi sodnega pooblastila kot odgovor na zaprosilo za pravno pomoč, ki ga izda sodnik v državi članici, ki je poslala zaprosilo. Tovrstna medsebojna pravna pomoči je lahko dolgotrajen proces in zato so bili v teh primerih nekateri od zahtevanih podatkov stari več kot šest mesecev.

## 5.3. Čezmejni zahtevki za hranjene podatke

Kazenske preiskave in kazenski pregon lahko vključujejo dokaze ali priče ali dogodke, ki so se zgodili v več kot eni državi članici. Glede na statistične podatke, ki so jih predložile države članice, je manj kot 1 % vseh zahtevkov za hranjene podatke zadeval podatke iz druge države članice. Organi pregona so navedli, da raje zahtevajo podatke od domačih ponudnikov, ki imajo morda shranjene relevantne podatke, kot da bi začeli postopek medsebojne pravne

<sup>103</sup> Češka, Danska, Estonija, Irska, Španija, Ciper, Latvija, Malta in Združeno kraljestvo.

pomoči, ki je lahko zelo dolgotrajen, ni pa nobenega zagotovila, da bo dostop do podatkov odobren. Okvirni sklep Sveta 2006/960/PNZ o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic<sup>104</sup>, ki določa roke za predložitev informacij po prejemu zahtevka iz druge države članice, se ne uporablja, ker se šteje, da so hranjeni podatki informacije, ki se pridobijo s prisilnimi ukrepi, kar je zunaj področja uporabe instrumenta. Kljub temu nobena država članica ali organ pregona ni pozval, naj se taka čezmejna izmenjava bolj olajša.

#### 5.4. Vrednost hranjenih podatkov v kazenskih preiskavah in kazenskem pregonu

Absolutna številka v poročilu o zahtevkih za podatke ne odraža nujno vrednosti podatkov v posameznih kazenskih preiskavah in države članice so na splošno poročale, da je hramba podatkov vsaj dragocena, v nekaterih zadevah pa nepogrešljiva<sup>105</sup> za preprečevanje kriminala in boj proti njemu, vključno z varstvom žrtev in oprostivijo nedolžnih v kazenskih postopkih. Uspešne obsodbe se opirajo na priznanje krivde, izjave prič ali forenzične dokaze. Po poročilih se je izkazalo, da so hranjeni podatki o prometu potrebni pri navezovanju stikov s pričami dogodkov, ki jih sicer ne bi bilo mogoče identificirati, in pri zagotavljanju dokazov o sotorilstvu pri kršitvi ali sledi pri ugotavljanju takega sotorilstva. Nekatere države članice<sup>106</sup> so trdile tudi, da jim je uporaba hranjenih podatkov pomagala pri oprostitvi oseb, ki so bile osumljene kaznivih dejanj, ne da bi jim bilo treba uporabljati druge metode nadzora, kot so prestrezanje podatkov in hišne preiskave, ki se lahko štejejo za bolj vsiljive.

V EU ni splošne opredelitve „hudega kaznivega dejanja“ in skladno s tem ni statistike EU o pogostosti hudih kaznivih dejanj ali kazenskih preiskav ali pregonih hudih kaznivih dejanj, čeprav se podatki o kaznivih dejanjih in kazenskem pravosodju redno objavljajo. Skupni obseg zahtevkov za hranjene podatke, o katerem je poročalo 19 držav članic, ki so predložile neke vrste podatkov za leti 2009 in/ali 2008, je bil okrog 2,6 milijona. V primerjavi z najnovejšo statistiko o kaznivih dejanjih in kazenskem pravosodju, ki je na voljo za teh 19 držav članic in se nanaša na vsa sporočena kazniva dejanja in ne samo na huda, bi to pomenilo nekaj več kot dva zahtevka na policista na leto ali približno enajst zahtevkov na 100 evidentiranih kaznivih dejanj<sup>107</sup>.

Na podlagi predložene statistike in ponazoritvenih primerov, ki povezujejo uporabo hranjenih podatkov o pretekli komunikaciji s številom obsodb, oprostitev, prekinjenih zadev in preprečenih kaznivih dejanj, je mogoče sklepati o vlogi in vrednosti hranjenih podatkov za kazenske preiskave.

---

<sup>104</sup> Okvirni sklep Sveta 2006/960/PNZ z dne 18. decembra 2006 o poenostavitvi izmenjave informacij in obveščevalnih podatkov med organi kazenskega pregona držav članic Evropske unije, UL L 386, 29.12.2006, str. 89–100 in UL L 200, 1.8.2007, str. 637–648.

<sup>105</sup> Češka je menila, da je hramba podatkov „v celoti nepogrešljiva v velikem številu primerov“; Madžarska je trdila, da je „nepogrešljiva v rednih dejavnostih [organov pregona]“; Slovenija je navedla, da bi odsotnost hranjenih podatkov „paralizirala delovanje organov pregona“; ena od policijskih izpostav v Združenem kraljestvu je opisala razpoložljivost podatkov o prometu kot „resnično bistvenega pomena ... pri preiskovanju nevarnosti terorizma in hudih kaznivih dejanj“.

<sup>106</sup> Nemčija, Poljska, Slovenija, Združeno kraljestvo.

<sup>107</sup> V letu 2007 je bilo v EU-27 1,7 milijona policistov, od tega jih je bilo 1,2 milijona v 19 državah članicah, ki so predložile statistične podatke o zahtevkih za hranjene podatke; v letu 2007 je policija v EU evidentirala 29,2 milijona kaznivih dejanj, od tega je bilo 24 milijonov evidentiranih v 19 državah članicah, ki so predložile statistične podatke. (Vir: Eurostat 2009).

## *Izdelava dokaznih sledi*

Prvič, hranjeni podatki omogočajo izdelavo sledi dokazov, ki vodijo k prekršku. Uporabljajo se za zaznavanje ali potrjevanje drugih oblik dokazov, dejavnosti in povezav med osumljenci. Organi pregona in obtoženci so uporabljali zlasti podatke o lokaciji za izključevanje osumljencev iz kraja storitve kaznivega dejanja ali preverjanje alibijev. Ta dokaz torej lahko ljudi izloči iz kazenskih preiskav, tako da ni treba uporabljati bolj vsiljivih preiskav, ali pa vodi k oprostivni pri sojenju. Belgija je navedla, da so bili leta 2008 obsojeni storilci ugrabitve zaposlenega na kazenskem sodišču v Antwerpnu, pri čemer so bili podatki o lokaciji, ki so povezovali njihove dejavnosti v treh različnih mestih, odločilni pri prepričevanju porote, da so sotorilci. V zadevi umora, povezanega z motoristično bando v letu 2007, so podatki o lokaciji mobilnih telefonov storilcev kaznivega dejanja dokazali, da so bili na tem območju, ko se je zgodil umor, kar je privedlo do delnega priznanja<sup>108</sup>. Po navedbah Belgije, Irske in Združenega kraljestva je mogoče nekatera kazniva dejanja, ki vključujejo komunikacijo prek interneta, preiskovati *samo* s pomočjo hranjenih podatkov: na primer grožnje z nasiljem, izražene v klepetalnicah, pogosto ne pustijo nobenih sledi razen podatkov o prometu v kibernetskem prostoru. Podobno velja za kazniva dejanja, storjena prek telefona. Madžarska in Poljska sta navedli primere goljufije zoper starejše osebe konec leta 2009 in v začetku leta 2010, storjene s pomočjo telefonskih klicev, v katerih so se storilci pretvarjali, da so družinski člani, ki potrebujejo posojilo. Odkriti jih je bilo mogoče samo prek hranjenih podatkov o telefoniji.

## *Sprožitev kazenskih preiskav*

Drugič, obstajajo primeri, v katerih ni bilo forenzičnih dokazov ali dokazov očitidcev, tako je bil edini način za začetek kazenske preiskave pregled hranjenih podatkov. Nemčija je navedla primer umora policista, po katerem je napadalec pobegnil z žrtvinim vozilom, ki ga je pozneje zapustil. Ugotoviti je bilo mogoče, da je potem po telefonu organiziral drugo prevozno sredstvo. Nobenih forenzičnih dokazov ali očitidcev ni bilo, ki bi lahko identificirali morilca, in organi so bili odvisni od razpoložljivosti podatkov o prometu, da so lahko nadaljevali preiskavo. V primerih spolne zlorabe otrok prek interneta je hramba podatkov nujna za uspešno preiskovanje. Skupaj z drugimi preiskovalnimi tehnikami hranjeni podatki omogočajo identifikacijo porabnikov vsebin o zlorabi otrok<sup>109</sup> in podpirajo identifikacijo in reševanje otrok žrtev. Češka je poročala, da bi bilo brez hranjenih podatkov, povezanih z internetom, nemogoče začeti preiskavo, omrežja uporabnikov in oseb, ki razširjajo otroško pornografijo, ki je bila del „operacije Vilma“. Na ravni EU je učinkovitost operacije Rešitev (ki jo omogoča Europol) pri varovanju otrok pred zlorabo ovirana, ker zakonodaja o hrambi ni bila prenesena in zato nekatere države članice niso mogle preveriti članov obsežne mednarodne pedofilske mreže z uporabo naslov IP, ki so lahko stari do enega leta.

V preiskovanju kibernetske kriminalitete je naslov IP pogosto prva sled. Organi pregona prek pridobitve podatkov o prometu lahko določijo naročnika, ki ima naslov IP, preden določijo,

---

<sup>108</sup> Nacionalna agencija za izboljšanje policijske dejavnosti (Združeno kraljestvo), *The Journal of Homicide and Major Incident Investigation*, zvezek 5, številka 1, pomlad 2009, str. 39–51.

<sup>109</sup> Projekt z naslovom „Merjenje in analiza dejavnosti vsak z vsakim zoper pedofilske vsebine“, ki ga podpira program za varnejši internet, je zagotovil točne informacije o pedofilski dejavnosti v sistemu vsak z vsakim eDonkey in omogočil identifikacijo 178 000 uporabnikov (od pregledanih 89 milijonov uporabnikov), ki so zahtevali pedofilsko vsebino.

ali se lahko uvede kazenska preiskava. Lahko tudi omogoča policiji, da vnaprej opozori potencialne žrtve na kibernetiske napade: kadar policiji uspe zaseči strežnik za upravljanje in nadzor, ki ga uporabljajo upravljavci botnetov, lahko vidi samo naslove IP, povezane na ta strežnik; prek dostopa do hranjenih podatkov pa policija lahko določi in opozori potencialne žrtve, ki imajo te naslove IP.

#### *Hranjeni podatki kot sestavni del kazenske preiskave*

Tretjič, medtem ko organi pregona in sodišča v večini držav članic ne hranijo statističnih podatkov o tem, katera vrsta dokazov je bila odločilna za obsodbe ali oprostitev, so hranjeni podatki sestavni del kazenskih preiskav in pregona v EU. Nekatere države članice so rekle, da niso vedno mogle izločiti učinka hranjenih podatkov na uspeh kazenskih preiskav in pregona, ker sodišča obravnavajo vse dokaze, ki so jim predloženi, in redko je odločilen en sam dokaz<sup>110</sup>. Nizozemska je poročala, da so bili od januarja do julija 2010 podatki o preteklem prometu odločilni dejavnik v 24 sodbah sodišč. Finska je poročala, da so bili v 56 % od 3405 zahtevkov hranjeni podatki bodisi „pomembni“ bodisi „bistveni“ za odkritje in/ali pregon kazenskih zadev. Združeno kraljestvo je posredovalo podatke, s katerimi so skušali količinsko opredeliti učinek hrambe podatkov na kazenske pregone; poročali so, da trije od njihovih organov pregona hranjene podatke uporabljajo v večini, če ne celo v vseh preiskavah, ki vodijo h kazenskemu pregonu ali obsodbi.

### **5.5. Tehnološki razvoj in uporaba predplačniških kartic SIM**

Organi pregona morajo slediti tehnološkemu razvoju, ki se uporablja za storitve ali podpiranje kaznivih dejanj. Hramba podatkov je med orodji kazenskih preiskav, s katerimi morajo biti opremljeni organi pregona za obvladljivo in stroškovno učinkovito soočanje s sodobnimi izzivi kriminala glede raznolikosti, obsega in hitrosti. Številne vse bolj pogoste oblike komunikacije so zunaj področja uporabe Direktive. Virtualna zasebna omrežja (VPN), na primer na univerzah ali v velikih gospodarskih družbah omogočajo več uporabnikom dostop do interneta prek enega samega prehoda in z uporabo istega naslova IP. Vendar se trenutno uvaja nova tehnologija, ki bo omogočala dodelitev naslovov posameznim uporabnikom VPN.

Delež uporabnikov mobilne telefonije, ki uporabljajo predplačniške storitve, je v EU različen. Nekatere države članice so trdile, da bi tudi udeleženci v kriminalni dejavnosti lahko uporabljali anonimne predplačniške kartice SIM, zlasti kupljene v drugi državi članici, kot način preprečevanja identifikacije v kazenski preiskavi<sup>111</sup>. Šest držav članic (Danska, Španija, Italija, Grčija, Slovaška in Bolgarija) je sprejelo ukrepe, ki zahtevajo registracijo predplačniških kartic SIM. Te in druge države članice (Poljska, Ciper, Litva) zagovarjajo ukrep v vsej EU, ki bi zahteval obvezno registracijo identitete uporabnikov predplačniških storitev. Dokazila o učinkovitosti teh nacionalnih ukrepov niso bila zagotovljena. Poudarjene so bile možne omejitve, na primer v primeru kraje identitete ali kadar kartico SIM kupi tretja oseba ali uporabnik gostuje s kartico, kupljeno v tretji državi. Na splošno Komisija ni prepričana, da je v tej fazi na tem področju treba ukrepati na ravni EU.

---

<sup>110</sup> Belgija, Češka in Litva.

<sup>111</sup> Sklepi Sveta o boju proti kaznivi zlorabi in anonimni uporabi elektronskih komunikacij.

## 6. UČINEK HRAMBE PODATKOV NA PONUDNIKE IN POTROŠNIKE

### 6.1. Ponudniki in potrošniki

Pet velikih panožnih združenj je v skupni izjavi Komisiji navedlo, da je gospodarski vpliv Direktive „znaten“ ali „ogromen“ „za manjše ponudnike storitev“, ker Direktiva dopušča „veliko maneverskega prostora“<sup>112</sup>. Osem ponudnikov je predložilo zelo različne ocene stroškov v smislu odhodkov iz poslovanja in investicijskih izdatkov zaradi skladnosti z Direktivo. Te trditve lahko izhajajo iz navedb ravni povračila stroškov ponudnikov, kot so jih sporočile štiri države članice (glej Preglednico 6).

Po ocenah študije, ki je bila izvedena pred prenosom Direktive v večini držav članic, so stroški vzpostavitve sistema za hrambo podatkov za ponudnika internetnih storitev, ki ima približno pol milijona strank, v prvem letu približno 375 240 EUR, nato so operativni stroški 9 870 EUR na mesec<sup>113</sup>, stroški vzpostavitve sistema za pridobivanje podatkov so bili ocenjeni na 131 190 EUR, operativni stroški pa na 28 960 EUR na mesec. Vendar je nemško ustavno sodišče v svoji sodbi z dne 2. marca 2010 ugotovilo, da uvedba obveznosti shranjevanja „ni posebej prekomerno obremenjujoča za prizadete ponudnike storitev [niti ni] nesorazmerna glede na finančno breme, ki ga imajo podjetja zaradi obveznosti shranjevanja“<sup>114</sup>. Stroški hrambe podatkov na enoto so obratno sorazmerni z velikostjo ponudnika in stopnjo standardizacije, ki jo je država članica sprejela za interakcijo s ponudniki<sup>115</sup>.

Večina ponudnikov v odgovoru na vprašalnik Komisije ni mogla količinsko opredeliti učinka Direktive na konkurenco, maloprodajne cene za potrošnike ali na naložbe v novo infrastrukturo in storitve.

Nobenega dokaza ni o količinsko opredeljivem ali znatnem vplivu Direktive na maloprodajne cene elektronskih komunikacijskih storitev; v letu 2009 predstavniki potrošnikov niso imeli nobenih prispevkov za javno posvetovanje. Raziskava, ki je bila opravljena v Nemčiji v imenu organizacije civilne družbe, je pokazala, da nameravajo potrošniki v nekaterih okoliščinah spremeniti svoje komunikacijsko vedenje in se izogibati storitvam elektronske komunikacije, vendar ni utemeljenih dokazov, da je v zadevni državi članici ali v EU na splošno prišlo do take spremembe vedenja<sup>116</sup>.

Komisija namerava oceniti učinek prihodnjih sprememb Direktive na gospodarsko panogo in potrošnike, po možnosti tudi s posebno raziskavo Eurobarometra, da se izmeri javno razumevanje.

---

<sup>112</sup> [http://www.gsmeurope.org/documents/Joint\\_Industry\\_Statement\\_on\\_DRD.PDF](http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF).

<sup>113</sup> Wilfried Gansterer & Michael Iger, *Data Retention – The EU Directive 2006/24/EC from a Technological Perspective* (Hranjenje podatkov – Direktiva EU 2006/24/ES iz tehnološke perspektive), Dunaj: Verlag Medien und Recht, 2008.

<sup>114</sup> Bundesverfassungsgericht, 1 BvR 256/08 z dne 2. marca 2010, točka 299.

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

<sup>116</sup> Raziskavo je po naročilu AK Vorratsdatenspeicherung opravila Forsa [http://www.vorratsdatenspeicherung.de/images/forsa\\_2008-06-03.pdf](http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf).

## 6.2. Povračilo stroškov

Direktiva ne ureja povračila stroškov, ki jih imajo ponudniki zaradi zahteve po hrambi podatkov. Te stroške je mogoče razumeti kot:

- (a) *odhodke iz poslovanja*, to je operativne stroške ali redne stroške, povezane z delovanjem podjetja, naprave, komponente, dela opreme ali naprave in
- (b) *investicijske izdatke*, to je odhodke za ustvarjanje prihodnjih koristi ali stroške razvoja ali zagotavljanja nepotrošnih delov za izdelek ali sistem, ki lahko vključujejo stroške delavcev ter stroške za objekte in naprave kot so najemnina in komunalne storitve.

Vse države članice zagotavljajo neko obliko povračila, če se podatki zahtevajo v okviru kazenskega postopka na sodišču. Štiri države članice so sporočile, da povrnejo odhodke iz poslovanja in investicijske izdatke. Šest držav povrne samo odhodke iz poslovanja. Komisiji niso bili priglašeni nobeni drugi sistemi povračil. Podrobnosti so v Preglednici 6.

<b>Preglednica 6: Države članice, ki povrnejo stroške</b>			
<b>Država članica</b>	<b>Odhodki iz poslovanja</b>	<b>Investicijski izdatki</b>	<b>Letno povračilo stroškov (v milijonih EUR)</b>
Belgija	da	ne	22 (2008)
Bolgarija	ne	ne	-
Češka	Direktiva ni prenesena <sup>117</sup> .		
Danska	da	ne	-
Nemčija	Direktiva ni prenesena.		
Estonija	da	ne	-
Irska	ne	ne	-
Grčija	ne	ne	-
Španija	ne	ne	-
Francija	da	ne	-
Italija	-	-	-
Ciper	ne	ne	-
Latvija	ne	ne	-
Litva	Da, če se zahteva in je utemeljeno.	ne	-
Luksemburg	ne	ne	-
Madžarska	ne	ne	-
Malta	ne	ne	-
Nizozemska	da	ne	-
Avstrija	Direktiva ni prenesena.		
Poljska	ne	ne	-
Portugalska	ne	ne	-
Romunija	Direktiva ni prenesena.		
Slovenija	ne	ne	-
Slovaška	ne	ne	-
Finska	da	da	1

<sup>117</sup> Pred razveljavitvijo češke zakonodaje o prenosu je Češka povrnila odhodke iz poslovanja in investicijske izdatke ter je za leto 2009 poročala o 6,8 milijona EUR stroškov za povračila.

Švedska	Direktiva ni prenesena.		
Združeno kraljestvo	da	da	55 (jih je skupaj dobilo povrnjene stroške, nastale v zadnjih treh letih)

Na podlagi zgoraj navedenega se lahko sklepa, da Direktiva ni v celoti dosegla cilja vzpostavitve enotnih pogojev delovanja za ponudnike v EU. Komisija bo proučila možnosti za zmanjšanje ovir pri delovanju notranjega trga z zagotavljanjem, da se ponudnikom, zlasti malim in srednje velikim, bolj dosledno povrnejo stroški, ki nastanejo zaradi izpolnjevanja zahtev po hrambi podatkov.

## 7. POSLEDICE HRAMBE PODATKOV ZA TEMELJNE PRAVICE

### 7.1. Temeljna pravica do zasebnosti in varstva osebnih podatkov

Hramba podatkov predstavlja omejitev pravice do zasebnega življenja in varstva osebnih podatkov, ki sta temeljni pravici v Evropski uniji<sup>118</sup>. V skladu s členom 52(1) Listine o temeljnih pravicah mora biti tako omejevanje „predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin, ob upoštevanju načela sorazmernosti“ ter utemeljeno kot potrebno in da izpolnjuje cilje v splošnem interesu, ki jih priznava Evropska unija, ali potrebo po zaščiti pravic in svoboščin drugih. V praksi to pomeni, da mora biti vsaka omejitev<sup>119</sup>:

- (a) opredeljena natančno in predvidljivo;
- (b) potrebna za izpolnitev cilja v splošnem interesu ali zaradi varovanja pravic in svoboščin drugih;
- (c) sorazmerna z zastavljenim ciljem in
- (d) spoštovati bistveno vsebino zadevnih temeljnih pravic.

Tudi člen 8(2) Evropske konvencije o človekovih pravicah priznava, da je poseganje javnega organa v pravico posameznika do zasebnosti lahko potrebno v interesu nacionalne in javne varnosti ali preprečevanja kriminala<sup>120</sup>. Člen 15(1) Direktive o e-zasebnosti in uvodne izjave Direktive o hrambi podatkov ponavljajo ta načela, ki podpirajo pristop EU k hrambi podatkov.

Poznejša sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice je razvila pogoje, ki jih mora izpolnjevati vsaka omejitev pravice do zasebnosti. Te sodbe so pomembne pri odločanju, ali bi bilo treba Direktivo spremeniti, zlasti glede pogojev za dostop do hranjenih podatkov in uporabe takih podatkov.

<sup>118</sup> Člena 7 in 8 Listine Evropske unije o temeljnih pravicah (UL C 83, 30.3.2010, str. 389) zagotavljata pravico vsakogar „do varstva osebnih podatkov, ki se nanj nanašajo.“ Tudi člen 16 Pogodbe o delovanju Evropske unije (UL C 83, 30.3.2010, str. 1) vsebuje pravico vsakogar „do varstva osebnih podatkov, ki se nanj nanašajo“.

<sup>119</sup> Glej kontrolni seznam temeljnih pravic za vse zakonodajne predloge v sporočilu Komisije COM(2010) 573/4 „Strategija za učinkovito izvajanje Listine o temeljnih pravicah v Evropski uniji“.

<sup>120</sup> Člen 8 Konvencije o varstvu človekovih pravic in temeljnih svoboščin (ETS št. 5), Svet Evrope, 4.11.1950.

*Vse omejitve pravice do zasebnosti morajo biti natančne in omogočati morajo predvidljivost*

V zadevi Österreichischer Rundfunk je Sodišče odločilo, da mora biti vsak poseg v pravico do zasebnosti „določen dovolj natančno, da bi naslovniki zakona lahko prilagodili svoja ravnanja... [ali ustreza] načelu predvidljivosti“.

*Vse omejitve pravice do zasebnosti morajo biti nujne ob zagotovitvi minimalnih zaščitnih ukrepov*

V zadevi Copland proti Združenemu kraljestvu, ki zadeva nadzor države nad telefonskimi klici, elektronsko korespondenco in uporabo interneta neke osebe, je Evropsko sodišče za človekove pravice odločilo, da bi se taka omejitev pravice do zasebnosti štela za potrebno le, če bi temeljila na ustrezni domači zakonodaji<sup>121</sup>. V zadevi S. in Marper proti Združenemu kraljestvu, ki zadeva hrambo profilov DNK ali prstnih odtisov osebe, ki je bila oproščena kaznivega dejanja ali je bil postopek opuščen pred obsodbo, je Sodišče odločilo, da je taka omejitev pravice do zasebnosti lahko utemeljena le, če rešuje perečo socialno potrebo, če je sorazmerna s ciljem in če so razlogi, ki jih navaja javni organ kot utemeljitev, ustrezni in zadostni<sup>122</sup>. Osnovna načela varstva podatkov so zahtevala, da je hramba podatkov sorazmerna z namenom zbiranja, obdobje hrambe pa mora biti omejeno<sup>123</sup>. Pri telefonskem prisluškovanju, tajnem nadzorovanju in prikritem zbiranju obveščevalnih podatkov „je [bilo] bistveno ..., da obstajajo jasna in podrobna pravila, ki urejajo področje uporabe in uporabo ukrepov ter minimalne zaščitne ukrepe med drugim o trajanju, shranjevanju, uporabi, dostopu tretjih oseb, postopkih za ohranjanje celovitosti in zaupnosti podatkov ter postopkih za uničenje, in tako zagotoviti zadostna jamstva pred nevarnostjo zlorabe in samovolje“.

*Vse omejitve pravice do zasebnosti morajo biti sorazmerne s splošnim interesom*

Podobno je Sodišče v svoji odločitvi o zadevi Schecke in Eifert v zvezi z objavo vseh prejemnikov kmetijskih subvencij na internetu<sup>124</sup> ugotovilo, da se zdi, da zakonodajalci EU niso sprejeli ustreznih ukrepov za uravnoteženje spoštovanja bistvene vsebine pravice do zasebnosti in splošnega interesa (preglednosti), kot ga priznava Evropska unija. Zlasti je Sodišče ugotovilo, da zakonodajalci niso upoštevali drugih metod, ki bi bile skladne s ciljem in bi povzročile manj poseganja v pravico prejemnikov subvencij do spoštovanja njihovega zasebnega življenja in varstva osebnih podatkov. Zato je Sodišče odločilo, da so zakonodajalci presegli meje sorazmernosti, ker „morajo biti omejitve varstva osebnih podatkov strogo omejene na tisto, kar je nujno“.

## **7.2. Kritika načela hrambe podatkov**

Komisiji je pisalo več civilnih skupin, ki trdijo, da je hramba podatkov načeloma neupravičena in nepotrebna omejitev pravice posameznika do zasebnosti. Menijo, da je „vsesplošna in neselektivna“ hramba podatkov posameznikov o telekomunikacijskem prometu, lokaciji in naročnikih brez privolitve nezakonito omejevanje temeljnih pravic. Po

---

<sup>121</sup> Copland proti Združenemu kraljestvu, sodba Evropskega sodišča za človekove pravice, Strasbourg, 3.4.2007, str. 9

<sup>122</sup> Marper proti Združenemu kraljestvu, sodba Evropskega sodišča za človekove pravice, Strasbourg, 4.12.2008, str. 31

<sup>123</sup> Marper, str. 30.

<sup>124</sup> Sodba Sodišča z dne 9. novembra 2010 v zadevi Volker in Markus Schecke GbR proti Land Hessen (C-92/09) in v zadevi Hartmut Eifert proti Land Hessen (C-93/09).

zadevi, ki jo je na sodišče v eni državi članici (Irska) predložila civilna skupina, je treba vprašanje zakonitosti Direktive posredovati Sodišču Evropske unije<sup>125</sup>. Tudi evropski nadzornik za varstvo podatkov je izrazil dvome glede nujnosti ukrepa.

### 7.3. Pozivi k strožjim pravilom o varovanju in varnosti podatkov

Delovna skupina iz člena 29 je v svojem poročilu o drugem skupnem izvršilnem ukrepu trdila, da so nevarnosti kršitev zaupnosti komunikacij in svobode izražanja del vsakega shranjevanja podatkov o prometu. Kritizirala je nekatere vidike nacionalnega izvajanja, zlasti beleženje podatkov, obdobja hrambe, vrsto podatkov, ki se hranijo, in ukrepe za varovanje podatkov. Delovna skupina je poročala o primerih, v katerih so se hranile podrobnosti o vsebini komunikacij v zvezi z internetom, kar je zunaj področja uporabe Direktive, vključno s ciljnim naslovom IP in naslovi spletnih strani, glavami elektronske pošte in seznamom prejemnikov v polju „kopija“. Zato je zahtevala razjasnitev, do so kategorije izčrpane in da se ponudnikom ne sme naložiti nobenih dodatnih obveznosti glede hrambe podatkov.

Evropski nadzornik za varstvo podatkov je potrdil, da Direktiva „ni uskladila nacionalne zakonodaje“ in da uporaba hranjenih podatkov ni strogo omejena na boj proti hudim kaznivim dejanjem<sup>126</sup>. Dejal je, da če se dokaže nujnost, bi moral instrument EU, ki vsebuje pravila o obvezni hrambi podatkov, vsebovati tudi pravila o dostopu za organe pregona in o nadaljnji uporabi. Od EU je zahteval, naj sprejme celovit zakonodajni okvir, ki ne bo samo nalagal ponudnikom obveznost hrambe podatkov, ampak bo tudi urejal način uporabe podatkov v državah članicah za namene kazenskega pregona, da se ustvari „pravna varnost za državljane“.

Organi za varstvo podatkov so na splošno trdili, da hramba podatkov sama pomeni nevarnost morebitnih kršitev zasebnosti, ki jih Direktiva ne obravnava na ravni EU, ampak od držav članic zahteva, da zagotovijo spoštovanje nacionalnih predpisov o varstvu podatkov. Čeprav ni konkretnih primerov hujših kršitev zasebnosti, bo nevarnost kršitve varnosti podatkov ostala ter se z razvojem tehnologije in načinov komunikacije lahko še poveča, ne glede na to ali so podatki shranjeni za komercialne ali varnostne namene, v EU ali zunaj EU, če ne bodo vzpostavljeni nadaljnji zaščitni ukrepi.

## 8. ZAKLJUČKI IN PRIPOROČILA

V tem poročilu so poudarjene številne koristi trenutne ureditve hrambe podatkov v EU in tudi področja za njeno izboljšanje. EU je Direktivo sprejela v času naraščajočega opozarjanja na nevarnost terorističnih napadov. Ocena učinka, ki jo namerava opraviti Komisija, je priložnost, da se hramba podatkov v EU oceni na podlagi preskusov nujnosti in sorazmernosti, v zvezi z notranjo varnostjo in v interesu notranje varnosti, nemotenega delovanja notranjega trga in okrepitve spoštovanja zasebnosti in temeljne pravice do varstva osebnih podatkov. Predlog Komisije za revizijo okvira hrambe podatkov bi moral graditi na naslednjih zaključkih in priporočilih.

---

<sup>125</sup> Irsko vrhovno sodišče je 5. maja 2010 družbi Digital Rights Ireland Limited odobrilo pobudo za posredovanje na EJC na podlagi člena 267 Pogodbe o delovanju Evropske unije.

<sup>126</sup> Govor Petra Hustinx na konferenci z naslovom „Prevzem Direktive o hrambi podatkov“, 3. december 2010.

### **8.1. EU bi morala podpirati in urediti hrambo podatkov kot varnostni ukrep**

Večina držav članic meni, da so pravila EU o hrambi podatkov potrebna kot orodje za kazenski pregon, varstvo žrtev in kazenskoopravne sisteme. Dokazi v obliki statistike in primerov, ki so jih posredovale države članice, so sicer v nekaterih pogledih omejeni, vendar potrjujejo zelo pomembno vlogo hranjenih podatkov v kazenskih preiskavah. Ti podatki zagotavljajo dragocene sledi in dokaze pri preprečevanju in pregonu kaznivih dejanj in pri zagotavljanju kazenskega pravosodja. Njihova uporaba je povzročila obsodbe zaradi kaznivih dejanj, ki brez hrambe podatkov morda ne bi bila nikoli rešena. Omogočila je tudi oprostitve nedolžnih osumljencev. Usklajeni predpisi na tem področju bi morali zagotoviti, da je hramba podatkov učinkovito orodje v boju proti kriminalu, da ima gospodarska panoga pravno varnost ob nemotenem delovanju notranjega trga in da se visoke stopnje spoštovanja zasebnosti in varstva osebnih podatkov v vsej EU uporabljajo dosledno.

### **8.2. Prenos ni bil enakomeren**

Zakonodaja za prenos velja v 22 državah članicah. Zaradi znatne svobode, ki jo imajo države članice pri sprejemanju ukrepov hrambe podatkov na podlagi člena 15(1) Direktive o zasebnosti je ocena Direktive o hrambi podatkov zelo težavna. V zakonodaji za prenos so na področju omejitve namena, dostopa do podatkov, obdobja hrambe, varovanja in varnosti podatkov in statistike velike razlike. Tri države članice kršijo Direktivo, ker so svojo zakonodajo za prenos ustavna sodišča razveljavila. Dve državi članici še nista prenesli Direktive. Komisija bo nadaljevala svoje delo z vsemi državami članicami, da pomaga zagotoviti učinkovito izvajanje Direktive. Še naprej bo ohranila svojo vlogo pri krepitvi prava EU in če bo potrebno, bo na koncu uporabila postopek zaradi neizpolnitve obveznosti.

### **8.3. Direktiva ni popolnoma uskladila pristopa na področju hrambe podatkov in ni ustvarila enotnih pogojev delovanja za ponudnike**

Direktiva je zagotovila, da se zdaj podatki hranijo v večini držav članic. Direktiva sama po sebi ne zagotavlja, da se hranjeni podatki shranjujejo, pridobivajo in uporabljajo popolnoma v skladu s pravico do zasebnosti in varstva osebnih podatkov. Države članice morajo zagotoviti ohranjanje teh pravic. Direktiva je dosegla samo delno uskladitev pristopov k hrambi podatkov; zato ni presenetljivo, da ni skupnega pristopa niti glede posebnih določb Direktive, kot sta omejitev namena ali obdobja hrambe, niti glede vidikov zunaj področja uporabe, kot je povračilo stroškov. Vendar poleg stopnje razlik, ki jih Direktiva izrecno določa, razlike v izvajanju v posameznih državah ponudnikom povzročajo velike težave.

### **8.4. Ponudnikom bi bilo treba dosledno povrniti nastale stroške**

V gospodarski panogi še naprej primanjkuje pravne varnosti. Obveznost hranjenja in pridobivanja podatkov predstavlja znatne stroške za ponudnike, zlasti manjše, in v nekaterih državah članicah to v primerjavi z drugimi na ponudnike različno vpliva, tudi v zvezi s povračilom stroškov, čeprav ni dokazov, da je bil telekomunikacijski sektor zaradi Direktive oškodovan. Komisija bo proučila načine za zagotavljanje doslednega povračila ponudnikom.

## **8.5. Zagotavljanje sorazmernosti postopka shranjevanja, pridobivanja in uporabe od začetka do konca**

Komisija bo zagotovila, da bo vsak prihodnji predlog o hrambi podatkov spoštoval načelo sorazmernosti in bo primeren za doseganje cilja boja proti hudim kaznivim dejanjem in terorizmu ter ne bo presegal tistega, kar je potrebno za doseganje cilja. Priznala bo, da se izjeme ali omejitve glede varstva osebnih podatkov lahko uporabljajo samo, če so potrebne. Natančno bo ocenila posledice strožjih predpisov za shranjevanje in uporabo hranjenih podatkov ter dostop do podatkov o prometu na učinkovitost in uspešnost kazenskega pregona in kazenskopravnega sistema, na zasebnost in na stroške za javne uprave in ponudnike. V oceni učinka je treba proučiti zlasti naslednja področja:

- doslednost pri omejevanju namena hrambe podatkov in vrstah kaznivih dejanj, za katera je mogoč dostop do hranjenih podatkov in uporaba podatkov;
- večjo uskladitev in morebitno skrajšanje obdobj obveznega hranjenja podatkov;
- zagotavljanje neodvisnega nadzora nad zahtevki za dostop in nad celotno hrambo podatkov in ureditev dostopa, ki se uporablja v vseh državah članicah;
- omejevanje organov, ki imajo dovoljenje za dostop do podatkov;
- zmanjševanje kategorij podatkov, ki jih je treba hraniti;
- navodila za tehnične in organizacijske varnostne ukrepe za dostop do podatkov, vključno s postopki primopredaje;
- navodila za uporabo podatkov, vključno s preprečevanjem podatkovnega rudarjenja in
- razvoj izvedljivih postopkov meritev in poročanja, ki bodo olajšali primerjavo uporabe in vrednotenje prihodnjega instrumenta.

Komisija bo tudi proučila, ali bi pristop EU k ohranitvi podatkov lahko dopolnjeval hrambo podatkov in kako bi bilo to mogoče.

V zvezi s „kontrolnim seznamom“ temeljnih pravic in pristopom k upravljanju informacij na območju svobode, varnosti in pravice<sup>127</sup> bo Komisija proučila vsako od teh področij glede načel sorazmernosti in zahteve po predvidljivosti. Zagotovila bo tudi usklajenost s tekočim pregledom okvira EU za varstvo podatkov<sup>128</sup>.

## **8.6. Kako naprej**

Komisija bo ob upoštevanju te ocene predlagala pregled sedanjega okvira hrambe podatkov. V posvetovanju z organi pregona, sodstvom, gospodarsko panogo in potrošniškimi skupinami, organi za varstvo podatkov in organizacijami civilne družbe bo pripravila več možnosti.

---

<sup>127</sup> Glej sklic zgoraj na sporočilo o izvajanju Listine o temeljnih pravicah „Pregled upravljanja informacij na območju svobode, varnosti in pravice“, COM(2010) 385, 20.7.2010.

<sup>128</sup> COM(2010) 609, 4.11.2010.

Nadalje bo raziskala, kako javnost dojema hrambo podatkov in vpliv hrambe podatkov na vedenje. Te ugotovitve bodo vključene v oceno učinka ugotovljenih možnosti politik, kar bo Komisija uporabila kot podlago za svoj predlog.

## Priloga: Dodatna statistika o hrambi podatkov o prometu

### Opombe k Prilogi:

1. Starost podatkov pomeni čas med dnevom, ko so bili podatki shranjeni, in dnevom, ko je pristojni organ zahteval prenos podatkov.
2. Podatki, povezani z internetom, pomenijo podatke o dostopu do interneta, internetni elektronski pošti in internetni telefoniji.
3. Statistika za Češko, Latvijo in Poljsko ob upoštevanju opozorila (glej oddelek 5.1).

### Statistika, ki so jo države članice predložile za leto 2008

<b>Preglednica 7: Zahtevki za hranjene podatke o prometu po starosti v letu 2008</b>									
Starost podatkov (mesecev)/država članica	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Skupaj
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	102691	18440	10110	319	0	0	0	0	131560
Danska	2669	672	185	37	23	2	7	4	3599
Nemčija	9363	2336	985	0	0	0	0	0	12684
Estonija	2773	733	157	827	0	0	0	0	4490
Irska	8981	2016	936	1855	90	85	78	54	14095
Grčija	razčlenitev po starosti ni predložena								
Španija	22629	15868	10298	4783	0	0	0	0	53578
Francija	razčlenitev po starosti ni predložena								
Italija	ni predloženo								
Ciper	30	4	0	0	0	0	0	0	34
Latvija	10539	2739	1368	1211	597	438	0	0	16892
Litva	55735	23817	5251	512	0	0	0	0	85315
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	810	59	0	0	0	0	0	0	869
Nizozemska	razčlenitev po starosti ni predložena								
Avstrija	razčlenitev po starosti ni predložena								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	razčlenitev po starosti ni predložena								
Slovaška	ni predloženo								
Finska	9134	1144	448	214	268				4008
Švedska	ni predloženo								
Združeno kraljestvo	315350	88339	34665	19398	6385	2973	1536	1576	470222
<b>Skupaj</b>	<b>533504</b>	<b>156167</b>	<b>64403</b>	<b>29156</b>	<b>7095*</b>	<b>3230*</b>	<b>1353*</b>	<b>1366*</b>	<b>1392281</b>

\* Podatek brez Finske.

<b>Preglednica 8: Zahtevki za hranjene podatke o prometu po vrstah podatkov v letu 2008</b> (v oklepajih so zadeve, v katerih zahtevkov za podatke ni bilo mogoče izpolniti – če je bilo predloženo)				
<b>Vrsta podatkov/ država članica</b>	<b>Fixed network telephony</b>	<b>Mobile telephony</b>	<b>Internet-related</b>	<b>Total</b>
Belgija	ni predloženo			
Bolgarija	ni predloženo			
Češka	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Danska	192 (0)	3273 (5)	134 (0)	3599 (5)
Nemčija	razčlenitev po vrstah podatkov ni predložena			12684 (931)
Estonija	4114 (1519)	376 (7)	ni predloženo	4490 (1526)
Irska	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Grčija	razčlenitev po vrstah podatkov ni predložena			584
Španija	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Francija	razčlenitev po vrstah podatkov ni predložena			503437
Italija	ni predloženo			
Ciper	3 (0)	31 (5)	0 (0)	34 (5)
Latvija	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Litva	765 (72)	84550 (5657)	ni predloženo	85315 (5729)
Luksemburg	ni predloženo			
Madžarska	ni predloženo			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Nizozemska	razčlenitev po vrstah podatkov ni predložena			85000
Avstrija	razčlenitev po vrstah podatkov ni predložena			3093
Poljska	ni predloženo			
Portugalska	ni predloženo			
Romunija	ni predloženo			
Slovenija	razčlenitev po vrstah podatkov ni predložena			2821
Slovaška	ni predloženo			
Finska	razčlenitev po vrstah podatkov ni predložena			4008
Švedska	ni predloženo			
Združeno kraljestvo	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Skupaj				1392281

<b>Preglednica 9: Zahtevki za hranjene podatke o prometu za telefonijo v fiksni omrežju, ki so bili posredovani, po starosti, v letu 2008</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	3669	916	143	124	0	0	0	0	4852
Danska	133	28	31	0	0	0	0	0	192
Nemčija	ni predloženo								
Estonija	1876	161	74	484	0	0	0	0	2595
Irska	4118	712	197	182	32	21	23	16	5301
Grčija	ni predloženo								
Španija	1948	1431	741	328	0	0	0	0	4448
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	3	0	0	0	0	0	0	0	3
Latvija	698	213	167	193	104	137	0	0	1512
Litva	251	442	0	0	0	0	0	0	693
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	28	1	0	0	0	0	0	0	29
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	54805	27052	5340	753	1135	437	1050	175	90747
<b>Skupaj</b>	<b>67529</b>	<b>30956</b>	<b>6693</b>	<b>2064</b>	<b>1271</b>	<b>595</b>	<b>1073</b>	<b>191</b>	<b>110372</b>

<b>Preglednica 10: Zahtevki za hranjene podatke o prometu za mobilno telefonijo, ki so bili posredovani, po starosti, v letu 2008</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Česka	98232	17013	7518	1	0	0	0	0	122764
Danska	2433	628	143	33	20	1	7	3	3268
Nemčija	ni predloženo								
Estonija	248	58	35	28	0	0	0	0	369
Irska	4326	820	230	240	57	63	52	37	5825
Grčija	ni predloženo								
Španija	17403	12114	7444	3052	0	0	0	0	40013
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	23	3	0	0	0	0	0	0	26
Latvija	8928	2298	1085	746	394	257	0	0	13708
Litva	55484	23375	14	20	0	0	0	0	78893
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	575	53	0	0	0	0	0	0	628
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	22937 5	52241	2622 8	1604 0	333 3	521	339	134 4	329421
<b>Skupaj</b>	<b>41702 7</b>	<b>10860 3</b>	<b>4269 7</b>	<b>2016 0</b>	<b>380 4</b>	<b>842</b>	<b>398</b>	<b>138 4</b>	<b>594915</b>

<b>Preglednica 11: Zahtevki za hranjene podatke o prometu, povezane z internetom, ki so bili posredovani, po starosti, v letu 2008</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	737	412	137	168	0	0	0	0	1454
Danska	102	14	11	2	3	1	0	1	134
Nemčija	ni predloženo								
Estonija	ni predloženo								
Irska	492	460	498	1422	0	0	0	0	2872
Grčija	ni predloženo								
Španija	3278	2323	2113	1403	0	0	0	0	9117
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	0	0	0	0	0	0	0	0	0
Latvija	424	150	75	219	74	34	0	0	976
Litva	ni predloženo								
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	76	3	0	0	0	0	0	0	79
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	31170	9046	3097	2605	1917	2015	147	57	50054
<b>Skupaj</b>	<b>36279</b>	<b>12408</b>	<b>5931</b>	<b>5819</b>	<b>1994</b>	<b>2050</b>	<b>147</b>	<b>58</b>	<b>64686</b>

## Statistika, ki so jo države članice predložile za leto 2009

Preglednica 12: Zahtevki za hranjene podatke po starosti v letu 2009									
Starost zahtevanih podatkov (mesecev)/država članica	0-3	3-6	6-9	9-12	12-15	15-18	18-21	21-24	Skupaj
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	210975	56623	11620	1053	0	0	0	0	280271
Danska	2980	685	179	104	54	38	12	14	4066
Nemčija	ni posredovano								
Estonija	4299	1836	1210	1065	0	0	0	0	8410
Irska	8117	1652	805	297	168	134	69	41	11283
Grčija	ni predloženo								
Španija	29775	19346	13999	6970	0	0	0	0	70090
Francija	razčlenitev po starosti ni predložena								514813
Italija	ni predloženo								
Ciper	31	8	1	0	0	0	0	0	40
Latvija	20758	2414	1088	796	565	475	0	0	26096
Litva	30247	35456	5886	884	0	0	0	0	72473
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	3336	362	151	174	0	0	0	0	4023
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Poljska	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovenija	razčlenitev po starosti ni predložena								1918
Slovaška	razčlenitev po starosti ni predložena								5214
Finska	2000	1310	532	152	76	0	0	0	4070
Švedska	ni predloženo								
Združeno kraljestvo	ni predloženo								
<b>Skupaj</b>	<b>954845</b>	<b>297998</b>	<b>110996</b>	<b>64021</b>	<b>27961</b>	<b>24571</b>	<b>14065</b>	<b>34683</b>	<b>2051085</b>

<b>Preglednica 13: Zahtevki za hranjene podatke po vrstah podatkov v letu 2009</b>				
<b>(v oklepajih so zadeve, v katerih zahtevkov za podatke ni bilo mogoče izpolniti – če je bilo predloženo)</b>				
<b>Vrsta podatkov/ država članica</b>	<b>Telefonija v fiksnem omrežju</b>	<b>Mobilna telefonija</b>	<b>Podatki, povezani z internetom</b>	<b>Skupaj</b>
Belgija	ni predloženo			
Bolgarija	ni predloženo			
Češka	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Danska	133 (0)	3771 (10)	162 (1)	4066 (11)
Nemčija	ni predloženo			
Estonija	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irska	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grčija	ni predloženo			
Španija	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Francija	razčlenitev po vrstah podatkov ni predložena			514813
Italija	ni predloženo			
Ciper	0 (0)	23 (3)	14 (0)	40 (3)
Latvija	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Litva	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luksemburg	ni predloženo			
Madžarska	ni predloženo			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Nizozemska	ni predloženo			
Avstrija	ni predloženo			
Poljska	razčlenitev po vrstah podatkov ni predložena			1048318
Portugalska	ni predloženo			
Romunija	ni predloženo			
Slovenija	razčlenitev po vrstah podatkov ni predložena			1918 (48)
Slovaška	razčlenitev po vrstah podatkov ni predložena			5214 (157)
Finska	razčlenitev po vrstah podatkov ni predložena			4070
Švedska	ni predloženo			
Združeno kraljestvo	ni predloženo			
Skupaj				2051082 (1069885)

<b>Preglednica 14: Zahtevki za hranjene podatke o telefoniji v fiksnem omrežju, ki so bili posredovani, po starosti, v letu 2009</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	9919	2907	47	36	0	0	0	0	12909
Danska	105	19	7	2	0	0	0	0	133
Nemčija	ni predloženo								
Estonija	2254	866	599	424	0	0	0	0	4143
Irska	3934	337	69	70	50	39	16	11	4526
Grčija	ni predloženo								
Španija	2371	1492	844	348	0	0	0	0	5055
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	0	0	0	0	0	0	0	0	0
Latvija	744	253	157	143	68	89	0	0	1454
Litva	469	773	73	6	0	0	0	0	1321
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	83	25	18	20	0	0	0	0	146
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	ni predloženo								
<b>Skupaj</b>	<b>19879</b>	<b>6672</b>	<b>1814</b>	<b>1049</b>	<b>118</b>	<b>128</b>	<b>16</b>	<b>11</b>	<b>29687</b>

<b>Preglednica 15: Zahtevki za hranjene podatke o mobilni telefoniji, ki so bili posredovani, po starosti, v letu 2009</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Česka	197620	48841	472	0	0	0	0	0	246933
Danska	2777	639	162	98	47	19	12	7	3761
Nemčija	ni predloženo								
Estonija	318	397	96	70	0	0	0	0	881
Irska	3669	835	220	210	115	92	50	28	5219
Grčija	ni predloženo								
Španija	24065	15648	11147	5273	0	0	0	0	56133
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	17	16	0	0	0	0	0	0	23
Latvija	18832	1912	778	515	394	263	0	0	22694
Litva	25713	19595	28	0	0	0	0	0	45336
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	2332	246	111	122	0	0	0	0	2811
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	ni predloženo								
<b>Skupaj</b>	<b>275343</b>	<b>88119</b>	<b>13014</b>	<b>6288</b>	<b>556</b>	<b>374</b>	<b>62</b>	<b>35</b>	<b>383791</b>

<b>Preglednica 16: Zahtevki za hranjene podatke, povezane z internetom, ki so bili posredovani, po starosti, v letu 2009</b>									
<b>Starost zahtevanih podatkov (mesecev)/država članica</b>	<b>0-3</b>	<b>3-6</b>	<b>6-9</b>	<b>9-12</b>	<b>12-15</b>	<b>15-18</b>	<b>18-21</b>	<b>21-24</b>	<b>Skupaj</b>
Belgija	ni predloženo								
Bolgarija	ni predloženo								
Češka	3369	4811	861	942	0	0	0	0	9983
Danska	98	27	10	4	4	7	0	1	151
Nemčija	ni predloženo								
Estonija	315	145	56	102	0	0	0	0	618
Irska	489	455	502	0	0	0	0	0	1446
Grčija	ni predloženo								
Španija	3339	2206	2008	1349	0	0	0	0	8902
Francija	ni predloženo								
Italija	ni predloženo								
Ciper	12	2	0	0	0	0	0	0	14
Latvija	852	198	74	90	88	86	0	0	1388
Litva	4060	15087	1	88	0	0	0	0	19236
Luksemburg	ni predloženo								
Madžarska	ni predloženo								
Malta	150	14	0	0	0	0	0	0	164
Nizozemska	ni predloženo								
Avstrija	ni predloženo								
Poljska	ni predloženo								
Portugalska	ni predloženo								
Romunija	ni predloženo								
Slovenija	ni predloženo								
Slovaška	ni predloženo								
Finska	ni predloženo								
Švedska	ni predloženo								
Združeno kraljestvo	ni predloženo								
<b>Skupaj</b>	<b>12684</b>	<b>22945</b>	<b>3512</b>	<b>2575</b>	<b>92</b>	<b>93</b>	<b>0</b>	<b>1</b>	<b>41902</b>