EIROPAS SAVIENĪBAS PADOME

Briselē, 2011. gada 19. aprīlī (03.05)
(OR. en)

9324/11

DAPIX 38
TELECOM 47
COPEN 85

PAVADVĒSTULE

Sūtītājs:	Direktors *Jordi AYET PUIGARNAU* kungs, Eiropas Komisijas ģenerālsekretāra vārdā
Saņemšanas datums:	2011. gada 18. aprīlis
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Pierre de BOISSIEU* kungs
K-jas. dok. Nr.	COM(2011) 225 galīgā redakcija
Temats:	Komisijas Ziņojums Padomei un Eiropas Parlamentam - Izvērtējuma ziņojums par Datu saglabāšanas direktīvu (Direktīva 2006/24/EK)

Pielikumā ir pievienota Komisijas dokumenta COM(2011) 225 galīgā redakcija.

_____

Pielikumā: COM(2011) 225 galīgā redakcija

EIROPAS KOMISIJA

Brisel?, 18.4.2011
COM(2011) 225 gal?g? redakcija

KOMISIJAS ZI?OJUMS PADOMEI UN EIROPAS PARLAMENTAM

Izv?rt?juma zi?ojums par Datu saglab?šanas direkt?vu (Direkt?va 2006/24/EK)

KOMISIJAS ZIŅOJUMS PADOMEI UN EIROPAS PARLAMENTAM

Izvērtējuma ziņojums par Datu saglabāšanas direktīvu (Direktīva 2006/24/EK)

1. IEVADS

Datu saglabāšanas direktīva[1] (turpmāk „direktīva") prasa, lai dalībvalstis uzliek par pienākumu publiski pieejamu elektronisko pakalpojumu sniedzējiem vai publiski pieejamu komunikāciju tīklu operatoriem (turpmāk „operatori") smagu noziegumu izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem saglabāt noslodzes datus un atrašanās vietas datus uz laiku, sākot no sešiem mēnešiem, līdz diviem gadiem.

Ņemot vērā elektroniskās komunikācijas tehnoloģijas attīstību un Komisijai iesniegto statistiku, Komisija saskaņā ar šīs direktīvas 14. pantu šajā ziņojumā izvērtē šīs direktīvas piemērošanu dalībvalstīs un tās ietekmi uz ekonomiskā procesa dalībniekiem un patērētājiem, lai noteiktu, vai ir nepieciešams grozīt šīs direktīvas noteikumus jo īpaši attiecībā uz aptvertajiem datiem un saglabāšanas periodiem. Komisija šajā ziņojumā arī pārbauda direktīvas ietekmi uz pamattiesībām, ņemot vērā kritiku, kas principā pausta par datu saglabāšanu, un pārbauda, vai nepieciešami pasākumi, lai novērstu bažas, kas saistītas ar anonīmu SIM karšu lietošanu noziedzīgos nolūkos[2].

Kopumā izvērtējumā ir skaidri redzams, ka datu saglabāšana ir vērtīgs krimināls justīcijas un tiesībaizsardzības instruments Eiropas Savienībā. Direktīvas ieguldījums datu saglabāšanas saskaņošanā ir bijis ierobežots, piemēram, nolūka ierobežošanas un saglabāšanas termiņu izteiksmē, kā arī operatoriem radušos izmaksu atlīdzības jomā, kas ir ārpus direktīvas darbības sfēras. Ņemot vērā datu saglabāšanas ietekmi uz iekšējo tirgu un radītos riskus, kā arī, lai ievērotu tiesības uz privātumu un personas datu aizsardzības principus, ES jāizstrādā kopīgi noteikumi, lai turpinātu nodrošināt, ka nepārtraukti tiek uzturēti augsti noslodzes datu un atrašanās vietas datu uzglabāšanas, izguves un lietošanas standarti. Ņemot vērā šos secinājumus un pamatojoties uz ietekmes novērtējumu, Komisija plāno ierosināt šīs direktīvas grozījumus.

2. IZVĒRTĒJUMA PAMATOJUMS

Šis izvērtējuma ziņojums ir sastādīts, izmantojot dalībvalstu, ekspertu un ieinteresēto pušu sniegto informāciju un informāciju, kas iegūta plašās diskusijās ar dalībvalstīm, ekspertiem un ieinteresētajām pusēm.

---

1 Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK, OV L 105, 13.4.2006, 54.-63. lpp.

2 Padomes secinājumi par elektronisko komunikāciju noziedzīgas vai anonīmas lietošanas apkarošanu, Padomes 2908. sanāksme Tieslietas un Iekšlietas Briselē, 2008. gada 27. un 28. novembrī.

Komisija 2009. gada maijā organizēja konferenci ar nosaukumu „Uzsākot Datu saglabāšanas direktīvas izvērtējumu", kuru apmeklēja pārstāvji no datu aizsardzības iestādēm, privātā sektora, pilsoniskās sabiedrības un augstākās izglītības iestādēm. Komisija 2009. gada septembrī šo grupu dalībniekiem izsūtīja aptauju, uz kuru saņēma aptuveni 70 atbildes[3]. Komisija 2010. gada decembrī organizēja otru konferenci ar nosaukumu „Uzsākot Datu saglabāšanas direktīvas īstenošanu", kuru apmeklēja līdzīgas ieinteresētās puses, lai dalītos viedoklī par direktīvas iepriekšējiem novērtējumiem un apspriestu tālāko rīcību šajā jomā.

Laikā no 2009. gada oktobra līdz 2010. gada martam Komisija tikās ar katras dalībvalsts un saistītās Eiropas Ekonomikas zonas dalībvalsts pārstāvjiem, lai padziļināti apspriestu jautājumus par direktīvas piemērošanu. Dalībvalstis direktīvu sāka piemērot vēlāk, nekā tas bija paredzēts, jo īpaši attiecībā uz datiem, kas saistīti ar internetu. Šīs aizkavētās direktīvas transponēšanas rezultātā deviņas dalībvalstis varēja iesniegt Komisijai pilnu statistiku par 2008. vai 2009. gadu saskaņā ar direktīvas 10. pantu, bet kopumā 19 dalībvalstis sniedza vismaz kaut kādu statistiku (sk. 4.7. nodaļu). Komisija 2010. gada jūlijā rakstīja dalībvalstīm, lūdzot iesniegt turpmāko kvantitatīvo un kvalitatīvo informāciju attiecībā uz to saglabāto datu nepieciešamību, kuru izmantošana sekmē tiesībaizsardzību. Desmit dalībvalstis sniedza informāciju par konkrētiem gadījumiem, kur dati izrādījās tiešām nepieciešami[4].

Ziņojumā paustie secinājumi iegūti no nostājas dokumentiem, kurus kopš tās dibināšanas 2008. gadā ir pieņēmusi ekspertu grupu „Platforma par elektronisko datu uzglabāšanu smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai"[5]. Komisija ir ņēmusi vērā 29. panta datu aizsardzības darba grupas ziņojumus[6], un jo īpaši ziņojumu par otro izpildu rīcību, tas ir, novērtējumu par dalībvalstu atbilstību direktīvā noteiktajām datu aizsardzības un drošības prasībām[7].

3. DATU SAGLABĀŠANA EIROPAS SAVIENĪBĀ

3.1. Datu saglabāšana kriminālās justīcijas un tiesībaizsardzības nolūkos

Pakalpojumu sniedzēji un tīkla operatori (turpmāk „operatori") savas darbības ietvaros apstrādā ievērojamu daudzumu personas datu ar nolūku nosūtīt komunikāciju, sagatavot rēķinus, veikt norēķinus par starpsavienojumiem, pakalpojumu tirdzniecību vai sniegt

---

3 Atbildes ir publicētas Komisijas tīmekļa vietnē (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm

4 Beļģija, Čehija, Kipra, Lietuva, Ungārija, Nīderlande, Polija, Slovēnija, Apvienotā Karaliste. Zviedrija arī ziņoja par dažiem konkrētiem smagu noziegumu gadījumiem, kur vēsturiskie dati, kuri bija pieejami, lai gan nepastāvēja datu saglabāšanas pienākums, bija izšķirošie, lai varētu notiesāt vainīgos.

5 Šī ekspertu grupa ir izveidota saskaņā ar Komisijas Lēmumu 2008/324/EK, OJ L 111, 23.04.2008, 11.-14. lpp. Komisija ar grupu tiekas regulāri. Tās nostājas dokumenti ir publicēti http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 Darba grupa personu aizsardzībai attiecībā uz personas datu apstrādi ir izveidota saskaņā ar Datu aizsardzības direktīvas 29. pantu (Eiropas Parlamenta un Padomes 1995. gada 24. oktobra direktīva par personas aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995, 31. lpp.).

7 Ziņojums 01/2010 par otro vienoto izpildu rīcību: Telekomunikāciju un interneta pakalpojumu sniedzēju atbilstība valsts līmenī valsts noslodzes datu saglabāšanas tiesību aktu prasībām, pamatojoties uz e-Privātuma Direktīvas 2002/58/EK 6. un 9. panta juridiskajām prasībām un Datu saglabāšanas direktīvu 2006/24/EK, ar ko groza E-privātuma direktīvu (WP 172), 13.07.2010., (skatīt http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

noteiktus cita veida pievienotās vērtības pakalpojumus. Šāda apstrāde ietver komunikācijas avota, galamērķa, datuma, laika, ilguma un veida, kā arī lietotāja komunikācijas aprīkojuma, un mobilās telefonijas gadījumā arī aprīkojuma atrašanās vietas datu noteikšanu. Saskaņā ar Direktīvu 2002/58/EK par elektroniskās komunikācijas privātumu (turpmāk „E-privātuma direktīva")[8] šādi noslodzes dati, kas iegūti, lietojot elektronisko komunikāciju pakalpojumus, principā ir jādzēš vai jāpadara anonīmi, kad tie vairs nav nepieciešami komunikāciju pārraidīšanai, ja vien tie nav nepieciešami un tikai tik ilgi, kamēr tie ir nepieciešami, lai sagatavotu rēķinu vai, ja abonents vai lietotājs ir devis savu piekrišanu. Atrašanās vietas datus var apstrādāt tikai tad, ja tie ir padarīti anonīmi vai ir iegūta attiecīgā lietotāja piekrišana, tikai tādā apmērā un tikai tik ilgi, cik nepieciešams, lai sniegtu pievienotās vērtības pakalpojumu.

Pirms direktīvas stāšanās spēkā saskaņā ar īpašiem nosacījumiem valstu iestādes no operatoriem pieprasītu piekļuvi šādiem datiem, lai, piemēram, noteiktu abonentus, kuri lieto IP adresi, analizētu iepriekšējās komunikāciju darbības un noteiktu mobilā tālruņa atrašanās vietu.

ES līmenī datu saglabāšana un lietošana tiesībaizsardzības nolūkos pirmo reizi tika skarta Direktīvā 97/66/EK par personas datu apstrādi un privātās dzīves aizsardzību telekomunikāciju nozarē. Šī direktīva pirmo reizi paredzēja iespēju dalībvalstīm pieņemt šādus tiesiskus pasākumus, ja tie nepieciešami sabiedrības drošības, aizsardzības vai sabiedriskās kārtības nodrošināšanai, tostarp valsts ekonomiskās labklājības nodrošināšanai, ja darbības bija saistītas ar valsts drošību un krimināltiesību īstenošanu[9].

Šis noteikums tālāk tika attīstīts E-privātuma direktīvā, kura paredz iespēju dalībvalstīm pieņemt tiesiskus pasākumus, ar kuriem atkāpjas no komunikāciju konfidencialitātes principa, tostarp no principa pie zināmiem nosacījumiem saglabāt, piekļūt un lietot datus tiesībaizsardzības nolūkiem. Direktīvas 15. panta 1. punkts ļauj dalībvalstīm ierobežot privātuma tiesības un pienākumus, tostarp, saglabājot datus ierobežotā laika posmā, ja „šādi ierobežojumi ir nepieciešami, atbilstīgi un samērīgi demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un krimināpārkāpumu vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un krimināvajāšanu".

Saglabāto datu loma kriminālās justīcijas un tiesībaizsardzības jomā sīkāk ir apskatīta 5. nodaļā.

3.2. Datu saglabāšanas direktīvas mērķis un juridiskais pamats

Saskaņā ar Direktīvas 97/66/EK un E-privātuma direktīvas noteikumiem, kas ļauj dalībvalstīm pieņemt tiesību aktus par datu saglabāšanu, dažās dalībvalstīs operatoriem prasīja, lai tie iepērk datu saglabāšanas aprīkojumu un algo darbiniekus, lai izgūtu datus tiesībaizsardzības iestāžu vārdā, bet citās dalībvalstīs operatoriem to neprasīja, kas noveda pie

---

[8] Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201 , 31/07/2002 37. – 47. lpp.).

[9] Eiropas Parlamenta un Padomes 1997. gada 15. decembra Direktīvas 97/66/EK par personas datu apstrādi un privātās dzīves aizsardzību telekomunikāciju nozarē 14. panta 1. punkts (OV L 24, 30.1.1998, 1.–8. lpp.).

iekšējā tirgus izkropļojumiem. Turklāt uzņēmējdarbības modeļu un pakalpojumu piedāvājumu tendences, piemēram, vienotas likmes tarifu, priekšapmaksas un bezmaksas elektronisko komunikāciju pakalpojumu attīstība veicināja to, ka operatori pakāpeniski pārstāja uzglabāt noslodzes datus un atrašanās vietas datus, lai sagatavotu rēķinus, tādejādi samazinot šādu datu pieejamību krimināltiesību un tiesībaizsardzības nolūkiem. Teroristu uzbrukumi Madridē 2004. gadā un Londonā 2005. gadā tikai pastiprināja nepieciešamību steidzīgi risināt šīs problēmas ES līmenī.

Ņemot vērā iepriekšminēto, Datu saglabāšanas direktīva noteica dalībvalstu publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem vai publiski pieejamu komunikāciju tīklu operatoriem pienākumu saglabāt komunikāciju datus, lai nodrošinātu, ka šie dati ir pieejami smagu noziegumu, kas katrā dalībvalstī noteikti tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, un centās saskaņot noteiktus saistītus jautājumus visā ES.

Direktīva grozīja E-privātuma direktīvas 15. panta 1. punktu, pievienojot punktu, kas paredz, ka 15. panta 1. punkts neattiecas uz datu saglabāšanu saskaņā ar Datu saglabāšanas direktīvu[10]. Tādejādi dalībvalstis (kā minēts Direktīvas 12. apsvērumā) vēl aizvien spēj atkāpties no komunikāciju konfidencialitātes principa. (Datu saglabāšanas) direktīva regulē vienīgi datu saglabāšanu daudz ierobežotākiem nolūkiem attiecībā uz smagu noziegumu izmeklēšanu, atklāšanu un kriminālvajāšanu.

Šīs sarežģītās tiesiskās attiecības starp šo direktīvu un E-privātuma direktīvu, kā arī fakts, ka abās direktīvās nav definēts termins „smags noziegums", rada grūtības atšķirt, no vienas puses, pasākumus, ko dalībvalstis veikušas, lai transponētu datu saglabāšanas pienākumus, kas noteikti direktīvā un, no otras puses, daudz vispārīgāku praksi dalībvalstīs attiecībā uz datu saglabāšanu, kas atļauta ar E-privātuma direktīvas 15. panta 1. punktu[11]. Šis jautājums ir sīkāk izskatīts 4. nodaļā.

Direktīva ir pamatota uz Eiropas Kopienas dibināšanas līguma 95. pantu (ko aizstāj Līguma par Eiropas Savienības darbību 114. pants) par iekšējā tirgus izveidi un darbību. Pēc šīs direktīvas pieņemšanas tās juridisko pamatu apstrīdēja Eiropas Kopienu tiesā, balstot argumentāciju uz to, ka galvenais mērķis ir smagu noziegumu izmeklēšana, atklāšana un kriminālvajāšana. Tiesa uzskatīja, ka direktīva regulē darbības, kas ir neatkarīgas no jebkuras politikas un tiesiskās sadarbības krimināllietās īstenošanas, un ar to nav saskaņota nedz valsts kompetento tiesībaizsardzības iestāžu piekļuve datiem, nedz arī datu lietošana un apmaiņa starp šīm iestādēm. Tādejādi Tiesa secināja, ka direktīva būtībā ir vērsta tieši uz operatoru

---

[10] Direktīvas 11. pants nosaka: „Direktīvas 2002/58/EK 15. pantā iekļauj šādu punktu: „1.a Šā panta 1. punkts neattiecas uz datiem, kurus Eiropas Parlamenta un Padomes Direktīva 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, konkrēti prasa saglabāt minētās direktīvas 1. panta 1. punktā paredzētajiem mērķiem"."

[11] 29. panta darba grupa jautā, vai "[datu saglabāšanas] direktīva bija domāta, lai varētu atkāpties no vispārējā pienākuma dzēst noslodzes datus, izbeidzot elektronisko komunikāciju, vai, lai uzliktu par pienākumu pakalpojumu sniedzējiem saglabāt visus tos datus, kurus tie jau ir tiesīgi glabāt saviem uzņēmējdarbības nolūkiem."

darbībām iekšējā tirgus attiecīgajā nozarē. Attiecīgi, tā apstiprināja direktīvas juridisko pamatu[12].

3.3. Datu saglabāšana

Datu saglabāšana atšķiras no datu operatīvas saglabāšanas (pazīstama arī kā „ātrā iesaldēšana"), saskaņā ar kuru operatoriem, kuriem izsniegts tiesas rīkojums, ir pienākums saglabāt datus saistībā tikai ar konkrētām personām, kuras tiek turētas aizdomās par noziedzīgu darbību, sākot no operatīvās saglabāšanas rīkojuma datuma. Datu operatīvā saglabāšana ir viens no izmeklēšanas instrumentiem, ko paredz un lieto Eiropas Padomes Konvencijas par kibernoziegumiem dalībvalstis[13]. Gandrīz visas konvencijas dalībvalstis ir izveidojušas kontaktpunktu, kura loma ir nodrošināt tūlītēja atbalsta sniegšanu kibernoziegumu izmeklēšanā vai tiesvedībā. Tomēr šķiet, ka ne visas konvencijas puses ir nodrošinājušas datu operatīvo saglabāšanu, un vēl līdz šim nav izvērtēts, cik efektīvs šis modelis ir kibernoziegumu apkarošanā[14]. Nesen ir izstrādāts jauns datu operatīvās saglabāšanas veids, pazīstams kā „ātrā iesaldēšana plus". Šis modelis ir plašāks par parasto datu operatīvās saglabāšanas modeli, paredzot, ka tiesnesis var piešķirt piekļuvi arī datiem, kurus operatori vēl nav dzēsuši. Tāpat ir paredzams, ka likums ļoti retos gadījumos pieļaus izņēmumu attiecībā uz pienākumu dzēst, uz īsu brīdi, konkrētus komunikāciju datus, kurus parasti neglabā, piemēram, atrašanās vietas un interneta savienojuma datus, dinamiskās IP adreses lietotājiem, kuri abonē pakalpojumu pēc vienotas likmes, kā arī, ja datus nav jāsaglabā, lai sagatavotu rēķinu.

Tās puses, kuras aizstāv datu operatīvo saglabāšanu, uzskata, ka tā mazāk aizskar privāto dzīvi, nekā datu saglabāšana. Tomēr vairākums dalībvalstu uzskata, ka neviens no datu operatīvās saglabāšanas veidiem nevar atbilstīgi aizstāt datu saglabāšanu, norādot, ka pretstatā datu saglabāšanai, kuras rezultātā ir pieejami arī vēsturiski dati, datu operatīvā saglabāšana negarantē iespēju konstatēt pierādījumu pēdas pirms operatīvās saglabāšanas rīkojuma izdošanas, kā arī neļauj iegūt pierādījumus par, piemēram, nozieguma upuru vai liecinieku kustību[15].

4. DATU SAGLABĀŠANAS DIREKTĪVAS TRANSPONĒŠANA

Dalībvalstīm prasīja, lai tās transponē direktīvu ne vēlāk kā līdz 2007. gada 15. septembrim, ar iespēju līdz 2009. gada 15. martam atlikt pienākumu piemērošanu attiecībā uz interneta piekļuves, interneta e-pasta un interneta telefonijas datu saglabāšanu.

Turpmākā analīze ir pamatota uz ziņojumiem par transponēšanu, ko Komisija ir saņēmusi no 25 dalībvalstīm, tostarp Beļģijas, kura direktīvu ir transponējusi tikai daļēji[16]. Austrijā un

---

12 EKT, C-301/6 Īrija pret Eiropas Parlamentu un Padomi, ECR [2009] I-00593.

13 Konvencijas par kibernoziegumiem 16. pants (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Avots: Eiropas Padome.

15 To atzina arī Vācijas Federālā konstitūcijas tiesa savā spriedumā, ar kuru atcēla Vācijas likumu, ar kuru transponēja direktīvu (skatīt 4.9. nodaļu) (Bundesverfassungsgericht, 1 BvR 256/08, 2010. gada 2. marts, 208. punkts).

16 Divdesmit piecas dalībvalstis, kuras ir paziņojušas Komisijai par direktīvas transponēšanu, ir: Beļģija, Bulgārija, Čehija, Dānija, Vācija, Grieķija, Igaunija, Īrija, Spānija, Francija, Itālija, Kipra, Latvija,

Zviedrijā tiesību akta projekts ir iesniegts apspriešanai. Šajās divās dalībvalstīs nepastāv pienākums saglabāt datus, bet tiesībaizsardzības iestādes var pieprasīt, arī pieprasa un iegūst noslodzes datus no operatoriem tādā mērā, kādā šie dati ir pieejami. Pēc sākotnējā Čehijas Republikas, Vācijas un Rumānijas paziņojuma par direktīvas transponēšanu šo divu dalībvalstu konstitucionālās tiesas anulēja vietējos tiesību aktus, ar kuriem transponēja direktīvu[17], un tagad šīs dalībvalstis apsver, kā vēlreiz transponēt direktīvu.

Šajā iedaļā analizēts, kā dalībvalstis transponējušas attiecīgos direktīvas noteikumus. Šeit analizēts arī tas, vai dalībvalstis ir izvēlējušās atlīdzināt operatoriem izdevumus, kas radušies datu saglabāšanas un izguves atļaušanas rezultātā (šis jautājums direktīvā nav regulēts), kā arī apskatīts, cik būtiski direktīvai ir Vācijas, Rumānijas un Čehijas Republikas konstitucionālo tiesu spriedumi.

4.1. Datu saglabāšanas nolūks (1. pants)

Direktīva nosaka dalībvalstīm pienākumu pieņemt pasākumus, lai nodrošinātu, ka dati ir saglabāti un pieejami smagu noziegumu, kas katrā dalībvalstī noteikti tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem. Tomēr vēl aizvien ES valstu tiesību aktos minētie mērķi saistībā ar datu saglabāšanu un/vai piekļuvi datiem ir atšķirīgi. Desmit dalībvalstis (Bulgārija, Igaunija, Īrija, Grieķija, Spānija, Lietuva, Luksemburga, Ungārija, Nīderlande, Somija) terminu „smags noziegums" ir definējušas ar atsauci uz minimālo brīvības atņemšanas sodu, uz iespēju saņemt nosacītu sodu vai uz tādu noziedzīgu nodarījumu sarakstu, kuri definēti citos valstu tiesību aktos. Astoņas dalībvalstis (Beļģija, Dānija, Francija, Itālija, Latvija, Polija, Slovākija, Slovēnija) pieprasa, lai datus saglabā ne tikai saistībā ar smagu noziegumu izmeklēšanu, atklāšanu un kriminālvajāšanu, bet arī saistībā ar visiem noziedzīgiem nodarījumiem un noziedzības novēršanu, vai uz vispārēja nacionālās vai valsts un/vai sabiedrības drošības pamata. Četru dalībvalstu (Kipra, Malta, Portugāle, Apvienotā Karaliste) tiesību akti atsaucas uz „smagu noziegumu" vai „smagu pārkāpumu", to vispār nedefinējot. Sīkāka informācija ir atspoguļota 1. tabulā.

1. tabula: valstu tiesību aktos minētie datu saglabāšanas nolūka ierobežojumi	
Beļģija	Noziedzīgu nodarījumu izmeklēšanai un kriminālvajāšanai, avārijas dienestu tālruņa numuru ļaunprātīgas izmantošanas kriminālvajāšanai, elektronisko komunikāciju tīklu vai pakalpojumu ļaunprātīgas izmantošanas izmeklēšanai, lai izlūkdienesti un drošības dienesti varētu veikt izlūkdatu vākšanas operācijas[18].
Bulgārija	Smagu noziegumu un noziegumu, kuri minēti Krimināl kodeksa 319a. līdz 319f. pantā, atklāšanai un izmeklēšanai, kā arī personu meklēšanai[19].

Lietuva, Luksemburga, Ungārija, Malta, Nīderlande, Polija, Portugāle, Rumānija, Slovēnija, Slovākija, Somija un Apvienotā Karaliste. Beļģija informēja Komisiju, ka tiesību akta projekts, ar kuru ir plānots pabeigt transponēšanu, vēl aizvien atrodas apspriešanā parlamentā.

[17] Rumānijas Konstitucionālās tiesas 2009. gada 8. oktobra lēmums Nr. 1258, Rumānijas oficiālais izdevums Nr. 789, 2009. gada 23. novembris; Vācijas Konstitucionālās tiesas 2010. gada 2. marta spriedums 1 BvR 256/08; 2011. gada 1. aprīļa oficiālais izdevums, Čehijas Konstitucionālas tiesas 22. marta spriedums par 97. iedaļas 3. un 4. punktu Aktā Nr. 127/2005 Coll. par elektronisko komunikāciju un citu saistītu aktu grozījumiem un Dekrētā Nr. 485/2005 Coll. par datu saglabāšanu un nosūtīšanu kompetentajām iestādēm.

[18] 2005. gada 13. jūnija Likuma par elektroniskajām komunikācijām 126. panta 1. punkts. .

[19] 2010. gada Elektronisko komunikāciju likuma (grozīts) 250a. panta 2. punkts.

1. tabula: valstu tiesību aktos minētie datu saglabāšanas nolūka ierobežojumi	
Čehijas Republika	Nav transponēta.
Dānija	Noziedzīgu darbību izmeklēšanai un saukšanai pie atbildības par tām[20].
Vācija	Nav transponēta.
Igaunija	Var izmantot, ja pierādījumu iegūšana ar citām procesuālām darbībām ir neiespējama vai īpaši sarežģīta, bet kriminālās tiesvedības objekts ir noziedzīgs nodarījums [pirmās pakāpes vai otrās pakāpes noziedzīgs nodarījums, kas izdarīts ar nolūku, ar piemērojamo sodu – brīvības atņemšanu uz laiku, sākot no trim gadiem][21].
Īrija	Lai novērstu smagus pārkāpumus [t.i., pārkāpumus, par kuriem piemērojamais soda mērs ir brīvības atņemšana uz laiku līdz 5 gadiem un vairāk, vai pārkāpums, kas paredzēts transponētajā likumā], aizsargātu valsts drošību, glābtu cilvēka dzīvību[22].
Grieķija	Lai atklātu īpaši smagus noziegumus[23].
Spānija	Krimināl kodeksā vai īpašos krimināllikumos paredzēto smagu noziegumu atklāšanai, izmeklēšanai un kriminālvajāšanai[24].
Francija	Noziedzīgu nodarījumu atklāšanai, izmeklēšanai un kriminālvajāšanai, kā arī, lai nodrošinātu tiesu iestādes ar nepieciešamo informāciju un novērstu terorisma aktus, un aizsargātu intelektuālo īpašumu[25].
Itālija	Noziedzīgu nodarījumu atklāšanai un apkarošanai[26].
Kipra	Smagu noziedzīgu nodarījumu izmeklēšanai[27].
Latvija	Lai aizsargātu valsts un sabiedrisko drošību vai nodrošinātu noziedzīgu nodarījumu izmeklēšanu, kriminālvajāšanu un krimināllietu iztiesāšanu[28].
Lietuva	Smagu un īpaši smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai, kā noteikts Lietuvas Krimināl kodeksā[29].
Luksemburga	Noziedzīgu nodarījumu, par kuriem piemērojamais soda mērs ir brīvības atņemšana uz vienu vai vairākiem gadiem, atklāšanai, izmeklēšanai un kriminālvajāšanai[30].

20 Datu saglabāšanas rīkojuma 1. pants.
21 Kriminālprocesa kodeksa 110. panta 1. punkts.
22 2011. gada Sakaru likuma (Datu saglabāšanas likums) 6. pants.
23 Tādus noziegumus, kuri minēti 2225/1994 Likuma 4. pantā; Likuma 3917/2011 1. pants.
24 Likuma 25/2007 1. panta 1. punkts.
25 Likumi, kas regulē saglabātu datu lietošanu, attiecīgi, noziedzīgu nodarījumu nolūkiem, terorisma aktu novēršanā un intelektuālā īpašuma aizsargāšanā, ir šādi: Pants L.34-1(II), CPCE, 2006. gada 23. janvāra Likums Nr. 2006-64, 2009. gada 12. jūnija Likums Nr. 2009-669.
26 Datu aizsardzības kodeksa 132. panta 1. punkts.
27 Likuma 183(I)/2007, 4. panta 1. punkts.
28 Elektronisko sakaru likuma 71. panta 1. punkts.
29 Likuma X-1835, 65. pants.
30 2010. gada 24. jūlija Likuma 1. panta 1. punkts.

1. tabula: valstu tiesību aktos minētie datu saglabāšanas nolūka ierobežojumi	
Ungārija	Lai ļautu izmeklēšanas iestādēm, valsts prokuroram, tiesām un valsts drošības dienestiem veikt savus pienākumus un ļautu policijai un Valsts Nodokļu un muitas dienestam izmeklēt noziegumus, kas izdarīti ar nodomu, par kuriem piemērojamais soda mērs ir brīvības atņemšana uz diviem vai vairāk gadiem[31].
Malta	Smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai[32].
Nīderlande	Noziedzīgu nodarījumu, kuriem var piemērot brīvības atņemšanas sodu, izmeklēšanai un kriminālvajāšanai[33].
Austrija	Nav transponēta.
Polija	Noziegumu novēršanai un atklāšanai, finanšu noziegumu novēršanai un atklāšanai, prokuroru un tiesu lietošanai, ja tas ir būtiski gaidāmajai tiesvedībai, Iekšlietu drošības aģentūras, Ārlietu izlūkošanas aģentūras, Galvenā korupcijas apkarošanas biroja, Militāro pretizlūkošanas dienestu un Militāro izlūkošanas dienestu nolūkiem pienākumu veikšanai[34].
Portugāle	Smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai [35].
Rumānija	Nav transponēta.
Slovēnija	Lai nodrošinātu valsts drošību, konstitucionālo regulējumu un drošību, valsts politiskās un ekonomiskās intereses … un valsts aizsardzības nolūkiem[36].
Slovākija	Noziedzīgu nodarījumu izmeklēšanai, atklāšanai un kriminālvajāšanai[37].
Somija	Smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai, kā izklāstīts Piespiedu pasākumu likuma 5a. nodaļas 3. panta 1. punktā[38].
Zviedrija	Nav transponēta.
Apvienotā Karaliste	Smagu noziegumu izmeklēšanai, atklāšanai un kriminālvajāšanai [39].

Vairākums dalībvalstu, kuras transponējušas direktīvu, saskaņā ar saviem tiesību aktiem ļauj piekļūt saglabātajiem datiem un lietot tos arī tādiem nolūkiem, uz kuriem šī direktīva neattiecas, tostarp novērst un apkarot noziedzību principā, kā arī attiecībā uz dzīvības un veselības apdraudējumu. Kaut arī ir atļauts saskaņā ar E-privātuma direktīvu, tomēr šajā jomā saskaņotības līmenis, kāds panākts ar ES tiesību aktiem, ir ierobežots. Visticamāk, ka atšķirības datu saglabāšanas nolūkos ietekmēs pieprasījumu apmēru un biežumu, kas, savukārt, ietekmēs izmaksas, kas radušās, nodrošinot atbilstību direktīvā noteiktajām

31 Datu saglabāšanas vispārējiem nolūkiem Likuma C/2003 159/A. pants, kā grozīts ar Likumu CLXXIV/2007; policijas piekļuves nolūkiem Likuma XXXIV/1994 68. pants; Valsts Nodokļu un muitas dienesta piekļuves nolūkiem Likuma CXXII/2010 59. pants.

32 Tiesiskā akta 198/2008 20. panta 1. punkts.

33 Kriminālprocesa kodeksa 126. pants.

34 2004. gada 16. jūlija Telekomunikāciju likuma 180a. pants, kā grozīts ar 2009. gada 24. aprīļa Likuma 1. pantu.

35 Likuma 32/2008 1. panta 3. punkta 1. apakšpunkts.

36 Elektronisko komunikāciju likuma 170a. panta 1. punkts.

37 Elektronisko komunikāciju likuma 59a. panta 6. punkts.

38 Elektronisko komunikāciju likuma 14a. panta 1. punkts.

39 Datu saglabāšanas (EK direktīva), 2009. gada noteikumi (2009 Nr. 859).

saistībām. Turklāt šādā situācija gūtie dati var nebūt pietiekami paredzamības nodrošināšanai, kas ir jebkura tiesiska pasākuma, ar kuru tiek ierobežotas tiesības uz privāto dzīvi, prasība[40]. Komisija novērtēs vajadzību pēc lielākas saskaņotības pakāpes šajā jomā un iespējas to panākt[41].

4.2. Operatoru pienākums saglabāt datus [1. pants]

Direktīva attiecas uz „publiski pieejamu elektronisko komunikāciju pakalpojumu vai publiski pieejamu komunikāciju tīklu sniedzējiem" (1. panta 1. punkts). Divas dalībvalstis (Somija un Apvienotā Karaliste) neprasa maziem operatoriem, lai tie saglabā datus, jo uzskata, ka izmaksas, kas radīsies gan pakalpojumu sniedzējam, gan valstij, būs lielākas par labumu, ko gūs kriminālā justīcija un tiesībaizsardzība. Četras dalībvalstis (Latvija, Luksemburga, Nīderlande un Polija) ziņo, ka ir ieviesušas alternatīvus administratīvus pasākumus. Kamēr dažās dalībvalstīs esoši lieli operatori gūst labumu no apjomradītiem ietaupījumiem izmaksu ziņā, citās dalībvalstīs mazi operatori, lai samazinātu izmaksas, mēdz izveidot kopuzņēmumus vai izmantot „ārpakalpojumiem" uzņēmumus, kuri specializējas saglabāšanas un izguves darbībās. Šāda tehnisko funkciju nodošana ārpakalpojuma sniedzējiem neietekmē pakalpojumu sniedzēju pienākumu pienācīgi uzraudzīt datu apstrādes operācijas un nodrošināt nepieciešamo drošības pasākumu esamību, kas var būt problemātiski jo īpaši maziem operatoriem. Komisija pārbaudīs datu drošības jautājumus un ietekmi uz maziem un vidējiem uzņēmumiem, saistībā ar iespēju grozīt datu saglabāšanas tiesisko ietvaru.

4.3. Piekļuve datiem: iestādes, procedūras un nosacījumi (4. pants)

Dalībvalstīm prasa, lai tās „nodrošinātu, ka [saglabātie dati] īpašos gadījumos un atbilstoši attiecīgās valsts tiesību aktiem tiek paredzēti vienīgi kompetentām valsts iestādēm". Dalībvalstu pašu ziņā savos tiesību aktos ir noteikt „procedūras, kas jāievēro, un nosacījumi, kas jāizpilda, lai saņemtu piekļuvi saglabātajiem datiem atbilstīgi nepieciešamības un proporcionalitātes prasībām, ņemot vērā attiecīgus Eiropas Savienības tiesību aktus vai starptautisko publisko tiesību aktus un jo īpaši Eiropas Cilvēktiesību konvenciju, kā to ir interpretējusi Eiropas Cilvēktiesību tiesa".

Visās dalībvalstīs valsts policija un, izņemot precedenta tiesību piekritībās (Īrija un Apvienotā Karaliste), prokuratūra var piekļūt saglabātajiem datiem. Četrpadsmit dalībvalstis kā kompetentās iestādes uzskaita arī drošības un izlūkošanas dienestus vai militāros spēkus. Sešas dalībvalstis min nodokļu un/vai muitas iestādes, bet trīs dalībvalstis nosauc arī robežsardzes iestādes. Viena dalībvalsts pieļauj, ka citas valsts iestādes piekļūst datiem, ja tās ar tiesību aktiem ir īpašos nolūkos tam pilnvarotas. Vienpadsmit dalībvalstis pieprasa, lai katram saglabāto datu piekļuves pieprasījumam būtu izsniegta tiesas atļauja. Trīs dalībvalstīs vairumā gadījumu ir nepieciešama tiesas atļauja. Četrās dalībvalstīs atļauja ir jāsaņem no

---

[40] Eiropas Kopienu tiesas 2003. gada 20. maija spriedums apvienotajās lietās C-465/00, C-138/01 un C-139/01 (Atsauce uz Konstitucionālās tiesas un Augstākās tiesas *(Verfassungsgerichtshof, Oberster Gerichtshof*) iepriekšēju nolēmumu): Valsts kontrole (C-465/100) pret Austrijas radio (*Rechnungshof* (C-465/100) *v Osterreichischer Rundfunk*) un citiem un starp Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) un Austrijas radio (*Österreichischer Rundfunk*) (Personu aizsardzība attiecībā uz personas datu apstrādi – Direktīva 95/46/EK – Privātās dzīves aizsardzība – Datu izpaušana par to darbinieku ienākumiem, kuri strādā Valsts kontroles pakļautībā esošās iestādēs).

[41] Par direktīvas pieņemšanu Komisija izdeva deklarāciju, kurā ierosināja, ka ir jāapsver Eiropas apcietināšanas orderī minēto noziegumu saraksts (Padomes 2002. gada 13. jūnija Pamatlēmums 2002/584/TI par Eiropas apcietināšanas orderi un par nodošanas procedūrām starp dalībvalstīm).

augstākas iestādes, bet nevis no tiesneša. Divās dalībvalstīs, šķiet, vienīgais nosacījums ir, lai pieprasījums būtu rakstisks.

2. tabula: piekļuve saglabātajiem telekomunikāciju datiem		
	Kompetentās valsts iestādes	*Procedūras un nosacījumi*
Beļģija	Tiesu koordinēšanas vienība, izmeklēšanas tiesneši, valsts prokurors, kriminālpolicija.	Piekļuvi atļauj tiesnesis vai prokurors. Pēc pieprasījuma operatoriem abonenta dati un noslodzes dati, un atrašanās vietas dati par zvaniem, kas veikti pēdējā mēneša laikā, jāsniedz „reālā laikā". Datus par vecākiem zvaniem iesniedz pēc iespējas ātrāk.
Bulgārija[42]	Nacionālās drošības valsts aģentūras īpaši direktorāti un departamenti, Iekšlietu ministrija, Militārās informācijas dienests, Militārās policijas dienests, Aizsardzības ministrs, Valsts izmeklēšanas aģentūra, tiesa un pirmstiesas iestādes pie noteiktiem nosacījumiem.	Piekļuve iespējama tikai ar apgabala tiesas priekšsēdētāja rīkojumu.
Čehijas Republika	Nav transponēta.	
Dānija[43]	Policija.	Piekļuvi piešķir ar tiesas atļauju; tiesas rīkojumus piešķir, ja pieteikums atbilst stingriem kritērijiem par aizdomām, nepieciešamību un proporcionalitāti.
Vācija	Nav transponēta	
Igaunija[44]	Policijas un Robežsardzes pārvalde, Drošības policijas pārvalde un, attiecībā uz priekšmetiem un elektronisko komunikāciju, Nodokļu un muitas pārvalde.	Piekļuvi atļauj iepriekšējas izmeklēšanas tiesnesis. Operatori steidzamos gadījumos „sniedz [saglabātos datus] ne vēlāk kā 10 stundās, pārējos gadījumos 10 darba dienās [pēc pieprasījuma saņemšanas]".
Īrija[45]	Garda Síochána (policija) biedri ar galvenā superintendanta vai augstāku pakāpi. Pastāvīgo aizsardzības spēku virsnieki ar pulkveža vai augstāku pakāpi. Ieņēmumu komisāri-amatpersonas ar galvenās amatpersonas vai augstāku pakāpi.	Pieprasījumiem jābūt rakstiskiem.
Grieķija[46]	Tiesu, militārās vai policijas valsts iestādes.	Piekļuvei nepieciešams tiesu iestādes lēmums par to, ka izmeklēšana ar citiem līdzekļiem ir neiespējama vai ārkārtīgi sarežģīta
Spānija[47]	Policija, kas atbildīga par smagu noziegumu atklāšanu, izmeklēšanu un kriminālvajāšanu, Nacionālais izmeklēšanas centrs un Muitas aģentūra.	Lai kompetentās valsts iestādes piekļūtu šiem datiem, nepieciešama iepriekšēja tiesu atļauja.
Francija[48]	Valsts prokurori, norīkoti policijas virsnieki un žandarmi.	Par katru pieprasījumu pēc piekļuves saglabātajiem datiem policijai ir jāsniedz pamatojums un jācenšas iegūt atļauja no

42 2010. gada Elektronisko komunikāciju likuma (grozīts) 250b. panta 1. punkts (iestādes); 2010. gada Elektronisko komunikāciju likuma (grozīts) 250b. panta 2. punkts (piekļuve) .

43 Tiesvedības akta 71. nodaļa.

44 Kriminālprocesa kodeksa 112. panta 2. un 3. punkts (par iestādēm un procedūru); Elektronisko komunikāciju likuma 111. panta 9. punkts (nosacījumi).

45 2009. gada Sakaru likuma (Datu saglabāšanas likums) 6. pants.

46 Likuma 2225/94 3. un 4. pants.

47 Likuma 25/2007 6. un 7. pants.

2. tabula: piekļuve saglabātajiem telekomunikāciju datiem		
Kompetentās valsts iestādes		*Procedūras un nosacījumi*
		amatpersonas Iekšlietu ministrijā, kuru iecēlusi Nacionālā drošības kontroles komisija (Commission nationale de contrôle des interceptions de sécurité). Pieprasījumus piekļuvei apstrādā iecelta amatpersona, kura strādā pie operatora.
Itālija[49]	Valsts prokurors; policija; aizstāvības advokāts vai nu atbildētājam, vai personai, pret kuru uzsākta izmeklēšana.	Piekļuvei nepieciešams „pamatots rīkojums", ko izdevis valsts prokurors.
Kipra[50]	Tiesas, valsts prokurors, policija.	Piekļuvi apstiprina prokurors, ja uzskata, ka tādejādi var iegūt pierādījumus par smaga nozieguma izdarīšanu. Tiesnesis var izdot šādu rīkojumu, ja pastāv pamatotas aizdomas, ka ir izdarīts smags noziedzīgs nodarījums un dati varētu būt ar to saistīti.
Latvija[51]	Pilnvarotas amatpersonas pirmstiesas izmeklēšanas iestādēs; personas, kuras veic izmeklēšanas darbības; valsts drošības iestāžu pilnvaroti darbinieki; Prokuratūra; tiesa.	Pilnvarotām amatpersonām, valsts prokuratūrai un tiesām ir jāizvērtē pieprasījuma „atbilstība un būtiskums", jāpiereģistrē pieprasījums un jānodrošina iegūto datu aizsardzība. Pilnvarotas iestādes var parakstīt vienošanos ar operatoru, piemēram, par sniegto datu šifrēšanu.
Lietuva[52]	Pirmstiesas izmeklēšanas iestādes, prokurors, tiesa (tiesneši) un izlūkošanas amatpersonas.	Pilnvarotām valsts iestādēm rakstiski jāpieprasa saglabātie dati. Lai piekļūtu pirmstiesas izmeklēšanas datiem, ir nepieciešams tiesu orderis.
Luksemburga[53]	Tiesu iestādes (izmeklēšanas tiesneši, prokurors), iestādes, kas atbildīgas par valsts drošības sargāšanu, aizsardzību, valsts drošību un noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu.	Piekļuvei nepieciešama tiesu atļauja.
Ungārija[54]	Policija, Valsts nodokļu un muitas dienests, valsts drošības dienesti, valsts prokurors, tiesas.	Policijai un Valsts Nodokļu un muitas dienestam ir nepieciešama prokurora atļauja. Prokurors un valsts drošības aģentūras var piekļūt šādiem datiem bez tiesas rīkojuma.
Malta[55]	Maltas policija; Drošības dienests.	Pieprasījumiem jābūt rakstiskiem.
Nīderlande[56]	Izmeklēšanas policijas amatpersona.	Piekļuvi atļauta ar prokurora vai izmeklēšanas tiesneša rīkojumu.
Austrija	Nav transponēta	

48 Kriminālprocesa kodeksa 60. panta 1. un 2. punkts (iestādes); L.31-1-1. pants (nosacījumi).

49 Datu aizsardzības kodeksa 132. panta 3. punkts.

50 Likuma 183(I)/2007 4. panta 2. punkts un 4. panta 4. punkts.

51 Elektronisko sakaru likuma 71. panta 1. punkts (iestādes). Ministru Kabineta noteikumi Nr. 820 (procedūras).

52 Likuma X-1835 77. panta 1. un 2. punkts; mutisks ziņojums Komisijai.

53 2010. gada 24. jūlija Likuma (iestādes) 5. panta 2. punkta 1) apakšpunkts un 9. panta 2. punkts; Kriminālprocesa kodeksa 67. panta 1. punkts (nosacījumi).

54 1994. gada Likuma XXXIV 68. panta 1. punkts un 69. panta 1. punkta c) un d) apakšpunkts; 1972. gada Likuma V 9/A. panta 1. punkts; 1998. gada Likuma XIX 71. panta 1., 3. un 4. punkts, 178/A. panta 4. punkts, 200., 201. pants un 268. panta 2. punkts; 1995. gada Likuma CXXV 40. panta 1. un 2. punkts, 53. panta 1. punkts, 54. panta 1. punkta j) apakšpunkts.

55 Tiesiskā akta 198/2008 20. panta 1. un 3. punkts.

56 Kriminālprocesa kodeksa 126ni. pants.

2. tabula: piekļuve saglabātajiem telekomunikāciju datiem		
	Kompetentās valsts iestādes	*Procedūras un nosacījumi*
Polija[57]	Policija, robežsargi, nodokļu inspektori, Iekšējās drošības aģentūra, Ārlietu izlūkošanas aģentūra, Galvenais korupcijas apkarošanas birojs, Militārie pretizlūkošanas dienesti, Militārie izlūkošanas dienesti, tiesas un valsts prokurors.	Pieprasījumiem jābūt rakstiskiem un, attiecībā uz policiju, robežsargiem, nodokļu inspektoriem, pieprasījumus jāapstiprina organizācijas vecākajai amatpersonai.
Portugāle[58]	Kriminālpolicija, Republikas Nacionālā gvarde, Valsts drošības birojs, Militārā kriminālpolicija, Imigrācijas un robežsardzes departaments, Jūras policija.	Datu nosūtīšanai nepieciešama tiesu atļauja, pamatojoties uz to, ka piekļuve ir izšķiroša, lai atklātu patiesību vai, ka pierādījumus jebkurā citā veidā būs neiespējami vai ārkārtīgi grūti iegūt. Tiesu atļaujai jābūt saskaņā ar nepieciešamības un proporcionalitātes prasībām.
Rumānija	Nav transponēta	
Slovēnija[59]	Policija, izlūkošanas un drošības aģentūras, aizsardzības aģentūras, kas atbildīgas par izlūkošanu un pretizlūkošanu, un drošības misijām.	Piekļuvei nepieciešama tiesu atļauja.
Slovākija[60]	Tiesībaizsardzības iestādes, tiesas.	Pieprasījumiem jābūt rakstiskiem.
Somija[61]	Policija, robežsardze, muitas iestādes (saglabātiem abonenta, noslodzes un atrašanās vietas datiem). Ārkārtas reaģēšanas centrs, Jūras glābšanas dienests, Jūras glābšanas apakšcentrs (identifikācijas un atrašanās vietas datiem ārkārtas situācijās).	Abonenta datiem var piekļūt visas kompetentās iestādes bez tiesu atļaujas Pārējiem datiem nepieciešams tiesas rīkojums.
Zviedrija	Nav transponēta	
Apvienotā Karaliste[62]	Policija, izlūkošanas dienesti, nodokļu un muitas iestādes, citas valsts iestādes, kas ieceltas šim nolūkam saskaņā ar sekundāriem tiesību aktiem.	Piekļuve atļauta, ja „ieceltā persona" to ir atļāvusi un ir veikta nepieciešamības un proporcionalitātes pārbaude, noteiktos gadījumos un apstākļos, kuros datu izpaušanu atļauj vai pieprasa ar likumu. Par īpašām procedūrām vienojas ar operatoriem.

Komisija izvērtēs vajadzību pēc lielākas saskaņotības pakāpes attiecībā uz iestādēm, kurām ir piekļuve saglabātajiem datiem un procedūrām šo datu iegūšanai, un iespējas to panākt. Šīs iespējas varētu ietvert skaidri noteiktus kompetento iestāžu sarakstus, neatkarīgu un/vai tiesisku datu pieprasījumu pārskatu un obligātos procedūru standartus operatoriem attiecībā uz piekļuves atļaušanu kompetentām iestādēm.

---

57 2004. gada 16. jūlija Telekomunikāciju likuma 179. panta 3. punkts, kā grozīts ar 2009. gada 24. aprīļa Likuma 1. pantu.

58 Likuma 32/2008 2. panta 1. punkts, 3. panta 2. punkts un 9. pants.

59 Elektronisko komunikāciju likuma 107c. pants; Kriminālprocesa kodeksa 149b. pants; Izlūkošanas un drošības aģentūras likuma 24. panta b) apakšpunkts; Aizsardzības likuma 32. pants.

60 Elektronisko komunikāciju likuma 59a. panta 8. punkts.

61 Elektronisko komunikāciju likuma 35. panta 1. punkts un 36. pants; Likuma par policiju 31.-33. pants; Robežsardzes likuma 41. pants.

62 2000. gada Izmeklēšanas pilnvaru likuma noteikumu 1. saraksta 25. pants; Datu saglabāšanas regulas 7. pants. Izmeklēšanas pilnvaru likuma noteikumu 22. panta 2. punkts nosaka nolūkus, kādiem šīs iestādes var iegūt datus.

4.4. Datu saglabāšanas direktīvas darbības joma un aptverto datu kategorijas (1. panta 2. punkts, 3. panta 2. punkts un 5. pants)

Direktīva attiecas uz fiksētā tīkla telefonijas, mobilās telefonijas, interneta piekļuves, interneta e-pasta un interneta telefonijas jomām. Tā nosaka (5. pantā) saglabājamo datu kategorijas, proti, tādu datu, kas vajadzīgi, lai identificētu un noteiktu:

(a) komunikācijas avotu;

(b) komunikācijas galamērķi;

(c) komunikācijas datumu, laiku un ilgumu;

(d) komunikācijas veidu;

(e) lietotāja komunikāciju aprīkojumu vai aprīkojumu, kas veic tā funkcijas; un

(f) mobilo sakaru iekārtas atrašanās vietu.

Tā attiecas arī uz (3. panta 2. punkts) neveiksmīgu izsaukuma mēģinājumu, tas ir, komunikāciju, ja tālruņa izsaukuma rezultātā veiksmīgi ir noticis savienojums, bet tas nav atbildēts vai notikusi tīkla pārvaldības iejaukšanās, kā arī kad datus par šiem mēģinājumiem ir ieguvuši vai apstrādājuši un uzglabājuši vai reģistrējuši operatori. Saskaņā ar direktīvu nedrīkst saglabāt datus, kas atklāj komunikācijas saturu. Tāpat ir kļuvis skaidrs, ka direktīva neattiecas arī uz meklēšanas jautājumu datiem, tas ir, servera ierakstiem, kas radīti, piedāvājot meklēšanas rīku pakalpojumus, jo tos drīzāk uzskata nevis par noslodzes datiem, bet par satura datiem[63].

Divdesmit viena dalībvalsts savos transponēšanas tiesību aktos ir paredzējušas katras šīs datu kategorijas saglabāšanu. Beļģija nav paredzējusi ne telefonijas datu veidu, ne ar internetu saistītu datu saglabāšanu. Tās dalībvalstis, kuras atbildēja uz Komisijas aptauju, neuzskatīja par vajadzīgi grozīt saglabājamo datu kategorijas, lai gan Eiropas Parlaments bija izsniedzis Komisijai rakstisku deklarāciju ar prasību paplašināt direktīvas darbības jomu attiecībā uz meklēšanas rīkiem „lai steidzīgi risinātu tiešsaistes bērnu pornogrāfijas un seksuālo pārkāpumu problēmas”[64]. Savā ziņojumā par otro izpildu rīcību 29. pantā minētā Darba grupa skaidroja, ka datu direktīvā noteiktās kategorijas ir jāuzskata par izsmeļošām un operatori nav jāapgrūtina ar papildu datu saglabāšanas pienākumiem. Komisija izvērtēs nepieciešamība pēc visām šīm datu kategorijām.

4.5. Saglabāšanas termiņi (6. un 12. pants)

Dalībvalstīm prasa, lai tās nodrošina, ka 5. pantā norādītās datu kategorijas saglabā laiku, kas ir ne mazāks kā seši mēneši un ne ilgāks kā divi gadi no komunikācijas datuma. Dalībvalsts, kurai „īpaši apstākļi nosaka, ka maksimālais saglabāšanas periods uz ierobežotu laiku jāpagarina”, drīkst to darīt; par šādu pagarinājumu dalībvalsts nekavējoties paziņo Komisijai,

---

63 29. panta Darba grupas 2008. gada 4. aprīļa atzinums par datu aizsardzības jautājumiem saistībā ar meklēšanas rīkiem.

64 Rakstiska deklarācija saskaņā ar Reglamenta par Eiropas Agrā brīdinājuma sistēmas (EABS) izveidi cīņai pret pedofiliem un citiem dzimumnoziedzniekiem 123. noteikums, 19.4.2010, 0029/2010.

kura sešu mēnešu termiņā pēc šī paziņojuma var lemt par šī pagarinājuma apstiprināšanu vai noraidīšanu. Kaut arī maksimālo saglabāšanas periodu var pagarināt, nav noteikumu, kā saīsināt saglabāšanas periodu, padarot to īsāku par sešiem mēnešiem. Visas dalībvalstis, izņemot vienu, kuras ir transponējušas direktīvu, piemēro šo saglabāšanas termiņu vai termiņus norādītajās robežās; Komisijai nav iesniegts neviens paziņojums par pagarinājumu. Tomēr vienotas pieejas visā ES nav.

Piecpadsmit dalībvalstis norāda vienu saglabāšanas termiņu visām datu kategorijām: viena dalībvalsts (Polija) norāda divu gadu saglabāšanas termiņu, viena norāda 1,5 gadus (Latvija), desmit norāda vienu gadu (Bulgārija, Dānija, Igaunija, Grieķija, Spānija, Francija, Nīderlande, Portugāle, Somija, Apvienotā Karaliste) un trīs dalībvalstis norāda sešus mēnešus (Kipra, Luksemburga, Lietuva). Piecas dalībvalstis ir noteikušas dažādus saglabāšanas termiņus dažādām datu kategorijām: divas dalībvalstis (Īrija, Itālija) fiksētās un mobilās telefonijas datiem norāda divu gadu termiņu un interneta piekļuves, interneta e-pasta un interneta telefonijas datiem – vienu gadu; viena dalībvalsts (Slovēnija) norāda 14 mēnešus telefonijas datiem un astoņus mēnešus ar internetu saistītiem datiem; viena dalībvalsts (Slovākija) fiksētai un mobilai telefonijai norāda viena gada termiņu, bet ar internetu saistītiem datiem – sešus mēnešus; viena dalībvalsts (Malta) norāda vienu gadu fiksētās, mobilās un interneta telefonijas datiem un sešus mēnešus interneta piekļuvei un interneta e-pastam. Viena dalībvalsts (Ungārija) visus datus saglabā vienu gadu, izņemot neveiksmīga izsaukuma mēģinājuma datus, kurus saglabā tikai sešus mēnešus. Viena dalībvalsts (Beļģija) nav norādījusi nevienu konkrētu datu saglabāšanas termiņu datu kategorijām, kuras noteiktas direktīvā. Sīkāka informācija atspoguļota 3. tabulā.

3. tabula: valstu tiesību aktos norādītie saglabāšanas termiņi	
Beļģija[65]	1 gads līdz 36 mēneši „publiski pieejamu" tālruņu pakalpojumiem Neviens noteikums neattiecas uz ar internetu saistītiem datiem.
Bulgārija	1 gads. Pēc pieprasījuma datus, kuriem ir piekļūts, var saglabāt vēl 6 mēnešus
Čehijas Republika	Nav transponēta.
Dānija	1 gads
Vācija	Nav transponēta
Igaunija	1 gads
Īrija	2 gadi fiksētās telefonijas un mobilās telefonijas datiem, 1 gads interneta piekļuves, interneta e-pasta un interneta telefonijas datiem
Grieķija	1 gads
Spānija	1 gads
Francija	1 gads
Itālija	2 gadi fiksētās telefonijas un mobilās telefonijas datiem, 1 gads interneta piekļuves, interneta e-pasta un interneta telefonijas datiem
Kipra	6 mēneši
Latvija	18 mēneši
Lietuva	6 mēneši
Luksemburga	6 mēneši
Ungārija	6 mēneši neveiksmīga izsaukuma mēģinājumiem un 1 gads visiem pārējiem datiem
Malta	1 gads fiksētās telefonijas, mobilās un interneta telefonijas datiem, 6 mēneši interneta piekļuves un interneta e-pasta datiem
Nīderlande	1 gads

[65] 2005. gada 13. jūnija Likuma par elektroniskajām komunikācijām 126. panta 2. punkts.

3. tabula: valstu tiesību aktos norādītie saglabāšanas termiņi	
Austrija	Nav transponēta
Polija	2 gadi
Portugāle	1 gads
Rumānija	Nav transponēta (6 mēneši saskaņā ar agrāk atcelto transponēšanas likumu)
Slovēnija	14 mēneši telefonijas datiem un 8 mēneši ar internetu saistītiem datiem
Slovākija	1 gads fiksētās telefonijas un mobilās telefonijas datiem, 6 mēneši interneta piekļuves, interneta e-pasta un interneta telefonijas datiem
Somija	1 gads
Zviedrija	Nav transponēta
Apvienotā Karaliste	1 gads

Lai gan šādu daudzveidīgu pieeju direktīva atļauj, no tā izriet, ka direktīva operatoriem, kuri darbojas vairāk nekā vienā dalībvalstī, un pilsoņiem, kuru komunikāciju datus var uzglabāt dažādās dalībvalstīs, ES līmenī nodrošina tikai ierobežotu tiesisko noteiktību un paredzamību. Ņemot vērā pieaugošo datu apstrādes internacionalizāciju, ārpakalpojumu izmantošanu datu uzglabāšanai un izkaisīto datu apstrādi, ir jāapsver iespējas vairāk saskaņot datu uzglabāšanas termiņus ES. Lai nodrošinātu atbilstību proporcionalitātes principam un, ņemot vērā skaitliskos pierādījumus un pierādījumus pēc būtības par saglabāto datu vērtību dalībvalstīs, kā arī jaunākās tendences komunikāciju un tehnoloģiju, kā arī noziedzības un terorisma jomā, Komisija apsvērs iespēju dažādām datu kategorijām un dažādām smagu noziegumu kategorijām, vai šo abu jēdzienu apvienojumam, piemērot dažādus termiņus[66]. Dalībvalstu līdz šim sniegtie skaitliskie pierādījumi par saglabāto datu vecumu, vedina domāt, ka aptuveni 90 % datu ir sešus mēnešus veci vai jaunāki un aptuveni 70 % datu ir trīs mēnešus veci vai jaunāki, kad tiesībaizsardzības iestādes izdara (sākotnējo) pieprasījumu. (sk. 5.2. iedaļu).

4.6. Datu aizsardzība un datu drošība, un uzraudzības iestādes (7. un 9. pants)

Direktīva prasa, lai dalībvalstis nodrošina, ka operatori attiecībā uz saglabājamiem datiem ievēro vismaz šādus četrus datu drošības principus, proti:

(a) saglabājamiem datiem ir tāda pati kvalitāte, un tiem piemēro tādus pašus drošības un aizsardzības noteikumus kā datiem [publisko komunikāciju] tīklā;

(b) attiecībā uz datiem īsteno atbilstīgus tehniskos un organizatoriskos pasākumus, lai aizsargātu tos pret nejaušu vai nelikumīgu iznīcināšanu, zudumu vai pārveidošanu vai neatļautu vai nelikumīgu saglabāšanu, apstrādi, piekļuvi vai izpaušanu;

(c) attiecībā uz datiem īsteno atbilstīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu, ka tie ir pieejami tikai īpaši pilnvarotiem darbiniekiem; un

(d) visus datus, izņemot tos, kuriem ir piekļūts un kuri ir rezervēti, saglabāšanas termiņa beigās iznīcina [šīs direktīvas nolūkiem].

[66] Komisijas priekšlikums direktīvai par datu saglabāšanu 2005. gadā paredzēja viena gada saglabāšanas termiņu telefonijas datiem un sešu mēnešu saglabāšanas termiņu interneta datiem.

Atbilstoši Datu aizsardzības direktīvai un E-privātuma direktīvai operatori nedrīkst apstrādāt datus, kas saglabāti saskaņā ar šo direktīvu citiem nolūkiem, ja citādi šie dati nebūtu saglabāti[67]. Dalībvalstīm prasa iecelt valsts iestādi, kura pilnīgi neatkarīgi ir atbildīga par šo principu piemērošanas uzraudzību; šīs iestādes var būt tās pašas iestādes, kuras nepieciešamas saskaņā ar Datu aizsardzības direktīvu[68].

Piecpadsmit dalībvalstis attiecīgajos tiesību aktos ir transponējušas visus šos principus. Četras dalībvalstis (Beļģija, Igaunija, Spānija, Latvija) ir transponējušas divus vai trīs no šiem principiem, bet skaidri neparedz datu iznīcināšanu saglabāšanas termiņa beigās. Divas dalībvalstis (Itālija, Somija) paredz datu iznīcināšanu. Nav skaidrs, kuri konkrētie tehniskie un organizatoriskie drošības pasākumi, piemēram, spēcīga autentificēšana un detalizēta piekļuves reģistrēšanas pārvaldība[69], ir piemēroti. Divdesmit divām dalībvalstīm ir uzraudzības iestāde, kas atbildīga par principu piemērošanas uzraudzību. Vairākumā gadījumu tā ir datu aizsardzības iestāde. Sīkāka informācija atspoguļota 4. tabulā.

4. tabula: Datu aizsardzība un datu drošība, un uzraudzības iestādes		
Dalībvalsts	*Datu aizsardzības un datu drošības noteikumi valstu tiesību aktos*	*Uzraudzības iestāde*
Beļģija	Operatoriem jānodrošina, ka datu pārraidi nevar pārtver trešās personas, kā arī operatoriem jāievēro Eiropas Telekomunikāciju standartu institūta telekomunikāciju drošības un likumīgas pārtveršanas standarti[70]. Nešķiet, ka ir ieviests princips par obligāto datu iznīcināšanu pēc saglabāšanas termiņa beigām.	Pasta pakalpojumu un telekomunikāciju institūts uzrauga, kā operatori ievēro datu saglabāšanas juridiskās saistības.
Bulgārija	Transponēšanas likumā ietverta prasība īstenot četrus principus[71].	Personas datu aizsardzības komisija uzrauga datu apstrādi un uzglabāšanu, lai nodrošinātu atbilstību saistībām. Nacionālās asamblejas parlamentārā komisija uzrauga datu piekļuves piešķiršanas un datu piekļuves procedūras
Čehijas Republika[72].	Nav transponēta.	
Dānija	Ir paredzēti visi četri principi[73].	Valsts IT un Telekomunikāciju aģentūra uzrauga elektronisko komunikāciju tīklu un pakalpojumu sniedzēju pienākumu nodrošināt, ka tehniskais aprīkojums un sistēmas nodrošina policijai piekļuvi informācijai par telekomunikāciju datu plūsmu.
Vācija	Nav transponēta.	

67 Direktīvas 95/46/EK 13. panta 1. punkts.

68 Direktīvas 95/46/EK 28. pants.

69 Spēcīga autentificēšana ietver divkāršas autentificēšanas mehānismus, piemēram, parole plus biometrija vai parole plus marķierierīce, lai nodrošinātu personas, kura atbildīga par noslodzes datu apstrādi, fizisko klātbūtni. Detalizēta piekļuves reģistrēšanas pārvaldība ietver detalizētu piekļuves un apstrādes darbību izsekošanu, saglabājot reģistrus, kuros norādīta lietotāja identitāte, piekļuves laiks un dokumenti, kuriem piekļūts.

70 2003. gada 9. janvāra Karaliskā dekrēta 6. pants.

71 2010. gada Elektronisko komunikāciju likuma (grozīts) 4. panta 1. punkts.

72 Likuma 127/2005 87. panta 3. punkts un 88. pants, kā grozīts ar Likumu 247/2008; Likuma 336/2005 2. pants; Likuma 485/2005 3. panta 4. punkts; Likuma 101/2000 28. panta 1. punkts.

73 Likums par personas datu apstrādi; 2008. gada 26. jūnija Izpildrīkojums Nr. 714 par Elektronisko komunikāciju tīklu un pakalpojumu nodrošināšanu.

4. tabula: Datu aizsardzība un datu drošība, un uzraudzības iestādes		
Dalībvalsts	*Datu aizsardzības un datu drošības noteikumi valstu tiesību aktos*	*Uzraudzības iestāde*
Igaunija	Transponēšanas likums paredz trīs no četriem principiem. Nav skaidri noteikts noteikums par ceturto principu, lai gan jebkura persona, kuras privātums ir aizskarts ar darbībām, kas saistītas ar novērošanu, var pieprasīt iznīcināt datus, pamatojoties uz tiesas spriedumu[74].	Atbildīgā iestāde ir Tehniskā novērošanas iestāde.
Īrija[75]	Transponēšanas likumā ietverta prasība īstenot četrus principus.	Ieceltam tiesnesim ir pilnvaras izmeklēt un ziņot par to, vai valsts iestādes ievēro transponēšanas likuma noteikumus.
Grieķija[76]	Transponēšanas likumā ietverta prasība īstenot četrus principus, kā arī prasība operatoriem sagatavot un piemērot plānu, lai nodrošinātu atbilstību saskaņā ar ieceltā datu drošības vadītāja prasībām.	Personas datu aizsardzības iestāde un Komunikāciju privātuma iestāde.
Spānija[77]	Datu drošības noteikumi aptver trīs no četriem principiem (saglabāto datu kvalitāte un drošība, pilnvaroto personu piekļuve datiem un aizsardzība pret neatļautu apstrādi).	Atbildīgā iestāde ir Datu aizsardzības aģentūra.
Francija[78]	Transponēšanas likumā ietverta prasība īstenot četrus principus.	Informācijas tehnoloģiju un pamatbrīvību valsts komisija uzrauga pienākumu ievērošanu.
Itālija	Nav skaidri izteikti noteikumi par saglabāto datu drošību, lai gan ir vispārēja prasība iznīcināt vai padarīt anonīmus noslodzes datus un saskaņoti apstrādāt atrašanās vietas datus[79].	Datu aizsardzības iestāde uzrauga operatoru darbību atbilstību direktīvai.
Kipra[80]	Transponēšanas likums paredz katru no četriem principiem.	Personas datu aizsardzības komisārs uzrauga transponēšanas likuma piemērošanu.
Latvija[81]	Transponēšanas likums paredz divus no principiem: saglabāto datu konfidencialitāte un pilnvarota piekļuve tiem, un datu iznīcināšana saglabāšanas termiņa beigās.	Valsts Datu inspektorāts uzrauga personas datu aizsardzību elektronisko komunikāciju nozarē, bet neuzrauga piekļuvi saglabātajiem datiem un to apstrādi.
Lietuva[82]	Transponēšanas likums paredz četrus principus.	Valsts Datu aizsardzības inspektorāts uzrauga transponēšanas likuma īstenošanu un ir atbildīgs par statistikas sniegšanu Eiropas Komisijai.

74 Elektronisko komunikāciju likuma 111. panta 9. punkts; Kriminālprocesa kodeksa 122. panta 2. punkts.

75 2009. gada Sakaru likuma (Datu saglabāšanas likums) 4. 11. un 12. pants.

76 Likuma 3917/2011 6. pants.

77 Likuma 25/2007 8. pants, Vispārējā telekomunikāciju likuma 38. panta 3. punkts; Likums (9. pants) attiecas uz izņēmumiem attiecībā uz piekļuvi un tiesību atcelšanu, kā paredzēts valsts pamatlikumā 15/1999 par personas datu aizsardzību (22. un 23. pants).

78 CPCE D.98-5. pants; CPCE L-34-1(V). pants; Likuma Nr. 78-17 34. pants; CPCE 43. panta 1. punkts; 1978. gada 6. janvāra Likuma Nr. 78-17 11. pants.

79 Datu aizsardzības kodeksa 123. un 126. pants.

80 Likuma 183(I)/2007 14. un 15. pants.

81 Elektronisko sakaru likuma 4. panta 4. punkts un 71. panta 6.-8. punkts.

82 Elektronisko komunikāciju likuma 12. panta 5. punkts, 66. panta 8. un 9. punkts, kā grozīts 2009. gada 14. novembrī.

4. tabula: Datu aizsardzība un datu drošība, un uzraudzības iestādes		
Dalībvalsts	*Datu aizsardzības un datu drošības noteikumi valstu tiesību aktos*	*Uzraudzības iestāde*
Luksemburga[83]	Transponēšanas likums paredz četrus principus.	Datu aizsardzības iestāde.
Ungārija[84]	Transponēšanas likums paredz četrus principus.	Datu aizsardzības un informācijas brīvības parlamentārais komisārs.
Malta[85]	Transponēšanas likums paredz četrus principus.	Datu aizsardzības komisārs.
Nīderlande[86]	Transponēšanas likums paredz četrus principus.	Radio komunikāciju aģentūra uzrauga telekomunikāciju pakalpojumu sniedzēju saistības un pienākumus, kas izriet no interneta piekļuves; datu aizsardzības iestāde uzrauga personas datu vispārīgo apstrādi; sadarbības starp šīm divām iestādēm sīkāk ir izklāstīta protokolā.
Austrija	Nav transponēta.	
Polija	Transponēšanas likums paredz četrus principus[87].	Datu aizsardzības iestāde.
Portugāle	Transponēšanas likums paredz četrus principus[88].	Portugāles Datu aizsardzības iestāde.
Rumānija	Nav transponēta.	
Slovēnija[89]	Transponēšanas likums paredz četrus principus.	Informācijas komisārs.
Slovākija[90]	Transponēšanas likums paredz četrus principus.	Valsts regulators un izcenojumu iestāde elektronisko komunikāciju jomā uzrauga personas datu aizsardzību.
Somija	Transponēšanas likums skaidri paredz tikai prasību iznīcināt datus pēc saglabāšanas termiņa beigām[91].	Somijas Komunikāciju regulatīvā iestāde uzrauga operatoru darbību atbilstību datu saglabāšanas noteikumiem. Datu aizsardzības tiesībsargs uzrauga vispārīgo datu apstrādi.
Zviedrija	Nav transponēta.	
Apvienotā Karaliste	Transponēšanas likums paredz četrus principus[92].	Informācijas komisārs uzrauga komunikāciju datu (un jebkuru citu personas datu) saglabāšanu un/vai apstrādi un atbilstīgu datu aizsardzības kontroli. Pārtveršanas komisārs (nodarbināts vai pensionēts vecākais tiesnesis) pārrauga komunikāciju datu iegūšanu, ko veic valsts iestādes saskaņā ar Izmeklēšanas pilnvaru likuma noteikumiem. Izmeklēšanas pilnvaru tribunāls izmeklē sūdzības par datu, kas iegūti saskaņā ar transponēšanas tiesību aktiem (Izmeklēšanas pilnvaru likuma noteikumi), ļaunprātīgu izmantošanu.

83 2010. gada 24. jūlija Likuma 1. panta 5. punkts.

84 Likuma C/2003 157. pants, kā grozīts ar Likumu CLXXIV/2007; Dekrēta 226/2003 2. pants; un Likums LXIII/1992 par datu aizsardzību.

85 Tiesiskā akta 198/2008 24.un 25. pants; Datu aizsardzības likuma 40. panta b) punkts (Cap.440).

86 Telekomunikāciju likuma 13. panta 5. punkts; sadarbības protokola garais nosaukums ir *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

87 Telekomunikāciju likuma 180a. un 180e. pants.

88 Likuma 32/2008 7. pants 1. un 5. punkts, 11. pants; Personas datu aizsardzības likuma 53. un 54. pants.

89 Elektronisko komunikāciju likuma 107a. panta 6. punkts un 107c. pants.

90 Elektronisko komunikāciju likuma 59a. pants; Likuma Nr. 428/2002 par personas datu aizsardzību S33. pants.

91 Elektronisko komunikāciju likuma 16. panta 3. punkts.

92 Datu saglabāšanas regulas 6. pants.

Direktīvas 7. panta transponēšana ir neatbilstīga. Saglabātie dati potenciāli ir ļoti personīgas un jūtīgas dabas dati, tādēļ augsti datu aizsardzības un datu drošības standarti ir jāpiemēro visā datu procesā gan attiecībā uz uzglabāšanu, gan arī uz izguvi un lietošanu, un tas ir jādara nepārtraukti un redzami, lai mazinātu privātuma aizskaršanas riskus un saglabātu pilsoņu uzticību. Komisija apsvērs iespējas uzlabot datu drošības un datu aizsardzības standartus, tostarp ieviest „integrētas privātās dzīves aizsardzības" risinājumus, lai nodrošinātu, ka šos standartus ievēro gan uzglabāšanas, gan nosūtīšanas jomā. Tāpat Komisija paturēs prātā 29. pantā minētās Datu aizsardzības darba grupas ziņojumā par otro izpildu rīcību iekļautos ieteikumus par obligātajiem aizsardzības pasākumiem un tehniskajiem un organizatoriskajiem drošības pasākumiem[93].

4.7. Statistika (10. pants)

Dalībvalstīm ir pienākums sniegt Komisijai gada statistiku par datu saglabāšanu, ietverot:

– gadījumus, kad informācija sniegta kompetentām iestādēm saskaņā ar attiecīgiem valsts tiesību aktiem;

– laiku, kas pagājis kopš datu saglabāšanas datuma līdz datumam, kad kompetentā iestāde ir pieprasījusi šo datu nosūtīšanu (tas ir, datu vecumu); un

– gadījumus, kad nav bijis iespējams izpildīt pieprasījumus pēc datiem.

Pieprasot statistiku atbilstoši šim noteikumam, Komisija lūdza dalībvalstīm sniegt sīku informāciju par datu individuālu „pieprasījumu" gadījumiem. Tomēr statistika gan informācijas, gan aptvertās jomas ziņā izrādījās atšķirīga: dažas dalībvalstis savās atbildēs izdalīja dažādus komunikāciju veidus, citas norādīja uz datu vecumu pieprasījuma brīdī, bet citas iesniedza tikai gada statistiku bez detalizēta sadalījuma. Deviņpadsmit dalībvalstis[94] sniedza statistiku par datu pieprasījumu skaitu 2009. un/vai 2008. gadā; ietverot arī Īriju, Grieķiju un Austriju, kur datus pieprasa kaut arī transponēšanas tiesību aktu pagaidām nav, un Čehijas Republiku un Vāciju, kuru datu saglabāšanas likumi ir atcelti. Septiņas dalībvalstis, kuras ir transponējušas direktīvu, statistiku neiesniedza, lai gan Beļģija sniedza aplēsi par telefonijas datu gada pieprasījumu skaitu (300 000).

Ticami kvantitatīvi un kvalitatīvi dati ir izšķiroši, lai skaidri parādītu tādu drošības pasākumu kā, piemēram, datu saglabāšanas nepieciešamību un vērtību. Tas jau tika atzīts 2006. gada rīcības plānā par noziedzības un krimināltiesību statistikas veidošanu[95], kurā bija ietverts mērķis izstrādāt metodes, lai regulāri ievāktu datus atbilstīgi direktīvai un iekļautu statistiku Eurostat datu bāzē (ja tie atbilst kvalitātes standartiem). Šo mērķi nav izdevies īstenot, ņemot vērā to, ka vairākums dalībvalstu pilnībā transponēja direktīvu tikai pēdējos divos gados un statistikas avotus skaidroja atšķirīgi. Komisija savā nākamajā priekšlikumā par datu saglabāšanas sistēmas pārskatīšanu, kā arī statistikas rīcības plāna pārskatīšanu, centīsies izstrādāt lietderīgas izvērtēšanas un ziņošanas procedūras, kas ļautu datu saglabāšanu uzraudzīt pārredzamā un nozīmīgā veidā, neuzliekot kriminālās justīcijas un tiesībaizsardzības iestādēm nevajadzīgu nastu.

---

93 29.panta Datu aizsardzības darba grupas atzinums 3/2006 (WP119); Ziņojums 01/2010.

94 Čehija, Dānija, Vācija, Igaunija, Īrija, Grieķija, Spānija, Francija, Kipra, Latvija, Lietuva, Malta, Nīderlande, Austrija, Polija, Slovēnija, Slovākija, Somija, Apvienotā Karaliste.

95 Komisijas paziņojums (2006) 437, „Visaptverošas un saskaņotas ES stratēģijas izstrāde, lai veidotu noziedzības un krimināljustīcijas statistiku: ES rīcības plāns 2006. – 2010. gadam".

4.8. Transponēšana EEZ valstīs

Datu saglabāšanas tiesību akti ir Īslandē, Lihtenšteinā un Norvēģijā[96].

4.9. Konstitucionālo tiesu lēmumi par transponēšanas likumiem

Rumānijas Konstitucionālā tiesa 2009. gada oktobrī, Vācijas Federālā konstitucionālā tiesa 2010. gada martā un Čehijas Konstitucionālā tiesa 2011. gada martā atcēla likumus, ar kuriem attiecīgajās jurisdikcijās bija transponēta direktīva, pamatojoties uz to, ka šie likumi neatbilda konstitūcijai. Rumānijas tiesa[97] pieņēma, ka iejaukšanās pamattiesībās var būt atļauta gadījumos, ja ir ievēroti konkrēti noteikumi un nodrošināti atbilstīgi un pietiekami aizsardzības pasākumi, lai novērstu iespējamo patvaļīgas dabas rīcību. Tajā pašā laikā, atsaucoties uz Eiropas Cilvēktiesību tiesas judikatūru[98], tiesa secināja, ka transponēšanas likuma darbības joma un mērķis ir neskaidri un drošības pasākumi nav pietiekami, un uzskatīja, ka „nepārtrauktas juridiskas saistības" saglabāt visus noslodzes datus sešus mēnešus principā nav savienojamas ar tiesībām uz privāto dzīvi un izpausmes brīvību, kā noteikts Eiropas Cilvēktiesību konvencijas 8. pantā.

Vācijas Konstitucionālā tiesa[99] paziņoja, ka datu saglabāšana rada novērošanas sajūtu, kas varētu kaitēt pamattiesību brīvai īstenošanai. Tā skaidri atzina, ka datu saglabāšana strikti ierobežotai lietošanai kopā ar pietiekami augstu datu drošību varētu garantēt, ka Vācijas pamatlikums nav pārkāpts. Tomēr tiesa uzsvēra, ka šādu datu saglabāšana ievērojami ierobežo tiesības uz privāto dzīvi, tādēļ to būtu jāatļauj tikai ļoti ierobežotos apstākļos, bet sešu mēnešu saglabāšanas termiņš ir jānosaka kā griesti (*an der Obergrenze*) attiecībā uz to, ko iespējams uzskatīt samērīgu (215. punkts). Dati būtu jāpieprasa vienīgi tad, ja pastāv aizdomas par smagu noziedzīgu nodarījumu vai ir pierādījumi par valsts drošības apdraudējumu, bet datu izguve būtu jāaizliedz attiecībā uz konkrētām priviliģētām komunikācijām (piemēram, kas saistītas ar emocionālajām vai sociālajām vajadzībām), kas ir balstītas uz konfidencialitāti. Datus būtu arī jāšifrē ar pārredzamu to lietošanas uzraudzību.

Čehijas Konstitucionāla tiesa[100] atcēla transponējošos tiesību aktus pamatojoties uz to, ka, ņemot vērā to ietekmi uz pamattiesībām, tiesību akti nebija pietiekami precīzi un skaidri. Tiesa kritizēja mērķa ierobežojumu ka nepietiekami šauru, ņemot vērā datu saglabāšanas prasības plašumu un apjomu. Tā uzskatīja, ka tiesību aktos nav pietiekami skaidra to kompetento iestāžu definīcija, kas tiesīgas piekļūt un izmantot saglabātos datus, un nav pietiekami skaidras datu piekļuves un izmantošanas procedūras, lai nodrošinātu datu integritāti un konfidencialitāti. Pilsoņiem tādējādi nebija nodrošinātas pietiekamas garantijas un drošības pasākumi pret iespējamu valsts iestāžu pilnvaru ļaunprātīgu izmantošanu. Tiesa nekritizēja pašu direktīvu un atzina, ka direktīva ļāva Čehijas Republikai to transponēt saskaņā ar konstitūciju. Tomēr tiesa *obiter dictum* izteica šaubas par noslodzes datu

---

96 Transponējošais tiesību akts Īslandē ir Telekomunikāciju likums 81/2003 (kā grozīts 2005. gada aprīlī); Lihtenšteinā tas ir 2006. gada Telekomunikāciju likums. Norvēģijā transponējošais tiesību akts tika pieņemts 2011. gada 5. aprīlī, likums vēl nav saņēmis Karalisko piekrišanu.

97 Rumānijas Konstitucionālās tiesas 2009. gada 8. oktobra lēmums Nr. 1258.

98 DECT, Rotaru pret Rumāniju 2000. gads, avīze „*Sunday Times*" pret Apvienoto Karalisti, 1979. gads, un Lihtenšteinas princis Hans-Adam pret Rumāniju 2001. gads.

99 Federālā konstitucionālā tiesa, 1 BvR 256/08, 1.-345. punkts.

100 Čehijas Konstitucionālās tiesas 22. marta spriedums par Aktu Nr.127/2005 un Dekrētu Nr. 485/2005; sk. jo īpaši 45. – 48. punktu, 50. – 51. punktu un 56. punktu.

saglabāšanas nepieciešamību, efektivitāti un piemērotību, ņemot vērā noziedzīgu nodarījumu pastrādāšanas jaunu metožu parādīšanos, izmantojot anonīmas SIM kartes.

Šīs trīs dalībvalstis pašreiz apsver, kā vēlreiz transponēt direktīvu. Lietas par datu saglabāšanu ir iesniegtas arī konstitucionālajās tiesās Bulgārijā, kā rezultātā transponēšanas likums tika pārskatīts, Kiprā, kur uzskatīja, ka tiesas rīkojumi, kas izdoti saskaņā ar transponēšanas likumu, ir antikonstitucionāli, un Ungārijā, kur ir paredzēta izskatīšanai lieta par to, ka transponēšanas likumā nav iekļauti datu apstrādes tiesiskie nolūki[101].

Komisija savā nākamajā priekšlikumā par datu saglabāšanas sistēmu izskatīs valstu tiesu praksēs radušos jautājumus.

4.10. Direktīvas īstenošana

Komisija sagaida, ka dalībvalstis, kas vēl nav pilnībā transponējušas direktīvu vai vēl nav pieņēmušas tiesību aktus, kas aizvietotu valstu tiesu anulētos transponējošos tiesību aktus, pēc iespējas ātrāk to izdarīs. Ja tas nenotiks, Komisija patur sev tiesības īstenot pilnvaras, kas tai piešķirtas saskaņā ar ES līgumiem. Līdz šim Tiesa jau ir konstatējusi, ka divas dalībvalstis, kas vēl nav transponējušas direktīvu (Austrija un Zviedrija), ir nav izpildījušas savus pienākumus saskaņā ar ES tiesībām[102]. Pēc tam, kad Zviedrijas parlaments nolēma atlikt transponējošo tiesību aktu pieņemšanu uz 12 mēnešiem, Komisija 2011.gada aprīlī nolēma otrreiz vērsties Tiesā pret Zviedriju par sprieduma, kas pieņemts lietā Nr. C-185/09 nepildīšanu, pieprasot noteikt sodanaudu saskaņā ar Līguma par Eiropas Savienības darbību 260. pantu. Komisija turpina cieši uzraudzīt situāciju Austrijā, kas ir iesniegusi transponējošo tiesību aktu tūlītējas pieņemšanas grafiku.

5. SAGLABĀTO DATU LOMA KRIMINĀLĀS JUSTĪCIJAS UN TIESĪBAIZSARDZĪBAS JOMĀ

Šajā nodaļā ir apkopotas saglabāto datu funkcijas, kā to aprakstījušas dalībvalstis, sniedzot savu ieguldījumu izvērtējumā.

5.1. Saglabāto datu apjoms, kuriem piekļuvušas kompetentās valsts iestādes

Gan telekomunikāciju datu plūsmas, gan pieprasījumu pēc piekļuves datiem apjoms pieaug. Statistika, ko iesniegušas 19 dalībvalstis par 2008. un/vai 2009. gadu norāda, ka kopumā visā ES katru gadu ir iesniegti vairāk nekā 2 miljoni datu pieprasījumu; šis skaits starp dalībvalstīm ievērojami atšķīrās – no mazāk nekā 100 pieprasījumiem gadā (Kipra) līdz vairāk nekā 1 miljonam pieprasījumu gadā (Polija). Saskaņā ar informāciju par pieprasīto datu veidu, ko iesniedza divpadsmit dalībvalstis par 2008. vai 2009. gadu, visbiežāk pieprasītais datu veids bija ar mobilo telefoniju saistīti dati (sk. 5.,8. un 12. tabulu). Statistikā nav norādīts kādam konkrētam nolūkam katrs pieprasījums ir iesniegts. Čehija, Latvija un Polija minēja, ka attiecībā uz mobilās telefonijas datiem kompetentajām iestādēm vienāds lūgums ir jāiesniedz

---

101 Bulgārijas Augstākā administratīvā tiesas 2008. gada 11. decembra lēmums Nr. 13627; Kipras Augstākās tiesas 2011. gada 1. februāra apelācijas lieta Nr. 65/2009, 78/2009, 82/2009 un 15/2010-22/2010; Ungārijas Konstitucionālajā tiesā Ungārijas Pilsoņu brīvību apvienība sūdzību iesniedza 2008. gada 2. jūnijā.

102 Attiecīgi lieta Nr. C-189/09 un lieta Nr. C-185/09.

ikvienam galvenajam mobilo tālruņu operatoram, tādēļ faktiskais pieprasījumu skaits uz gadījumu ir ievērojami mazāks, nekā norādīts statistikā.

Acīmredzama izskaidrojuma šīm atšķirībām nav, lai gan iedzīvotāju skaits, dominējošās noziedzības tendences, nolūku ierobežojumi un nosacījumi piekļuvei, kā arī datu iegūšanas izmaksas ir svarīgi faktori

5.2. Saglabāto datu vecums, kuriem piekļuvušas kompetentās valsts iestādes

Pamatojoties uz statistikas iedalījumu, ko iesniegušas deviņas dalībvalstis[103] par 2008. gadu (sk. kopsavilkumu 5. tabulā un papildu informāciju pielikumā), aptuveni 90 % datu, kuriem kompetentās iestādes piekļuvušas šajā gadā, bija sešus mēnešus veci vai jaunāki, un aptuveni 70 % datu bija trīs mēnešus veci vai jaunāki, kad tika izdarīts (sākotnējais) piekļuves pieprasījums.

5. tabula: Kopsavilkums par saglabāto datu vecumu, kuriem piekļuvušas kompetentās iestādes, deviņās dalībvalstīs, kas iesniedza sadalījumu pa datu veidiem 2008. gadā

Vecums	*Fiksētā telefonija*	*Mobilā telefonija*	*Interneta dati*	*Kopumā*
Jaunāki par trim mēnešiem	61%	70%	56%	67%
Trīs līdz sešus mēnešus veci	28%	18%	19%	19%
Sešus līdz divpadsmit mēnešus veci	8%	11%	18%	12%
Vairāk nekā gadu veci	3%	1%	7%	2%

Saskaņā ar vairuma dalībvalstu sniegto informāciju saglabāto datu, kuri ir vecāki par trīs vai pat sešiem mēnešiem, lietošana nav tik bieža, bet tā var būt izšķiroša un tās izmatošanu var iedalīt trīs kategorijās. Pirmkārt, kriminālizmeklēšanas gaitā ar internetu saistītus datus parasti pieprasa vēlāk nekā cita veida pierādījumus. Fiksēto tīklu un mobilās telefonijas datu analīze bieži rada potenciālus pavedienus, kā rezultāta papildus tiek pieprasīti vecāki dati. Piemēram, ja izmeklēšanas laikā, pamatojoties uz fiksētā tīkla vai mobilās telefonijas datiem, ir atrasts vārds, izmeklētāji var vēlēties identificēt interneta protokola (IP) adresi, kuru šī persona ir lietojusi, un var vēlēties noteikt, ar ko šī persona ir sazinājusies dotajā laika periodā, izmantojot šo IP adresi. Pēc šāda scenārija izmeklētāji, visticamāk, pieprasīs datus, kas ļauj izsekot arī komunikācijām ar citām IP adresēm un atklāt to personu identitāti, kuras šīs IP adreses ir lietojušas.

Otrkārt, sevišķi smagu noziegumu, noziegumu sēriju, organizētās noziedzības un terorisma uzbrukumu izmeklēšanās parasti paļaujas uz vecākiem saglabātajiem datiem, kuri atspoguļo laika periodu, kas patērēts, plānojot šos pārkāpumus, lai noteiktu noziedzīgas uzvedības modeļus, attiecības starp nozieguma līdzdalībniekiem un konstatētu noziedzīgu nodomu. Rīcības, kas saistītas ar sarežģītiem finanšu noziegumiem, bieži atklāj tikai pēc vairākiem mēnešiem. Treškārt, un izņēmuma kārtā, dalībvalstis ir arī pieprasījušas noslodzes datus, kas

[103] Čehija, Dānija, Igaunija, Īrija, Spānija, Kipra, Latvija, Malta, Apvienotā Karaliste.

turēti citā dalībvalstī, kur parasti šādiem datiem var ļaut piekļūt tikai ar tiesu atļauju, atbildot uz lūguma vēstuli, kuru izsniedzis pieprasītājas dalībvalsts tiesnesis. Šāda veida savstarpējā tiesiskā palīdzība var būt ilgstošs process, kas arī izskaidro to, kādēļ daži no pieprasītajiem datiem šajos gadījumos bija vecāki par sešiem mēnešiem.

5.3. Saglabāto datu pārrobežu pieprasījumi

Kriminālizmeklēšanā un kriminālvajāšanā var būt iesaistīti pierādījumi vai liecinieki no vairākām dalībvalstīm, kā arī notikumi, kas notikuši vairākās dalībvalstīs. Saskaņā ar dalībvalstu iesniegto statistiku mazāk nekā 1% no visiem saglabāto datu pieprasījumiem attiecās uz datiem, kurus tur citā dalībvalsti. Tiesībaizsardzības iestādes norāda, ka labāk pieprasa datus no iekšzemes operatoriem, kuri var būt uzglabājuši būtiskos datus, nekā uzsāk savstarpējās tiesiskās palīdzības procedūru, kas var būt ilgstoša un bez garantijas, ka piekļuvi datiem piešķirs. Padomes Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu[104], ar kuru nosaka termiņu informācijas sniegšanai pēc lūguma saņemšanas no citas dalībvalsts, šajā gadījumā nepiemēro, jo saglabātos datus uzskata par informāciju, kas jāiegūst piespiedu kārtā, kas ir ārpus instrumenta darbības jomas. Tomēr neviena no dalībvalstīm nav pieprasījusi, lai šādu pārrobežu apmaiņu turpinātu veicināt.

5.4. Saglabāto datu vērtība kriminālizmeklēšanā un kriminālvajāšanā

Lai gan ziņojumā norādītais datu pieprasījuma kopējais skaits nebūt pilnībā neatspoguļo datu vērtību individuālās kriminālizmeklēšanās, principā dalībvalstis ziņojušas, ka datu saglabāšana ir svarīga, un dažos gadījumos pat nepieciešama[105], noziedzības novēršanai un apkarošanai, tostarp cietušo aizsardzībai un nevainīgo attaisnošanai kriminālajā tiesvedībā. Veiksmīga vainīgo notiesāšana ir pamatota uz vainas atzīšanu, liecinieku liecībām vai tiesu ekspertīzes pierādījumiem. Tiek ziņots, ka saglabātie noslodzes dati ir izrādījušies nepieciešami, lai sazinātos ar atgadījuma lieciniekiem, kurus citādi nebūtu varēts atpazīt, kā arī pierādījumu nodrošināšanā vai konstatēšanā attiecībā uz nozieguma sarežģītību. Konkrētas dalībvalstis[106] turklāt ir paziņojušas, ka saglabāto datu lietošana ir palīdzējusi attaisnot personas, kuras turētas aizdomās par nozieguma izdarīšanu, nepielietojot citas novērošanas metodes, piemēram, noklausīšanos vai kratīšanu dzīvesvietā, kuras varētu tikt uzskatītas par daudz aizskarošākām.

ES nepastāv vispārēja „smaga nozieguma" definīcija, un, attiecīgi, nepastāv ES statistika par smagu noziegumu izdarīšanas vai smagu noziegumu izmeklēšanu vai kriminālvajāšanu biežumu, lai gan datus par noziedzību un tiesiskumu publicē regulāri. Kā ziņoja 19 dalībvalstis, kuras iesniedza vismaz kaut kādus datus par 2009. un/vai 2008. gadu, kopējais saglabāto datu pieprasījumu skaits bija aptuveni 2,6 miljoni. Salīdzinot ar jaunāko noziedzības un kriminālās justīcijas statistiku, kas pieejama par šīm 19 dalībvalstīm, kas attiecas uz visiem

---

104 Padomes 2006. gada 18. decembra Pamatlēmums 2006/960/TI par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu OV L 386, 29/12/2006, 89.-100. lpp. un OV L 200, 01/08/2007, 637.-648. lpp.

105 Čehija uzskata datu saglabāšanu par „pilnīgi nepieciešamu ļoti daudzos gadījumos"; Ungārija minēja, ka tā „ir nepieciešama [tiesībaizsardzības aģentūru] ikdienas darbībai"; Slovēnija norādīja, ka saglabāto datu neesamība „paralizētu tiesībaizsardzības aģentūru darbību"; Apvienotās Karalistes policijas aģentūra aprakstīja noslodzes datu pieejamību kā „absolūti izšķirošu…terorisma un smagu noziegumu draudu izmeklēšanā".

106 Vācija, Polija, Slovēnija, Apvienotā Karaliste.

reģistrētiem noziegumiem, ne tikai smagiem noziegumiem, varētu teikt, ka tas būtu nedaudz vairāk nekā divi pieprasījumi uz policistu gadā vai aptuveni vienpadsmit pieprasījumi uz katriem 100 reģistrētiem noziegumiem[107].

Pamatojoties uz iesniegto statistiku un ilustratīvajiem piemēriem, kas sasaista saglabāto vēsturisko komunikāciju datu lietošanu ar notiesāšanu un attaisnošanu, izbeigto lietu un novērsto noziegumu skaitu, var nonākt pie vairākiem secinājumiem par saglabāto datu lomu un vērtību kriminālizmeklēšanā.

Pierādījumu ķēdes veidošana

Pirmkārt, saglabātie dati ļauj veidot pierādījumu ķēdes, kas noved pie pārkāpuma. Datus lieto, lai saskatītu vai nostiprinātu citus pierādījumu veidus par darbībām un saikni starp aizdomās turamajām personām. Gan tiesībaizsardzības iestādes, gan aizstāvji jo īpaši lieto atrašanās vietas datus, lai izslēgtu aizdomās turamos no nozieguma vietām un apstiprinātu alibi. Tādejādi šie pierādījumi var izslēgt personas no kriminālizmeklēšanas, tā samazinot nepieciešamību veikt daudz aizskarošākas izmeklēšanas darbības, vai vainagoties ar nevainīgo personu attaisnošanu tiesas sēdē. Beļģija atsaucās uz 2008. gada vainīgo notiesāšanu krimināllietā, kur viens Antverpenes kriminmāltiesas darbinieks nolaupīja tīģeri. Atrašanās vietas datu sasaistīšana ar viņu darbībām trīs dažādās pilsētās bija izšķiroša, lai pārliecinātu zvērinātos par viņu līdzdalību. Citā piemērā, lietā par 2007. gadā notikušu slepkavību saistībā ar motociklistu bandu, atrašanās vietas dati no pārkāpēju mobilajiem tālruņiem pierādīja, ka viņi atradās teritorijā, kurā notika slepkavība, kā rezultātā tika panākta daļēja atzīšanās[108]. Saskaņā ar Beļģijas, Īrijas un Apvienotās Karalistes sniegto informāciju noteiktus noziegumus, kas saistīti ar komunikāciju internetā, var izmeklēt, *tikai* izmantojot datu saglabāšanu: piemēram, tērzēšanas istabās paustie vardarbības draudi neatstāj nekādas pēdas, tikai datu plūsmu kibertelpā. Līdzīga situācija ir gadījumos, kad noziegumus veic, izmantojot tālruni. Ungārija un Polija atsaucās uz 2009. gada beigās/2010. gada sākumā notikušo krāpšanu pa tālruni – vainīgie zvanīja vecāka gada gājuma cilvēkiem un izlikās par ģimenes locekļiem, kuriem nepieciešams aizdevums. Šos vainīgos varēja noteikt, tikai pateicoties saglabātajiem telefonijas datiem.

Kriminālizmeklēšanu uzsākšana

Otrkārt, ir bijuši gadījumi, kad tiesu ekspertīzes pierādījumu vai aculiecinieku trūkuma dēļ vienīgais veids, kā uzsākt kriminālizmeklēšanu, ir bijis pārbaudīt saglabātos datus. Vācija atsaucās uz piemēru par policista slepkavību, kad uzbrucējs bija aizmucis ar upura transportlīdzekli, kuru pēc tam pameta. Varēja nokonstatēt, ka viņš bija zvanījis, lai sameklētu alternatīvu transportlīdzekli. Tā kā nebija ne tiesu ekspertīzes pierādījumu, ne aculiecinieku liecības, lai noskaidrotu slepkavnieka personību, iestādes paļāvās uz šo noslodzes datu pieejamību, lai varētu uzsākt izmeklēšanu. Ar internetu saistītās bērnu seksuālas izmantošanas

---

107 ES-27 2007. gadā bija 1,7 miljoni policistu, no kuriem 1,2 miljoni bija tajās 19 dalībvalstīs, kuras sniedza statistiku par saglabāto datu pieprasījumiem; ES policija 2007. gadā ziņoja par 29,2 miljoniem noziegumu, no kuriem 24 miljoni bija reģistrēti tajās 19 dalībvalstīs, kuras sniedza statistiku. (Avots: Eurostat 2009. gads).

108 Nacionālā patrulēšanas uzlabošanas aģentūra (*National Policing Improvement Agency*) (Apvienotā Karaliste), Slepkavību un smagu noziegumu izmeklēšanas žurnāls (*The Journal of Homicide and Major Incident Investigation*), 5. sējums, 1. izdevums, *Spring* 2009. gada pavasaris, 39.-51. lpp.

lietās veiksmīgai izmeklēšanai ir bijusi nepieciešama datu saglabāšana. Līdztekus citām izmeklēšanas metodēm saglabātie dati ļauj noteikt bērnu seksuālās izmantošanas saturu patērētājus[109], un palīdz noteikt un glābt bērnus – upurus. Čehija ziņoja, ka bez piekļuves ar internetu saistītiem saglabātiem datiem nebūtu bijis iespējams „Operācijas Vilma" ietvaros veikt izmeklēšanas bērnu pornogrāfijas lietotāju un izplatītāju tīklā. ES līmenī operācija „Glābšana" (*Operation Rescue*) (ko atbalsta Eiropols), kas paredzēta bērnu aizsardzībai pret seksuālu izmantošanu, nav tik efektīva, cik plānots, jo noteiktās dalībvalstīs datu saglabāšanas direktīva nav transponēta tiesību aktos, tādēļ šīs dalībvalstis nevarēja veikt izmeklēšanu attiecībā uz ārkārtīgi plaša starptautiska pedofilu tīkla biedriem, kuri lieto IP adreses, kuras var būt pat vienu gadu vecas.

Kibernoziegumu izmeklēšanā bieži pirmais pavediens ir IP adrese. Tiesībaizsardzība, pirms lemt par kriminālizmeklēšanas uzsākšanu, izgūstot noslodzes datus, var noteikt IP adreses abonentu. Tas ļauj arī policistiem iepriekš brīdināt potenciālos upurus par kiberuzbrukumiem: ja policijai izdodas konfiscēt robottīklu operatoru izmantotus komandas un kontroles serverus, tā var redzēt tikai IP adreses, kas saistītas ar to serveri; bet, piekļūstot saglabātajiem datiem, policija var noteikt un brīdināt potenciālos upurus, kuriem šīs IP adreses pieder.

Saglabātie dati ir kriminālās izmeklēšanas neatņemama sastāvdaļa

Treškārt, lai gan tiesībaizsardzības iestādes un tiesas vairākumā dalībvalstu neved statistiku par to, kāda veida pierādījumi izrādījās izšķirošie notiesāšanas vai attaisnošanas nodrošināšanā, saglabātie dati ir būtiski kriminālizmeklēšanai un krimināltvajāšanai ES. Dažas dalībvalstis pauda, ka nevar vienmēr nošķirt saglabāto datu ietekmi uz kriminālizmeklēšanas un krimināltvajāšanas veiksmi, jo tiesas izvērtē visus iesniegtos pierādījumus un ļoti reti tikai viens vienīgs pierādījuma fakts ir izšķirošais[110]. Nīderlande ziņoja, ka laikā no 2010. gada janvāra līdz jūlijam vēsturiskie noslodzes dati bija izšķirošais faktors 24 tiesas spriedumos. Somija ziņoja, ka 56% no 3405 pieprasījumiem saglabātie dati izrādījās „svarīgi" vai „būtiski" krimināllietu atklāšanā un/vai krimināltvajāšanā. Apvienotā Karaliste iesniedza datus, kuri it kā parādīja saglabāto datu ietekmi uz krimināltvajāšanu; tā ziņoja, ka trīs no tās tiesībaizsardzības aģentūrām saglabātie dati bija vajadzīgi gandrīz visās izmeklēšanās, kuras vainagojās ar krimināltvajāšanu vai notiesāšanu.

5.5. Tehnoloģiju attīstība un priekšapmaksas SIM karšu lietošana

Tiesībaizsardzībai ir nepieciešams iet kopsolī ar tehnoloģiju attīstību, kuras izmanto, lai izdarītu noziegumu vai kūdītu uz to. Datu saglabāšana ir to kriminālizmeklēšanas instrumentu starpā, kuri vajadzīgi, lai tiesībaizsardzības iestādes spētu paveicamā un rentablā veidā cīnīties ar mūsdienu noziedzības izaicinājumu daudzveidību, apjomu un ātrumu. Vairāki aizvien populārāki komunikāciju veidi ir ārpus direktīvas darbības jomas. Virtuālie privātie tīkli (VPN), piemēram, universitātēs vai lielās korporācijās, ļauj vairākiem lietotājiem piekļūt internetam caur vienu vārteju, izmantojot vienu un to pašu IP adresi. Tomēr pašlaik ievieš jaunas tehnoloģijas, kas ļauj individuāliem VPN lietotājiem pievienot adreses.

---

109 Projekts par „P2p (vienādranga) darbības novērtēšanu un analīzi pedofilijas satura apkarošanai", kas atbalstīts Drošāka interneta programmas ietvaros, nodrošināja precīzu informāciju par pedofilu darbībām eDonkey vienādranga sistēmā, tā ļaujot noteikt 178 000 lietotājus (no 89 miljoniem pārbaudīto lietotāju), kuri pieprasīja pedofilijas saturu.

110 Beļģija, Čehijas Republika, Lietuva.

ES mobilās telefonijas lietotāju skaits, kuri izmanto priekšapmaksas pakalpojumus, atšķiras. Dažas dalībvalstis ir paziņojušas, ka anonīmas priekšapmaksas SIM kartes, jo īpaši, ja nopirktas citā dalībvalstī, arī var izmantot personas, kuras iesaistītas noziedzīgās darbībās, kā iespēju izvairīties no atpazīšanas kriminālizmeklēšanā[111]. Sešas dalībvalstis (Dānija, Spānija, Itālija, Grieķija, Slovākija un Bulgārija) ir pieņēmušas pasākumus, ar kuriem pieprasa priekšapmaksas SIM karšu reģistrēšanu. Šīs un citas dalībvalstis (Polija, Kipra un Lietuva) ir iestājušās par labu ES mēroga pasākumam priekšapmaksas pakalpojumu lietotāju identitātes obligātai reģistrācijai. Par šo valsts pasākumu efektivitāti pierādījumi nav iesniegti. Potenciālie ierobežojumi ir uzsvērti, piemēram, gadījumos, ka identitāte nozagta vai SIM karti ir nopirkusi trešā persona, vai lietotājs klejo apkārt ar karti, kas pirkta trešā valstī. Kopumā Komisija nav pārliecināta par to, ka šajā jomā un šajā brīdī ES līmenī ir nepieciešama rīcība.

6. DATU SAGLABĀŠANAS IETEKME UZ OPERATORIEM UN PATĒRĀTĀJIEM

6.1. Operatori un patērētāji

Kopējā paziņojumā Komisijai piecas galvenās nozares asociācijas paziņoja, ka direktīvas ekonomiskā ietekme ir „ievērojama" vai „milzīga attiecībā uz mazajiem pakalpojumu sniedzējiem", jo direktīva ļauj „lielu vaļu manevriem"[112]. Astoņi operatori iesniedza ļoti atšķirīgas aplēses kapitālizdevumu un darbības izdevumu izteiksmē par to, cik izmaksā atbilstība direktīvas prasībām. Šos apgalvojumus varētu būt radījuši norādījumi par operatoriem radīto izmaksu atlīdzināšanas līmeņiem, kā ziņojušas četras no dalībvalstīm (sk. 6. tabulu).

Pēc izpētes aprēķiniem, kuru veica pirms direktīvas transponēšanas vairākumā dalībvalstu, izrādās, ka interneta pakalpojumu sniedzējam, kurš apkalpo pusmiljonu klientu, datu saglabāšanas sistēmas izveidošana izmaksā aptuveni EUR 375 240 pirmajā gadā, bet ekspluatācijas izmaksas ir EUR 9 870 mēnesī[113]; datu izguves sistēmas izveidošanas izmaksas ir lēstas uz EUR 131 190, kur ekspluatācijas izmaksas ir EUR 28 960 mēnesī. Taču Vācijas Konstitucionālā tiesa savā 2010. gada 2. marta spriedumā uzskatīja, ka pienākums saglabāt datus „nav īpaši apgrūtinošs ietekmētajiem pakalpojumu sniedzējiem, kā arī [nav] neproporcionāls attiecībā uz finansiālo slogu, kas radīts uzņēmējiem datu saglabāšanas pienākuma rezultātā"[114]. Datu saglabāšanas izmaksas uz vienību ir pretēji saistītas ar operatora lielumu un standartizācijas līmeni, ko pieņēmusi dalībvalsts sadarbībai ar operatoriem[115].

Savās atbildēs uz Komisijas aptauju vairākums operatoru nevarēja noteikt, cik būtiski direktīva ir ietekmējusi konkurenci, mazumtirdzniecības cenas patērētājiem vai ieguldījumus jaunā infrastruktūrā un pakalpojumos.

---

111 Padomes secinājumi par elektronisko komunikāciju ļaunprātīgas izmantošanas un anonīmas izmantošanas apkarošanu

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

113 *Wilfried Gansterer & Michael Ilger*, Datu saglabāšana – ES Direktīva 2006/24/EK No tehnoloģiskās perspektīvas, Vīne: : *Verlag Medien und Recht*, 2008.

114 Federālā konstitucionālā tiesa, 1 BvR 256/08, 2010. gada 2. marts, 299. punkts (*Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010, para. 299.*)

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

Nav neviena pierādījuma, cik lielā mērā un cik būtiski direktīva ir ietekmējusi elektronisko komunikāciju pakalpojumu patērētāju cenas; patērētāju pārstāvji 2009. gada sabiedriskajā diskusijā nekādu informāciju nesniedza. Apsekojums, ko Vācijā veica pilsoniskās sabiedrības organizācija, parādīja, ka patērētāji plānoja mainīt savu komunikāciju uzvedību un dažos gadījumos izvairīties lietot elektronisko komunikāciju pakalpojumus, taču nav nekādu pierādījumu, kas apstiprinātu, ka kādā attiecīgā dalībvalstī vai jebkur citur ES šāda uzvedības maiņa ir notikusi[116].

Komisija plāno novērtēt turpmāko direktīvas izmaiņu ietekmi uz nozari un patērētājiem, tostarp, iespējams, veicot konkrētu Eurobarometer apsekojumu, lai novērtētu sabiedrības reakciju

6.2. Izmaksu atlīdzināšana

Direktīva neregulē operatoriem datu saglabāšanas prasību ievērošanas radīto izmaksu atlīdzināšanu. Šīs izmaksas var uzskatīt par:

(a) *ekspluatācijas izdevumiem*, tas ir, ekspluatācijas izmaksām vai kārtējām izmaksām, kuras ir saistītas ar uzņēmējdarbības veikšanu, iekārtu, sastāvdaļu, aprīkojuma vai telpu izmantošanu; un

(b) *kapitālizdevumiem*, tas ir, izdevumiem, kas rada turpmākus labumus, vai par produkta vai sistēmas nepatērējamu daļu izstrādāšanas vai nodrošināšanas izmaksām, kas var ietvert darbaspēka un telpu izdevumus, piemēram, īres un pakalpojumu izmaksas.

Visas dalībvalstis nodrošina kaut kāda veida izdevumu atlīdzinājumu, ja datus pieprasa saistībā ar tiesas kriminālprocesu. Divas dalībvalstis ziņoja, ka atlīdzina gan ekspluatācijas, gan kapitāla izdevumus. Sešas dalībvalstis atlīdzina tikai ekspluatācijas izdevumus. Par jebkādām citām atlīdzības shēmām Komisijai nav ziņots. Sīkāka informācija atspoguļota 6. tabulā.

6. tabula: Dalībvalstis, kuras atlīdzina izmaksas

Dalībvalsts	**Ekspluatācijas izdevumi**	**Kapitālizdevumi**	**Atlīdzības izmaksas gadā (miljonos euro)**
Beļģija	Jā	Nē	22 (2008)
Bulgārija	Nē	Nē	-
Čehijas Republika	Nav transponēta[117].		
Dānija	Jā	Nē	-
Vācija	Nav transponēta		
Igaunija	Jā	Nē	-
Īrija	Nē	Nē	-
Grieķija	Nē	Nē	-
Spānija	Nē	Nē	-
Francija	Jā	Nē	-

[116] Apsekojumu veica *Forsa AK Vorratsdatenspeicherung* uzdevumā. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

[117] Pirms tranponējošo tiesību aktu atcelšanas Čehijas Republika atlīdzināja gan ekspluatācijas, gan kapitālizdevumus un ziņoja, ka 2009. gadā ir atlīdzinājusi 6,8 miljonus eiro.

Itālija	-	-	-
Kipra	Nē	Nē	-
Latvija	Nē	Nē	-
Lietuva	Jā, ja pieprasīts un pamatots	Nē	-
Luksemburga	Nē	Nē	-
Ungārija	Nē	Nē	-
Malta	Nē	Nē	-
Nīderlande	Jā	Nē	-
Austrija	Nav transponēta		
Polija	Nē	Nē	-
Portugāle	Nē	Nē	-
Rumānija	Nav transponēta		
Slovēnija	Nē	Nē	-
Slovākija	Nē	Nē	-
Somija	Jā	Jā	1
Zviedrija	Nav transponēta		
Apvienotā Karaliste	Jā	Jā	55 (Kopumā atlīdzināts par izmaksām, kas radušās trīs gadu laikā)

No iepriekšminētā var secināt, ka direktīva nav pilnībā sasniegusi savu mērķi izveidot līdzvērtīgus darbības apstākļus operatoriem ES. Komisija apsvērs variantus, kā samazināt iekšējā tirgus darbības traucējumus, lai nodrošinātu, ka operatoriem daudz konsekventāk atlīdzina izmaksas, kas tiem rodas, ievērojot datu saglabāšanas prasības, jo īpaši pievēršot uzmanību maziem un vidējiem operatoriem.

7. DATU SAGLABĀŠNAS IETEKME UZ PAMATTIESĪBĀM

7.1. Tiesības uz privāto dzīvi un personas datu aizsardzību

Datu saglabāšana ierobežo tiesības uz privāto dzīvi un personas datu aizsardzību, kas ir Eiropas Savienības pamattiesības.[118] Saskaņā ar Eiropas Savienības Pamattiesību hartas 52. panta 1. punktu šādiem „ierobežojumiem ir jābūt noteiktiem tiesību aktos, un tajos jārespektē šo tiesību un brīvību būtība. Ievērojot proporcionalitātes principu, ierobežojumus drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiesi atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības". Praksē tas nozīmē, ka šādiem ierobežojumiem jābūt[119]:

(a) formulētiem precīzi un paredzami;

---

118 Eiropas Savienības Pamattiesību hartas 7. un 8. pants (OV C 83, 30.3.2010, 389. lpp.) garantē, ka „ikvienai personai ir tiesības uz savu personas datu aizsardzību." Līguma par Eiropas Savienības darbību (OV C 83, 30.3.2010, 1. lpp.) 16. pants arī nostiprina ikvienas personas tiesības uz „savu personas datu aizsardzību".

119 Sk. Komisijas Pamattiesību pārbaudes lapu attiecībā uz visiem tiesību aktu ierosinājumiem Komisijas paziņojumā COM (2010) 573/4, „Stratēģija Pamattiesību hartas efektīvai īstenošanai Eiropas Savienībā".

(b) nepieciešamiem, lai īstenotu vispārējas nozīmes mērķi vai lai aizsargātu citu personu tiesības un brīvības;

(c) proporcionāliem sasniedzamajam mērķim; un

(d) tādiem, kas respektētu attiecīgo pamattiesību būtību.

Eiropas Cilvēktiesību konvencijas 8. panta 2. punkts arī paredz, ka valsts institūcijas drīkst traucēt personai baudīt šīs tiesības, ja tas ir vajadzīgs, lai aizstāvētu valsts un sabiedriskās drošības intereses nepieļautu noziegumus[120]. E-privātuma direktīvas 15. panta 1. punkts un Datu saglabāšanas direktīvas izklāsti atkārto šos principus, kas ir pamatā ES datu saglabāšanas pieejai.

Pēc tam Eiropas Kopienu tiesas un Eiropas Cilvēktiesību judikatūra ir nodrošinājusi nosacījumus, kuri ir jāievēro, piemērojot ikvienu privātās dzīves tiesību ierobežojumu. Šie spriedumi ir būtiski attiecībā uz to, vai direktīva būtu jāgroza, jo īpaši attiecībā uz saglabāto datu piekļuves un lietošanas nosacījumiem.

Jebkuram privātās dzīves tiesību ierobežojumam ir jābūt precīzam un jānodrošina paredzamība

Lietā ar Austrijas radio (*Österreichischer Rundfunk*) Tiesa uzskatīja, ka jebkuru iejaukšanos likumā ar tiesībām uz privāto dzīvi ir „jāformulē pietiekami precīzi, lai pilsonis spētu attiecīgi pielāgot savu uzvedību…[lai ievērotu] paredzamības prasību."

Jebkuram privātās dzīves ierobežojumam ir jābūt nepieciešamam un ar obligātajiem aizsardzības pasākumiem

Lietā *Copland* pret Apvienoto Karalisti, kas attiecās uz to, ka valsts uzrauga personas tālruņa zvanus, e-pasta korespondenci un interneta lietošanu, Eiropas Cilvēktiesību tiesa uzskatīja, ka šāds privātās dzīves tiesību ierobežojums var būt nepieciešams tikai tad, ja ir pamatots uz attiecīgajiem valsts tiesību aktiem[121]. Lietā S. un *Marper* pret Apvienoto Karalisti, kas attiecās uz jebkuras personas, kura attaisnota, vai attiecībā uz kuru tiesvedība ir izbeigta pirms notiesāšanas, DNS profilu vai pirkstu nospiedumu saglabāšanu, Tiesa uzskatīja, ka šādu privātās dzīves tiesību ierobežojumu var attaisnot tikai tad, ja tas ir ārkārtīgi nepieciešams sabiedrības vajadzībām, ja tas ir proporcionāls vēlamajam mērķim un ja valsts iestādes minētie iemesli šāda ierobežojuma pamatošanai ir būtiski un pietiekami[122]. Datu aizsardzības pamatprincipi prasa, lai datu saglabāšana ir samērīga attiecībā uz datu ievākšanas nolūku un lai uzglabāšanas termiņš ir ierobežots[123]. Attiecībā uz tālruņa sarunu noklausīšanos, slepenu novērošanu un slēptu izlūkdatu ievākšanu „[bija] būtiski… skaidri, sīki izklāstīti noteikumi, kas regulē pasākumu darbības sfēru un piemērošanu, kā arī obligātos aizsardzības pasākumus attiecībā uz, *cita starpā*, ilgumu, uzglabāšanu, lietošanu, trešo personu piekļuvi, datu konfidencialitātes un viengabalainības saglabāšanas procedūrām un datu iznīcināšanas

---

120 Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 8. pants (ETS Nr. 5), Eiropas Padome, 4.11.1950.

121 *Copland* pret Apvienoto Karalisti, Eiropas Cilvēktiesību tiesas spriedums, Strasbūra, 3.4.2007, 9. lpp.

122 *Marper* pret Apvienoto Karalisti (*Marper v the United Kingdom)*, Eiropas Cilvēktiesību tiesas spriedums, Strasbūra, 4.12.2008, 31. lpp.

123 Marper, 30. lpp.

procedūrām, tādejādi nodrošinot pietiekamas garantijas pret datu ļaunprātīgas un patvaļīgas izmantošanas risku."

Jebkuriem privātās dzīves tiesību ierobežojumiem jābūt samērīgiem ar vispārējās nozīmes mērķiem

Eiropas Kopienu tiesa savā nolēmumā lietā *Schecke & Eifert* par visu lauksaimniecības subsīdiju saņēmēju publicēšanu internetā[124] arī uzskatīja, ka neizskatās, ka ES likumdevēja vara būtu veikusi atbilstošos pasākumus, lai ieviestu līdzsvaru starp tiesību uz privāto dzīvi būtības ievērošanu un vispārējas nozīmes mērķiem (pārredzamība), ko atzinusi ES. Jo īpaši Tiesa uzskatīja, ka likumu veidotāji nav ņēmuši vērā citas metodes, kas būtu bijušas gan atbilstīgākas mērķiem, gan mazāk aizskartu subsīdiju saņēmēju tiesības uz privātās dzīves neaizskaramību un personas datu aizsardzību. Tādejādi Tiesa uzskatīja, ka likuma veidotāji ir pārsnieguši proporcionalitātes robežas, jo „ierobežojumi attiecībā uz personas datu aizsardzību ir jāpiemēro tikai tik tālu, cik absolūti nepieciešams."

7.2. Datu saglabāšanas principa kritika

Vairākas pilsoniskās sabiedrības organizācijas ir rakstījušas Komisijai, uzsverot, ka datu saglabāšana ir, principā, nepamatota un nevajadzīga personu tiesību uz privāto dzīvi ierobežošana. Viņi uzskata, ka „vispārējā un nekritiska" personu telekomunikāciju noslodzes, atrašanās vietas un abonentu datu saglabāšana ir nelikumīga pamattiesību ierobežošana. Pēc tam, kad vienā dalībvalstī (Īrijā) kāda pilsoņu tiesību grupa iesniedza tiesā prasību, ir paredzams, ka jautājumu par direktīvas likumību iesniegs izskatīšanai Eiropas Kopienu tiesā[125]. Arī Eiropas Datu aizsardzības uzraudzītājs izteica šaubas par šā pasākuma nepieciešamību.

7.3. Aicinājums pēc spēcīgākiem datu drošības un datu aizsardzības noteikumiem

29. panta Darba grupas ziņojumā par otro izpildu rīcību bija uzsvērts, ka komunikāciju konfidencialitātes un izteiksmes brīvības pārkāpumu riski bija raksturīgi jebkuru noslodzes datu uzglabāšanā. Ziņojumā bija kritizēti valstu īstenošanas pasākumu konkrēti aspekti, jo īpaši datu reģistrēšana, saglabāšanas termiņi, saglabāto datu veidi un datu drošības pasākumi. Darba grupa ziņoja par gadījumiem, kad bija saglabāta informācija par ar internetu saistītu komunikāciju saturu, tostarp galamērķu IP adreses un URL tīmekļu vietnes, e-pastu galvenes un saņēmēju saraksts „kopija" ailē. Tādēļ Darba grupa skaidroja, ka datu kategorijas ir izsmeļošas un operatorus nav jāapgrūtina ar papildu datu saglabāšanas pienākumiem.

Eiropas Datu aizsardzības uzraudzītājs ir apstiprinājis, ka direktīvai „nav izdevies saskaņot valstu tiesību aktus" un saglabāto datu lietošana nav strikti ierobežota tikai attiecībā uz smagu noziegumu apkarošanu[126]. Viņš ir minējis, ka ES dokumentā, kurā ir ietverti noteikumi par obligātu datu saglabāšanu, ja nepieciešamība pēc datiem ir skaidri parādīta, ir jābūt ietvertiem arī noteikumiem par tiesībaizsardzības piekļuvi šiem datiem un tālāku lietošanu. Viņš ir

---

124 Lieta C-92/09 *Volker* un *Markus Schecke GbR* pret *Land Hessen* un lieta C-93/09 *Eifert* pret *Land Hessen* un *Bundesanstalt für Landwirtschaft und Ernahrung*, 9.11.10.

125 2010. gada 5. maijā Īrijas Augstā tiesa piekrita *Digital Rights Ireland Limited* ierosmei vērsties Eiropas Savienības Tiesā saskaņā ar Līguma par Eiropas Savienības darbību 267. pantu.

126 *Peter Hustinx* runa 2010. gada 3. decembra konferencē „Uzsākot Datu saglabāšanas direktīvas īsteno anu".

aicinājis ES pieņemt visaptverošu tiesību aktu sistēmu, ar kuru ne tikai uzliktu pienākumus operatoriem saglabāt datus, bet arī regulētu to, kā dalībvalstis lieto šos datus tiesībaizsardzības nolūkiem, lai šādi radītu „tiesisko noteiktību pilsoņiem".

Datu aizsardzības iestādes vispār ir uzsvērušas, ka datu saglabāšana pati par sevi rada iespējamo privātās dzīves aizskaršanas risku, ko direktīva nerisina ES līmenī, bet tā vietā pieprasa dalībvalstīm nodrošināt, lai tiek ievēroti valsts datu aizsardzības noteikumi. Lai gan nav konkrētu privātās dzīves aizskāruma piemēri, ja neievieso turpmākus aizsardzības pasākumus, datu drošības pārkāpumu risks paliks un var pat palielināties, ņemot vērā tehnoloģiju attīstību un komunikāciju veidu tendences, neatkarīgi no tā, vai datus saglabā komerciāliem vai drošības nolūkiem un ES vai ārpus tās.

8. SECINĀJUMI UN IETEIKUMI

Šajā ziņojumā ir uzsvērti vairāki labumi, kas gūti no pašreizējā datu saglabāšanas režīma ES, kā arī jomas, kuras jāuzlabo. ES direktīvu pieņēma laikā, kad bija pastiprināts trauksmes stāvoklis attiecībā uz gaidāmajiem terorisma uzbrukumiem. Ietekmes novērtējums, ko Komisija ir paredzējusi veikt, sniedz iespēju novērtēt datu saglabāšanu ES attiecībā uz nepieciešamības un proporcionalitātes pārbaudēm un iekšējās drošības interesēs, kā arī izlīdzināt iekšējā tirgus darbību, stiprināt pamattiesību uz privāto dzīvi un personas datu aizsardzību ievērošanu. Komisijas priekšlikumam par datu saglabāšanas sistēmas pārskatu jābalstās uz zemāk minētajiem secinājumiem un ieteikumiem.

8.1. ES ir jāatbalsta un jāregulē datu saglabāšana kā drošības pasākums

Vairākums dalībvalstu uzskata, ka ES noteikumi par datu saglabāšanu ir nepieciešami kā instruments tiesībaizsardzības un kriminālās justīcijas sistēmām, kā arī upuru/cietušo aizsardzībai. Dalībvalstu iesniegtie pierādījumi statistikas un piemēru veidā zināmā mērā ir ierobežoti, tomēr, neskatoties uz to, tie liecina, ka saglabātie dati spēlē ļoti svarīgu lomu kriminālizmeklēšanā. Šie dati sniedz vērtīgus pavedienus un pierādījumus noziedzības novēršanā un kriminālvajāšanā un krimināltiesību nodrošināšanā. Datu lietošana ir vainagojusies ar pārkāpēju notiesāšanu par noziedzīgu nodarījumu veikšanu, kurus bez saglabātajiem datiem, iespējams, nekad nevarētu atklāt. Datu lietošana ir arī vainagojusies ar nevainīgu aizdomās turamo personu attaisnošanu. Saskaņotiem noteikumiem šajā jomā būtu jānodrošina, ka datu saglabāšana ir efektīvs instruments noziedzības apkarošanā, ka nozarei ir tiesiskā noteiktība pareizi funkcionējošā iekšējā tirgū un ka visā ES konsekventi piemēro augsta līmeņa standartus privātās dzīves un personas datu aizsardzībai.

8.2. Transponēšana nav bijusi vienmērīga

Transponēšanas tiesību akti ir spēkā 22 dalībvalstīs. Šī ievērojamā laika rezerve, kas piešķirta dalībvalstīm, lai pieņemtu datu saglabāšanas pasākumus saskaņā ar E-privātuma direktīvas 15. panta 1. punktu, padara Datu aizsardzības direktīvas novērtējumu ārkārtīgi sarežģītu. Transponēšanas tiesību aktos pastāv ievērojamas atšķirības attiecībā uz nolūku ierobežošanu, piekļuvi datiem, saglabāšanas termiņiem, datu aizsardzību un datu drošību un statistiku. Trīs dalībvalstis ir pārkāpušas direktīvu, jo to transponēšanas tiesību aktus attiecīgās konstitucionālās tiesas atcēla. Divām dalībvalstīm direktīva vēl ir jātransponē. Komisija turpinās strādāt kopā ar visām dalībvalstīm, lai palīdzētu nodrošināt efektīvu direktīvas īstenošanu. Komisija turpinās pildīt savu pienākumu īstenot ES tiesības, kā pēdējo līdzekli nepieciešamības gadījumā izmantojot arī pārkāpuma procedūru.

8.3. Direktīva nav pilnībā saskaņojusi pieeju datu saglabāšanai un nav radījusi līdzvērtīgus darbības apstākļus operatoriem

Direktīva ir nodrošinājusi, ka tagad datus saglabā lielākā daļa dalībvalstu. Direktīva pati par sevi negarantē to, ka saglabātos datus uzglabā, iegūst un lieto pilnīgi atbilstīgi privātās dzīves un personas datu aizsardzības tiesību principiem. Atbildība par šo tiesību ievērošanu gulstas uz dalībvalstu pleciem. Tā kā direktīvas mērķis bija tikai daļēji saskaņot datu saglabāšanas pieejas, nav pārsteidzoši, ka vienotas pieejas nav nedz attiecībā uz direktīvas īpašiem noteikumiem, piemēram, nolūku ierobežojumiem vai saglabāšanas termiņiem, nedz arī uz jautājumiem, kas neietilpst direktīvas darbības jomā, piemēram, izmaksu atlīdzināšanu. Tomēr, lai gan direktīva skaidri ir paredzējusi zināmu variāciju pakāpi, atšķirības datu saglabāšanas prasību piemērošanā valstīs ir lielākas un ir radījušas ievērojamas grūtības operatoriem.

8.4. Operatoriem konsekventi jāatlīdzina par radītajām izmaksām

Nozarē vēl aizvien nepastāv tiesiskā noteiktība. Pienākums saglabāt un iegūt datus operatoriem rada ievērojamas izmaksas, jo īpaši maziem operatoriem, un operatorus šis pienākums katrā dalībvalstī ietekmē atšķirīgi, arī izmaksu atlīdzināšana atšķiras, lai gan nav pierādījumu, ka kopumā telekomunikāciju nozari direktīva būtu ietekmējusi negatīvi. Komisijai apsvērs veidus, kā nodrošināt konsekventu izmaksu atlīdzināšanu operatoriem.

8.5. Proporcionalitātes nodrošināšana datu uzglabāšanas, izguves un lietošanas procesā

Komisija nodrošinās, ka ikvienā turpmākā priekšlikumā par datu saglabāšanu ir ievērots proporcionalitātes princips, ka priekšlikums ir atbilstīgs, lai sasniegtu mērķi – smagas noziedzības un terorisma apkarošana, un nepārkāpj noteikto darbības jomu. Komisija atzīs, ka ikvienu izņēmumu vai ierobežojumu attiecībā uz personas datu aizsardzību ir jāpiemēro tikai tik tālu, cik nepieciešams. Komisija rūpīgi novērtēs tiesībaizsardzības un kriminālās justīcijas sistēmu efektivitāti un lietderību, privātumu un valsts pārvaldei un operatoriem radītās izmaksas, kā arī saglabāto noslodzes datu uzglabāšanu, piekļuvi un lietošanu. Ietekmes novērtējumā jo īpaši jāizpēta šādas jomas:

- saskaņotība attiecībā uz datu saglabāšanas nolūku ierobežojumiem un noziegumu veidiem, saistībā ar kuriem saglabātajiem datiem var piekļūt un tos lietot;
- obligāto datu saglabāšanas termiņu lielāka saskaņotība un iespējama saīsināšana;
- neatkarīgas piekļuves pieprasījumu uzraudzības nodrošināšana saistībā ar kopējo datu saglabāšanas un piekļuves režīmu, ko piemēro visās dalībvalstīs;
- to iestāžu skaita ierobežošana, kurām atļauta piekļuve datiem;
- saglabājamo datu kategoriju samazināšana;
- vadlīnijas par tehniskajiem un organizatoriskajiem drošības pasākumiem saistībā ar piekļuvi datiem, tostarp attiecībā uz nodošanas procedūrām,
- norādījumi par datu lietošanu, tostarp datizraces novēršanu; un

- lietderīgas izvērtēšanas un ziņošanas procedūras izstrāde, lai veicinātu turpmākā instrumenta piemērošanas salīdzinājumu, kā arī novērtēšanu.

Tāpat arī Komisija izvērtēs, vai ES pieeja datu operatīvai saglabāšanai varētu papildināt datu saglabāšanu, un, ja varētu, tad kā.

Attiecībā uz pamattiesību „kontrolsarakstu" un pieeju informācijas pārvaldībai brīvības, drošības un tiesiskuma telpā[127], Komisija katru no šīm jomām novērtēs atbilstīgi proporcionalitātes principam un paredzamības prasībai. Tā arī nodrošinās saskaņotību ar pašreiz notiekošo ES datu aizsardzības tiesiskā regulējuma pārskatīšanas procesu[128].

8.6. Turpmākie pasākumi

Ņemot vērā šo novērtējumu, Komisija ierosinās pārskatīt esošo datu saglabāšanas sistēmu. Apspriežoties ar tiesībaizsardzības un tiesu varas iestādēm, nozares pārstāvjiem un patērētāju grupām, datu aizsardzības iestādēm un pilsoniskās sabiedrības organizācijām, Komisija izstrādās vairākus variantus. Komisija turpinās pētīt sabiedrības attieksmi pret datu saglabāšanu un datu saglabāšanas ietekmi uz sabiedrības uzvedību. Šos faktus iestrādās noteikto politikas variantu ietekmes novērtējumā, kas nodrošinās pamatu Komisijas priekšlikumam.

---

127 Sk. iepriekš atsauci uz paziņojumu par Pamattiesību hartas īstenošanu. „Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā", COM(2010)385, 20.07.2010.

128 COM (2010) 609, 4.11.2010.

Pielikums: papildu statistika par noslodzes datu saglabāšanu

Piezīmes pielikumam:

1. Datu vecums ir laiks, kas pagājis kopš datu saglabāšanas sākuma dienas un dienas, kurā kompetentā iestāde pieprasīja datu nosūtīšanu.

2. Ar internetu saistīti dati ir dati, kas attiecas uz interneta piekļuvi, interneta e-pastu un interneta telefoniju.

3. Čehijas Republikas, Latvijas un Polijas statistika ir pakļauta iebildumiem (sk. 5.1. nodaļu).

Dalībvalstu iesniegtā statistika par 2008. gadu

7. tabula: saglabāto datu pieprasījumu skaits, pēc vecuma, 2008. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	102691	18440	10110	319	0	0	0	0	131560
Dānija	2669	672	185	37	23	2	7	4	3599
Vācija	9363	2336	985	0	0	0	0	0	12684
Igaunija	2773	733	157	827	0	0	0	0	4490
Īrija	8981	2016	936	1855	90	85	78	54	14095
Grieķija	Nav iesniegts iedalījums pēc vecuma								584
Spānija	22629	15868	10298	4783	0	0	0	0	53578
Francija	Nav iesniegts iedalījums pēc vecuma								503437
Itālija	Nav iesniegti								
Kipra	30	4	0	0	0	0	0	0	34
Latvija	10539	2739	1368	1211	597	438	0	0	16892
Lietuva	55735	23817	5251	512	0	0	0	0	85315
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	810	59	0	0	0	0	0	0	869
Nīderlande	Nav iesniegts iedalījums pēc vecuma								85000
Austrija	Nav iesniegts iedalījums pēc vecuma								3093
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegts iedalījums pēc vecuma								2821
Slovākija	Nav iesniegti								
Somija	9134	1144	448	214	268				4008
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	315350	88339	34665	19398	6385	2973	1536	1576	470222
Kopā	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Izņemot Somiju

8. tabula: saglabāto datu pieprasījumu skaits, pēc veida, 2008. gads (iekavās to gadījumu skaits, kad pieprasījumu pēc datiem nevarēja izpildīt – ja iesniegts)				
Datu veids/ Dalībvalsts	**Fiksētā tīkla telefonija**	**Mobilā telefonija**	**Saistībā ar internetu**	**Kopā**
Beļģija	Nav iesniegti			
Bulgārija	Nav iesniegti			
Čehijas Republika	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Dānija	192 (0)	3273 (5)	134 (0)	3599 (5)
Vācija	Nav iesniegts iedalījums pēc datu veida			12684 (931)
Igaunija	4114 (1519)	376 (7)	Nav iesniegti	4490 (1526)
Īrija	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Grieķija	Nav iesniegts iedalījums pēc datu veida			584
Spānija	4448 (0)	40013 (0)	9117 (0)	53578 (0)
Francija	Nav iesniegts iedalījums pēc datu veida			503437
Itālija	Nav iesniegti			
Kipra	3 (0)	31 (5)	0 (0)	34 (5)
Latvija	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Lietuva	765 (72)	84550 (5657)	Nav iesniegti	85315 (5729)
Luksemburga	Nav iesniegti			
Ungārija	Nav iesniegti			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Nīderlande	Nav iesniegts iedalījums pēc datu veida			85000
Austrija	Nav iesniegts iedalījums pēc datu veida			3093
Polija	Nav iesniegti			
Portugāle	Nav iesniegti			
Rumānija	Nav iesniegti			
Slovēnija	Nav iesniegts iedalījums pēc datu veida			2821
Slovākija	Nav iesniegti			
Somija	Nav iesniegts iedalījums pēc datu veida			4008
Zviedrija	Nav iesniegti			
Apvienotā Karaliste	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Kopā				1392281

9. tabula: saglabāto *fiksētā tīkla telefonijas* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2008. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	3669	916	143	124	0	0	0	0	4852
Dānija	133	28	31	0	0	0	0	0	192
Vācija	Nav iesniegti								
Igaunija	1876	161	74	484	0	0	0	0	2595
Īrija	4118	712	197	182	32	21	23	16	5301
Grieķija	Nav iesniegti								
Spānija	1948	1431	741	328	0	0	0	0	4448
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	3	0	0	0	0	0	0	0	3
Latvija	698	213	167	193	104	137	0	0	1512
Lietuva	251	442	0	0	0	0	0	0	693
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	28	1	0	0	0	0	0	0	29
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	54805	27052	5340	753	1135	437	1050	175	90747
Kopā	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

10. tabula: saglabāto *mobilās telefonijas* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2008. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	98232	17013	7518	1	0	0	0	0	122764
Dānija	2433	628	143	33	20	1	7	3	3268
Vācija	Nav iesniegti								
Igaunija	248	58	35	28	0	0	0	0	369
Īrija	4326	820	230	240	57	63	52	37	5825
Grieķija	Nav iesniegti								
Spānija	17403	12114	7444	3052	0	0	0	0	40013
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	23	3	0	0	0	0	0	0	26
Latvija	8928	2298	1085	746	394	257	0	0	13708
Lietuva	55484	23375	14	20	0	0	0	0	78893
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	575	53	0	0	0	0	0	0	628
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	229375	52241	26228	16040	3333	521	339	1344	329421
Kopā	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

11. tabula: saglabāto *ar internetu saistīto* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2008. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	737	412	137	168	0	0	0	0	1454
Dānija	102	14	11	2	3	1	0	1	134
Vācija	Nav iesniegti								
Igaunija	Nav iesniegti								
Īrija	492	460	498	1422	0	0	0	0	2872
Grieķija	Nav iesniegti								
Spānija	3278	2323	2113	1403	0	0	0	0	9117
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	0	0	0	0	0	0	0	0	0
Latvija	424	150	75	219	74	34	0	0	976
Lietuva	Nav iesniegti								
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	76	3	0	0	0	0	0	0	79
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	31170	9046	3097	2605	1917	2015	147	57	50054
Kopā	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Dalībvalstu iesniegtā statistika par 2009. gadu

12. tabula: saglabāto datu pieprasījumu skaits, pēc vecuma, 2009. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	210975	56623	11620	1053	0	0	0	0	280271
Dānija	2980	685	179	104	54	38	12	14	4066
Vācija	Nav iesniegti								
Igaunija	4299	1836	1210	1065	0	0	0	0	8410
Īrija	8117	1652	805	297	168	134	69	41	11283
Grieķija	Nav iesniegti								
Spānija	29775	19346	13999	6970	0	0	0	0	70090
Francija	Nav iesniegts iedalījums pēc vecuma								514813
Itālija	Nav iesniegti								
Kipra	31	8	1	0	0	0	0	0	40
Latvija	20758	2414	1088	796	565	475	0	0	26096
Lietuva	30247	35456	5886	884	0	0	0	0	72473
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	3336	362	151	174	0	0	0	0	4023
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Polija	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovēnija	Nav iesniegts iedalījums pēc vecuma								1918
Slovākija	Nav iesniegts iedalījums pēc vecuma								5214
Somija	2000	1310	532	152	76	0	0	0	4070
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	Nav iesniegti								
Kopā	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

13. tabula: saglabāto datu pieprasījumu skaits, pēc veida, 2009. gads (iekavās to gadījumu skaits, kad pieprasījumu pēc datiem nevarēja izpildīt – ja iesniegts)				
Datu veids/ Dalībvalsts	**Fiksētā tīkla telefonija**	**Mobilā telefonija**	**Saistībā ar internetu**	**Kopā**
Beļģija	Nav iesniegti			
Bulgārija	Nav iesniegti			
Čehijas Republika	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Dānija	133 (0)	3771 (10)	162 (1)	4066 (11)
Vācija	Nav iesniegti			
Igaunija	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Īrija	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grieķija	Nav iesniegti			
Spānija	5055 (0)	56133 (0)	8902 (0)	70090 (0)
Francija	Nav iesniegts iedalījums pēc datu veida			514813
Itālija	Nav iesniegti			
Kipra	0 (0)	23 (3)	14 (0)	40 (3)
Latvija	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Lietuva	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luksemburga	Nav iesniegti			
Ungārija	Nav iesniegti			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Nīderlande	Nav iesniegti			
Austrija	Nav iesniegti			
Polija	Nav iesniegts iedalījums pēc datu veida			1048318
Portugāle	Nav iesniegti			
Rumānija	Nav iesniegti			
Slovēnija	Nav iesniegts iedalījums pēc datu veida			1918 (48)
Slovākija	Nav iesniegts iedalījums pēc datu veida			5214 (157)
Somija	Nav iesniegts iedalījums pēc datu veida			4070
Zviedrija	Nav iesniegti			
Apvienotā Karaliste	Nav iesniegti			
Kopā				2051082 (1069885)

14. tabula: saglabāto *fiksētā tīkla telefonijas* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2009. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	9919	2907	47	36	0	0	0	0	12909
Dānija	105	19	7	2	0	0	0	0	133
Vācija	Nav iesniegti								
Igaunija	2254	866	599	424	0	0	0	0	4143
Īrija	3934	337	69	70	50	39	16	11	4526
Grieķija	Nav iesniegti								
Spānija	2371	1492	844	348	0	0	0	0	5055
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	0	0	0	0	0	0	0	0	0
Latvija	744	253	157	143	68	89	0	0	1454
Lietuva	469	773	73	6	0	0	0	0	1321
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	83	25	18	20	0	0	0	0	146
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	Nav iesniegti								
Kopā	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

15. tabula: saglabāto *mobilās telefonijas* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2009. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	197620	48841	472	0	0	0	0	0	246933
Dānija	2777	639	162	98	47	19	12	7	3761
Vācija	Nav iesniegti								
Igaunija	318	397	96	70	0	0	0	0	881
Īrija	3669	835	220	210	115	92	50	28	5219
Grieķija	Nav iesniegti								
Spānija	24065	15648	11147	5273	0	0	0	0	56133
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	17	16	0	0	0	0	0	0	23
Latvija	18832	1912	778	515	394	263	0	0	22694
Lietuva	25713	19595	28	0	0	0	0	0	45336
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	2332	246	111	122	0	0	0	0	2811
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	Nav iesniegti								
Kopā	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

16. tabula: saglabāto ar *internetu saistīto* noslodzes datu, kas nosūtīti, pieprasījumu skaits, pēc vecuma, 2009. gads									
Pieprasīto datu vecums (mēneši)/ dalībvalsts	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Kopā**
Beļģija	Nav iesniegti								
Bulgārija	Nav iesniegti								
Čehijas Republika	3369	4811	861	942	0	0	0	0	9983
Dānija	98	27	10	4	4	7	0	1	151
Vācija	Nav iesniegti								
Igaunija	315	145	56	102	0	0	0	0	618
Īrija	489	455	502	0	0	0	0	0	1446
Grieķija	Nav iesniegti								
Spānija	3339	2206	2008	1349	0	0	0	0	8902
Francija	Nav iesniegti								
Itālija	Nav iesniegti								
Kipra	12	2	0	0	0	0	0	0	14
Latvija	852	198	74	90	88	86	0	0	1388
Lietuva	4060	15087	1	88	0	0	0	0	19236
Luksemburga	Nav iesniegti								
Ungārija	Nav iesniegti								
Malta	150	14	0	0	0	0	0	0	164
Nīderlande	Nav iesniegti								
Austrija	Nav iesniegti								
Polija	Nav iesniegti								
Portugāle	Nav iesniegti								
Rumānija	Nav iesniegti								
Slovēnija	Nav iesniegti								
Slovākija	Nav iesniegti								
Somija	Nav iesniegti								
Zviedrija	Nav iesniegti								
Apvienotā Karaliste	Nav iesniegti								
Kopā	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**