



EIROPAS KOPIENU KOMISIJA

Briselē, 21.9.2005
COM(2005) 438 galīgā redakcija

2005/0182 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

**par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru
pakalpojumu sniegšanu, ar ko labo Direktīvu 2002/58/EK**

(iesniegusi Komisija)

{SEC(2005) 1131}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Pilsoņi veic arvien vairāk ikdienas darbību un darījumu, izmantojot elektronisko sakaru tīklus un pakalpojumus. Šī saziņa rada informāciju par datu plūsmu vai datus par atrašanās vietu, kas satur, piemēram, ziņas par zvanītāja atrašanās vietu, izsaukto numuru, sarunas laiku un ilgumu. Apvienojumā ar datiem, kas ļauj identificēt pakalpojuma abonentu vai lietotāju, minētās informācijas par datu plūsmu pieejamība ir svarīga mērķiem, kas saistīti ar tiesībsardzību un drošību, piemēram, tādu nopietnu noziegumu novēršanai, izmeklēšanai, atklāšanai un kriminālvajāšanai kā terorisms un organizētā noziedzība.

Tomēr līdz ar pārmaiņām darījumu modeļos un pakalpojumu piedāvājumos, piemēram, tādu pakalpojumu pieaugumu kā vienotās likmes tarifi, priekšapmaksas un bezmaksas elektronisko sakaru pakalpojumi, ne vienmēr visi operatori spēj uzglabāt informāciju par datu plūsmu tādā apmērā, kā tas bija iespējams pēdējos gados atkarībā no piedāvātajiem pakalpojumiem. Šo tendenci pastiprina pēdējā laikā piedāvātie balss pārraides pakalpojumi, izmantojot interneta protokolu, vai pat vienotas likmes pakalpojumi fiksētajos telefona sakaros. Šādā režīmā operatoriem vairs nebūs nepieciešams uzglabāt informāciju par datu plūsmu rēķinu sagatavošanas mērķiem. Ja informācija par datu plūsmu netiek uzglabāta rēķinu sagatavošanas vai citiem darījumu mērķiem, valsts iestādēm tā nebūs pieejama gadījumos, kad ir likumīgs pamats piekļūt šai informācijai. Citiem vārdiem, šīs norises ļoti apgrūtina organizētās noziedzības un terorisma novēršanas pienākumu izpildi, ko veic valsts iestādes, un atvieglo noziedznieku savstarpējo sazināšanos, nebaudoties, ka tiesībsardzības iestādes varētu izmantot šos saziņas datus viņu kavēšanai.

Ir radusies nepieciešamība steidzami pieņemt saskaņotus nosacījumus šajā jautājumā ES līmenī. Vairākas dalībvalstis ir noteikušas vai arī plāno noteikt valsts mēroga pasākumus, kuros paredzēta prasība visiem operatoriem saglabāt noteiktus datu veidus, lai tos vajadzības gadījumā varētu izmantot iepriekš norādītajiem mērķiem. Atšķirības dalībvalstu tiesiskajos, regulēšanas un tehniskajos nosacījumos attiecībā uz informācijas par datu plūsmu saglabāšanu rada šķēršļus iekšējam elektronisko sakaru tirgum, jo pakalpojumu sniedzējiem tiek izvirzītas atšķirīgas prasības attiecībā uz saglabājamo datu veidiem, kā arī uz saglabāšanas nosacījumiem. Tāpēc ir nepieciešams tālāk saskaņot šos noteikumus atbilstoši EK Līguma 14. pantam.¹²⁰

• Vispārējais konteksts

Eiropas Padome 2004. gada 25. marta Deklarācijā par terorisma apkarošanu apstiprināja nepieciešamību pēc ES līmeņa noteikumiem, kas terorisma apkarošanas nolūkā garantē informācijas par datu plūsmu pieejamību visās 25 dalībvalstīs. Pēc teroristu rīkotajiem sprādzieniem Madridē Eiropas Padome deva norādījumus Padomei izvērtēt „priekšlikumus noteikumu izveidei operatoriem un pakalpojumu sniedzējiem attiecībā uz informācijas par datu plūsmu saglabāšanu”, lai tos pieņemtu 2005. gadā. Prioritāte, kas noteikta atbilstošu tiesību aktu pieņemšanai par šo tēmu, nesen tika apstiprināta 16. un 17. jūnija Eiropas Padomes atzinumos, kā arī Tieslietu

un iekšlietu padomes 2005. gada 13. jūlija īpašajā sanāksmē, kura notika pēc teroristu rīkotajiem sprādzieniem Londonā.

- **Spēkā esošie noteikumi šā priekšlikuma darbības jomā**

Direktīvas 2002/58/EK par privāto dzīvi un elektronisko komunikāciju 6. un 9. pants saskaņo personas datu aizsardzības noteikumus, kas ir piemērojami elektronisko sakaru pakalpojumu izmantošanas rezultātā iegūtās informācijas par datu plūsmu un atrašanās vietas datu apstrādei. Tad, kad šī informācija vairs nav nepieciešama pārraides mērķiem, tā ir jāizdzēš vai jāpadara anonīma, izņemot informāciju, kura ir nepieciešama rēķinu sagatavošanai vai norēķiniem par starpsavienojumiem; saņemot piekrišanu, noteiktu informāciju var apstrādāt arī mārketinga mērķiem un pievienotās vērtības pakalpojumu sniegšanai. 15. panta 1. punkts nosaka, ka dalībvalstis var pieņemt tiesību aktus, lai ierobežotu (citu starpā) 5., 6. un 9. pantā minētās darbības jomas, ja šādi ierobežojumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstošiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un kriminālpārkāpumu novēršanu, izmeklēšanu, noteikšanu un kriminālvajāšanu.

- **Atbilstība Eiropas Savienības mērķiem un politikai citās jomās**

Šis priekšlikums saskan ar Kopienas tiesību aktiem un Eiropas Savienības Pamattiesību hartu. Lai gan ir skaidrs, ka ierosinātā direktīva ietekmēs hartas 7. pantā garantētās pilsoņu tiesības uz privāto dzīvi, kā arī hartas 8. pantā garantētās tiesības uz personas datu aizsardzību, hartas 52. pants attaisno iejaukšanos šajās tiesībās. Šajā priekšlikumā paredzētie tiesību ierobežojumi ir samērīgi un nepieciešami, lai sasniegtu vispārējos noziedzības un terorisma novēršanas un apkarošanas mērķus.

Turklāt šī priekšlikuma ietekme uz pilsoņu privāto dzīvi ir ierobežota – pirmkārt, skaidri nosakot mērķus, kādiem var izmantot saglabātos datus, otrkārt, ierobežojot saglabājamo datu kategorijas, un, treškārt, ierobežojot datu saglabāšanas ilgumu. Vēl viens svarīgs papildu nodrošinājums ir tas, ka šī direktīva nav piemērojama komunikāciju saturam, jo tas nozīmētu telekomunikāciju pārtveršanu, kas ir ārpus šī tiesību akta darbības jomas.

Šīs direktīvas noteikumos paredzētā pakalpojumu sniedzēju un tīkla operatoru saglabāto personas datu apstrāde ir ietverta vispārējos un īpašajos datu aizsardzības noteikumos, kurus paredz Direktīva 95/46/EK un Direktīva 2002/58/EK, kas praksē nozīmē to, ka nav nepieciešami konkrēti papildu nosacījumi attiecībā uz vispārējiem datu aizsardzības principiem un datu drošību. Tas nozīmē arī to, ka minēto datu apstrāde pilnībā ietilps visās dalībvalstīs izveidoto datu aizsardzības iestāžu uzraudzības pilnvarās.

2. APSPRIEŠANĀS AR IEINTERESĒTĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMS

• Apspriešanās ar ieinteresētajām personām

Apspriešanās metodes, galvenās mērķnozares un vispārējs respondentu raksturojums

Jautājums par informācijas par datu plūsmu saglabāšanu tika ierosināts kibernetizācijas foruma sēdēs 2001. gadā, un kopš tā laika tas ir bijis konsultāciju priekšmets apspriedēs ar tiesībsardzības iestāžu pārstāvjiem, elektronisko sakaru nozares un datu aizsardzības ekspertiem.

Organizētās noziedzības foruma pārraudzībā 2004. gada 14. jūnijā tika organizēta īpaša apaļā galda tikšanās, kurā piedalījās tiesībsardzības, nozares un datu aizsardzības organizāciju pārstāvji. Gatavojoties 2004. gada 21. septembrī paredzētajam publiskajam semināram, 2004. gada 30. jūlijā Informācijas sabiedrības ģenerāldirektorāts un Tieslietu un iekšlietu ģenerāldirektorāts iesniedza kopīgu apspriežu dokumentu par datu saglabāšanu. Atbildot uz kopīgo apspriežu dokumentu, tika saņemts atbalsts un sekoja reakcija no dažādām pusēm, jo īpaši no nozares un civilo tiesību asociācijām. Turpmāku ieguldījumu Komisijai deva publiskais seminārs, kurš notika 21. septembrī.

Priekšlikuma sagatavošanā Komisija izmantoja arī plašas publiskas debates par šo jautājumu, to skaitā apspriedes Eiropas Parlamentā.

Atbilžu apkopojums un tas, kā tās ņemtas vērā

Apspriežu procesā apstiprinājās, ka informācijas saglabāšana par sakaru datu plūsmu ir nozīmīgs noziedzības un terorisma novēršanas un apkarošanas rīks tiesībsardzības iestādēm. Tiesībsardzības iestādes norādīja, ka, lai sasniegtu to mērķus, saglabāšanas periodam jābūt tik ilgam, cik ir nepieciešams, un tajā jāietver tik daudz informācijas, cik ir nepieciešams. Jo īpaši sarežģītās smagu noziedzumu izmeklēšanās, kuru pabeigšana var prasīt vairākus gadus, joprojām regulāri tiek pieprasīta vecāka informācija par datu plūsmu. Tika minēti vairāki piemēri lietās, kur šāda informācija ir izrādījusies būtiska kriminālizmeklēšanas gaitā, lielākoties izmeklējot tādus noziedzumus kā sprādzienu rīkošana un slepkavības.

Eiropas telekomunikāciju un interneta nozares pārstāvju organizāciju dalībnieki, kā arī atsevišķi elektronisko sakaru uzņēmumi iebilda, ka, lai gan tie piekrīt sadarboties un ir sadarbojušies ar tiesībsardzības iestādēm, ilgstoši saglabāšanas periodi radītu ievērojamas izmaksas, un datu konservācija būtu pietiekama. Tā kā liela daļa no datiem, kurus pieprasa tiesībsardzības iestādes, nav vecāki par sešiem mēnešiem, viņi tomēr lūdza noteikt saglabāšanas periodus, kas nav garāki par sešiem mēnešiem, kā arī izveidot mehānismus, lai kompensētu tiem radītās papildu izmaksas.

Datu aizsardzības iestāžu un civiltiesību asociāciju pārstāvji iebilda, ka datu saglabāšana ir iejaukšanās pilsoņu privātajā dzīvē, un šī iemesla dēļ saglabāšanas periodiem ir jābūt pēc iespējas īsākiem. Kopumā viņi apšaubīja, vai par samērīgiem uzskatāmi saglabāšanas periodu, kas ir garāki par sešiem mēnešiem. Viņi arī izteica bažas par šīs saglabāšanas galīgumu un mērķiem, kuri ir skaidri jānorāda.

Šis priekšlikums ir uzskatāms par līdzsvarotu pieeju un ir balstīts uz klāt pievienoto ietekmes novērtējumu. Vienu gadu ilgs saglabāšanas periods mobilās un fiksētās telefonijas informācijai par datu plūsmu un sešus mēnešus ilgs periods informācijai par datu plūsmu, kas saistīta ar interneta lietošanu, ietvers galvenās tiesībaizsardzības vajadzības, tajā pašā laikā ierobežojot iejaukšanos pilsoņu privātajā dzīvē un nozares izmaksas, kas saistītas ar tās saglabāšanu. Sešus mēnešus ilgs saglabāšanas periods attiecībā uz visiem datiem būtu par īsu, jo, kaut arī liela daļa no pieprasījumiem, kurus iesniedz tiesībaizsardzības iestādes, attiecas uz datiem, kas nav vecāki par sešiem mēnešiem, attiecībā uz visnopietnākajiem noziegumiem, piemēram, terorismu, organizēto noziedzību vai slepkavībām parasti tiek pieprasīti dati, kuri ir vecāki par sešiem mēnešiem.

- **Speciālu zināšanu vākšana un izmantošana**

Speciālas ārējas zināšanas nebija nepieciešamas.

- **Ietekmes novērtējums**

Tika izskatītas dažādas iespējas. Ar mērķi rast tādu risinājumu jautājumā par informācijas par datu plūsmu saglabāšanu, kas apmierina gan nepieciešamību pēc efektīva kriminālnoziedzumu novēršanas, atklāšanas, izmeklēšanas un kriminālvajāšanas rīka, gan pēc fizisku personu pamata tiesību un brīvību aizsardzības rīka, jo īpaši tiesību uz privāto dzīvi, datu aizsardzību un sarakstes noslēpumu, Padome 2002. gadā nepārprotami aicināja uz dialogu valstu un ES līmenī. Lai gan par šo jautājumu notika plašas publiskas apspriešanas un debates, ieskaitot diskusijas Eiropas Parlamentā, kopējs risinājums netika rasts.

Ja netiks izrādīta iniciatīva datu saglabāšanas jautājumā, saglabāsies esošā dažādība datu saglabāšanas noteikumos. Nesaistošu tiesību normu ieviešana tika noraidīta, jo tā nenodrošina atbilstošu juridiskās noteiktības līmeni. Trešā pīlāra iniciatīva par datu saglabāšanas saistībām tika noraidīta, jo tā būtu pretrunā Kopienas likumam. Eiropas Padome ir aicinājusi uz tiesisku pieeju arī deklarācijā par terorisma apkarošanu.

Direktīvas priekšlikuma iespējama pieņemšana nodrošina saskaņošanas līmeni, kas ir nepieciešams iekšējā tirgū. Salīdzinājumā ar regulu tas atstāj dalībvalstīm zināmas manevru iespējas ieviešanā jutīgā zonā. Regula būtu pārāk stingra, jo īpaši, ņemot vērā atšķirīgās tehniskās arhitektūras, kuras izmanto dažādi operatori dažādās valstīs. Direktīva atstās dalībvalstīm pietiekamas iespējas pielāgoties valstu ierobežojumiem. Jebkurā gadījumā, ņemot vērā šķēršļus, kurus brīvai pakalpojumu sniegšanai radījuši atšķirīgie valstu noteikumi šajā jomā, *status quo* vairs nav saglabājams. Uz šā tiesību akta un konkrētās EK 95. pantā paredzētās juridiskās bāzes izvēli norādīja arī juridiskā analīze, kas izklāstīta 2005. gada 22. marta Komisijas dienestu darba dokumentā SEK (2005) 420. Komisija veica ietekmes novērtējumu, un ziņojums par to ir pieejams http://europa.eu.int/comm/dgs/justice_home/evaluation/dg_coordination_evaluation_annexe_en.htm.

3. PRIEKŠLIKUMA JURIDISKIE ASPEKTI

- **Ierosinātās rīcības kopsavilkums**

Ierosinātās direktīvas mērķis ir saskaņot publiski pieejamu elektronisko sakaru pakalpojumu sniedzēju vai publiskā sakaru tīkla operatoru saistības attiecībā uz noteiktas informācijas par datu plūsmu saglabāšanu, lai to varētu sniegt kompetentām dalībvalstu iestādēm tādu nopietnu noziegumu kā terorisms un organizētā noziedzība novēršanai, izmeklēšanai, atklāšanai un kriminālvajāšanai.³¹⁰

- **Juridiskais pamats**

EK Līguma 95. pants.

- **Subsidiaritātes princips**

Subsidiaritātes principu piemēro, ciktāl priekšlikums nav Kopienas ekskluzīvā kompetencē.

Dalībvalstis nevar pietiekami sasniegt priekšlikuma mērķus šāda(-u) iemesla(-u) dēļ.

Dalībvalstis pašas nevar panākt informācijas par datu plūsmu saglabāšanas periodu saskaņošanu. ES rīcība, uz kuru aicināja Eiropas Padome, nodrošinās informācijas par datu plūsmu saglabāšanu visā Eiropas Savienībā un padarīs to pieejamu tiesībsardzības iestādēm.

Tā kā tiesībsardzības iestāžu veikto izmeklēšanu efektivitāte lielā mērā ir atkarīga no starptautiskas sadarbības un valstu atšķirīgām izvēlēm ir negatīva ietekme uz elektronisko sakaru tirgu, vispiemērotākā izvēlētā politika ir shēmu saskaņošana informācijas par datu plūsmu saglabāšanai Eiropas mērogā. Izmaksu atlīdzināšanas princips ļaus radīt elektronisko sakaru pakalpojumu sniedzējiem līdzvērtīgus darbības apstākļus iekšējā tirgū.

Priekšlikuma mērķi būs labāk sasniedzami ar Kopienas rīcību šāda(-u) iemesla(-u) dēļ.

Priekšlikuma mērķi būs labāk sasniedzami ar ES rīcību, nodrošinot informācijas par datu plūsmu saglabāšanu visā Eiropas Savienībā un padarot to pieejamu tiesībsardzības iestādēm ar tādiem pašiem nosacījumiem. Pateicoties iespējai standartizēt tehnoloģijas, tas arī dos labumu elektronisko sakaru nozarei, jo īpaši tiem uzņēmumiem, kuri piedāvā pakalpojumus vairākās dalībvalstīs.³²⁵

Kvalitatīvie rādītāji, kas liecina, ka mērķus var labāk sasniegt Savienība, ir tiesībsardzības iestāžu efektivitāte noziedzības un terorisma novēršanā un apkarošanā, īpaši tādos gadījumos kā organizētā noziedzība un terorisms, kam bieži ir pārrobežu raksturs.³²⁷

Priekšlikums aprobežojas ar to, ko dalībvalstis nespēj apmierinoši panākt, un ko Savienība var izdarīt labāk, ierobežojot datu saglabāšanas saistību apjomu elektronisko sakaru pakalpojumu sniedzējiem vai publiski pieejama sakaru tīkla

operatoriem. Priekšlikums ļauj dalībvalstīm izvēlēties, kurām iestādēm un ar kādiem nosacījumiem jānodrošina piekļuve saglabātajiem datiem. Piekļuve informācijai un informācijas apmaiņa starp attiecīgām tiesībaizsardzības iestādēm ir jautājums, kas neietilpst EK līguma darbības jomā.

Šajā kontekstā ir vērts piebilst, ka atbilstoši Līgumam par Eiropas Savienību Komisija pašlaik gatavo tiesību aktu priekšlikumu projektus attiecībā uz principu, kas paredz informācijas pieejamību tiesībaizsardzības mērķiem, un attiecībā uz datu aizsardzības principu noteikšanu trešā pīlāra vajadzībām. Turklāt jāpiebilst, ka saskaņā ar šo direktīvu piekļuve saglabātajiem datiem atļauta vienīgi tiesībaizsardzības nolūkos, t.i., elektronisko sakaru pakalpojumu sniedzējiem ir liegta piekļuve saglabātajiem datiem.

Tāpēc priekšlikums atbilst subsidiaritātes principam.

- **Proporcionalitātes princips**

Priekšlikums atbilst proporcionalitātes principam, jo tā ietekme uz pilsoņiem un uz nozari ir ierobežota līdz maksimāli iespējamam apjomam. Jāatceras, ka šis tiesību akts attiecas tikai uz informāciju par datu plūsmu, kuru apstrādā elektronisko sakaru pakalpojumu sniedzēji. Elektronisko sakaru saturs neietilpst šīs direktīvas darbības jomā.

Pamata tiesību un brīvību, jo īpaši tiesību uz dzīvi ievērošana un stingri privātās dzīves neaizskaramības pārkāpšanas ierobežojumi bija galvenais virzītājspēks, lai atrastu visatbilstošāko līdzsvaru starp visām iesaistītajām interesēm – sociālajām, ekonomiskajām, drošības un privātuma – interesēm.

Līdz ar to šajā direktīvas priekšlikumā ir ņemta vērā proporcionalitāte, jo īpaši attiecībā uz ierosinātajiem saglabāšanas periodiem, atšķirība starp telefona un interneta datiem, saglabājamo datu kategoriju ierobežojums un izmaksu atlīdzināšanas shēma. Jo īpaši šis priekšlikums stingri ierobežo mērķus, kādiem saglabātos datus atļauts sniegt tiesībaizsardzības iestādēm. Saglabātajiem datiem būs pilnībā piemērojami tiesību akti par datu aizsardzību, savukārt ietekme uz individuālajām tiesībām un ekonomiskā procesa dalībniekiem tiek ierobežota, izvēloties ierobežotu informācijas par datu plūsmu kopumu, kuru nepieciešams saglabāt. Turklāt atšķirībā no informācijas par datu plūsmu, kura iegūta, izmantojot „standarta” mobilo un fiksēto telefoniju, attiecībā uz īsāko saglabāšanas periodu, kas noteikts informācijai par datu plūsmu, kura iegūta, izmantojot internetu, tiek ņemta vērā pašreizējā uzņēmējdarbības prakse un ievērojami samazināts saglabājamo datu apjoms.

Valstu valdību, ekonomiskā procesa dalībnieku un pilsoņu finansiālais un administratīvais slogs ir samazināts vairākos veidos. Pirmkārt, direktīva paredz saskaņošanu, kas nozīmē samazinātas atbilstības nodrošināšanas izmaksas elektronisko sakaru pakalpojumu sniedzējiem vai publiskā sakaru tīkla operatoriem. Otrkārt, izmaksas ir samazinātas, nosakot stingrus ierobežojumus attiecībā uz datu saglabāšanas periodiem un saglabājamo datu kopām. Ņemot vērā pasākuma nozīmīgumu noziedzības un terorisma novēršanā un apkarošanā, papildu izmaksas, kas jāsedz dalībvalstīm saskaņā ar izmaksu atlīdzināšanas nosacījumu, ir uzskatāmas par samērīgām (sk. ietekmes novērtējumu).

Tāpat arī jāuzsver, ka direktīva neierobežo dalībvalstu iespējas pieprasīt īpašus datu konservācijas pasākumus, piemēram, gadījumā, ja aizdomās turētais vai kāds noziedzīgs grupējums jau ir atklāts, vai arī konkrētu notikumu, piemēram, teroristu uzbrukumu gadījumā.

- **Tiesību aktu izvēle**

Ierosinātie tiesību akti: direktīva.

Citi līdzekļi nebūtu piemēroti šāda(-u) iemesla(-u) dēļ.

Jautājums par pareizo juridisko pamatu priekšlikumam par informācijas par datu plūsmu saglabāšanu nesen tika skatīts Komisijas personāla darba dokumentā. Īsāk sakot, šajā dokumentā izklāstītais viedoklis ir tāds, ka jautājums par informācijas par datu plūsmu saglabāšanu jau ir risināts iepriekšējos tiesību aktos, balstoties uz pirmā pīlāra juridisko pamatu, piemēram, iepriekš minētajā Direktīvā 2002/58/EK un Direktīvā 95/46/EK. Analīze joprojām rāda, ka Direktīvā 2002/58/EK jautājums netika pilnībā saskaņots tikai tāpēc, ka nebija iespējams panākt politisku lēmumu par datu saglabāšanas faktisko ilgumu, un analīzē secināts, ka līdz ar to jebkādi turpmāki tiesību akti par informācijas par datu plūsmu saglabāšanu kā tādu (pretstatā noteikumam, kas reglamentē minēto datu apmaiņu un tiesībaizsardzības iestāžu piekļuvi minētajiem datiem) ir jāpieņem, pamatojoties uz pirmā pīlāra juridisko bāzi. Šī loģika ir saskaņā ar Līguma par Eiropas Savienību 47. pantu, kas reglamentē attiecības starp Līgumu par Eiropas Savienību un EK līgumu un paredz, ka neviens tiesību akts, kas pieņemts saskaņā ar Līgumu par Eiropas Savienību, nedrīkst ietekmēt saskaņā ar EK līgumu pieņemto tiesisko regulējumu.

4. IETEKME UZ BUDŽETU

Priekšlikums neietekmē Kopienas budžetu.

5. PAPILDU INFORMĀCIJA

- **Pārskatīšanas/revīzijas/termiņa izbeigšanās klauzula**

Priekšlikumā ietverta pārskatīšanas klauzula. Lai palīdzētu Komisijai izpildīt pārskatīšanas uzdevumu, paredzēts izveidot datu saglabāšanas darba grupu. Minētā grupa var sasaukt kopā elektronisko sakaru tehniskos ekspertus, kā arī tiesībaizsardzības un datu aizsardzības iestāžu pārstāvjus.

- **Atbilstības tabula**

Dalībvalstīm jādara Komisijai zināms to valsts noteikumu teksts, ar kuriem transponē šo direktīvu, kā arī jāiesniedz minēto noteikumu un šīs direktīvas atbilstības tabula.

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA

par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu, ar ko labo Direktīvu 2002/58/EK

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un jo īpaši tā 95. pantu,

ņemot vērā Komisijas priekšlikumu¹,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu²,

ņemot vērā Reģionu komitejas atzinumu³,

saskaņā ar Līguma 251. pantā noteikto procedūru,

tā kā:

- (1) Eiropas Parlamenta un Padomes Direktīva 95/46/EK par fizisku personu aizsardzību attiecībā uz personas datu apstrādi⁴ nosaka, ka dalībvalstīm jānodrošina fizisku personu tiesības un brīvības attiecībā uz personas datu apstrādi un jo īpaši viņu tiesības uz privāto dzīvi, lai panāktu personas datu brīvu plūsmu Kopienā.
- (2) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē⁵ principus, kas izklāstīti Direktīvā 95/46/EK, pārveido par īpašiem noteikumiem elektronisko komunikāciju nozarē.
- (3) Direktīvas 2002/58/EK 5., 6. un 9. pants definē noteikumus, kuri piemērojami informācijas par datu plūsmu un atrašanās vietas datu apstrādei, ko veic tīkla operatori un pakalpojumu sniedzēji, un kuri iegūti, izmantojot elektronisko sakaru pakalpojumus. Tad, kad minētā informācija vairs nav nepieciešama komunikācijas pārraidīšanai, tā ir jāizdzēš vai jāpadara anonīma, izņemot datus, kuri ir nepieciešami rēķinu sagatavošanai vai norēķiniem par starpsavienojumiem; saņemot piekrišanu, noteiktus datus var apstrādāt arī mārketinga mērķiem un pievienotās vērtības pakalpojumu sniegšanai.

¹ OV C [...], [...], [...]. lpp.

² OV C [...], [...], [...]. lpp.

³ OV C [...], [...], [...]. lpp.

⁴ OV L 281, 23.11.1995., 31. lpp.

⁵ OV L 201, 30.7.2002., 37. lpp.

- (4) Direktīvas 2002/58/EK 15. panta 1. punktā izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis var ierobežot direktīvas 5. pantā, 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā minēto tiesību un pienākumu darbības jomu; šādi izņēmumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, t.i., lai garantētu valstu drošību (t.i., valsts drošību), aizsardzību, sabiedrības drošību un kriminālpārskatību vai elektronisko sakaru sistēmu nesankcionētas izmantošanas novēršanu, izmeklēšanu, atklāšanu un kriminālvajāšanu.
- (5) Vairākas dalībvalstis ir pieņēmušas tiesību aktus, kuri paredz, ka pakalpojumu sniedzēji saglabā datus noziedzības un kriminālnoziedzumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem; dažādu valstu tiesību aktu nosacījumi ievērojami atšķiras.
- (6) Juridiskās un tehniskās atšķirības valstu nosacījumos attiecībā uz datu saglabāšanu kriminālnoziedzumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem rada šķēršļus iekšējo elektronisko sakaru tirgum. Pakalpojumu sniedzējiem tiek izvirzītas atšķirīgas prasības attiecībā uz saglabājamās informācijas par datu plūsmu veidiem, kā arī uz saglabāšanas nosacījumiem un periodiem.
- (7) Tieslietu un iekšlietu padomes 2001. gada 20. septembra secinājumos izteikts aicinājums nodrošināt iespēju tiesībaizsardzības iestādēm izmeklēt noziedzīgas darbības, kas saistītas ar elektronisko sakaru izmantošanu, un veikt juridiskus pasākumus pret šo noziedzumu izdarītājiem, tajā pašā laikā panākot līdzsvaru starp personas datu aizsardzību un tiesībaizsardzības iestāžu nepieciešamību piekļūt datiem kriminālizmeklēšanas mērķiem.
- (8) Tieslietu un iekšlietu padomes 2002. gada 19. decembra secinājumos uzsvērts, ka sakarā ar elektronisko sakaru iespēju ievērojamo pieaugumu īpaši svarīgi ir dati, kuri attiecas uz elektronisko sakaru izmantošanu, un tāpēc tie ir vērtīgs noziedzības un kriminālnoziedzumu, jo īpaši organizētās noziedzības novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas rīks.
- (9) Deklarācijā par terorisma apkarošanu, kuru Eiropas Padome pieņēma 2004. gada 25. martā, doti norādījumi Padomei pārbaudīt pasākumus noteikumu izveidei pakalpojumu sniedzējiem attiecībā uz informācijas par datu plūsmu saglabāšanu.
- (10) Deklarācijā, kuru 2005. gada 13. jūlijā pieņēma īpaša neformāla padome, uzsvērtā nepieciešamība pēc iespējas ātrāk pieņemt pasākumus attiecībā uz informācijas par elektronisko sakaru datu plūsmu saglabāšanu.
- (11) Ņemot vērā informācijas par datu plūsmu nozīmi tādu nopietnu kriminālnoziedzumu kā terorisms un organizētā noziedzība novēršanā, izmeklēšanā, atklāšanā un kriminālvajāšanā, par ko liecina vairāku dalībvalstu veiktie pētījumi un praktiskā pieredze, ir nepieciešams nodrošināt, lai dati, kurus apstrādā elektronisko sakaru pakalpojumu sniedzēji, piedāvājot publiskos elektronisko sakaru pakalpojumus vai publiskos sakaru tīklus, tiktu saglabāti noteiktu laika periodu.
- (12) Saglabājamās informācijas kategorijas atspoguļo atbilstošu līdzsvaru starp priekšrocībām, ko dod nopietnu noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana un kriminālvajāšana, un privātās dzīves neaizskaramības pārkāpuma līmeni, ko tā izraisīs. Arī piemērojamais saglabāšanas periods – viens gads un attiecīgi seši

mēneši, ja dati attiecas uz elektroniskajiem sakariem, kuri notiek, izmantojot vienīgi interneta protokolu, nodrošina saprātīgu visu attiecīgo interešu ievērošanu.

- (13) Ņemot vērā, ka datu saglabāšana rada ievērojamas papildu izmaksas elektronisko sakaru operatoriem, bet tās priekšrocības attiecībā uz sabiedrības drošību ietekmē sabiedrību kopumā, ir lietderīgi paredzēt, ka dalībvalstis operatoriem atlīdzina pierādītās izmaksas, kuras tiem radušās sakarā ar saistību izpildi, ko uzliek šī direktīva.
- (14) Tehnoloģijas, kas saistītas ar elektroniskajiem sakariem, strauji mainās, un var mainīties kompetento iestāžu likumīgās prasības; lai konsultētu šajos jautājumos, Komisija paredz izveidot darba grupu, kas sastāv no tiesībaizsardzības iestāžu, elektronisko sakaru nozares un datu aizsardzības iestāžu pārstāvjiem.
- (15) Jāatceras, ka Direktīva 95/46/EK un Direktīva 2002/58/EK ir pilnībā piemērojamas datiem, kuri saglabāti atbilstoši šai direktīvai. Direktīvas 95/46/EK 30. panta 1. punkta c) apakšpunkts pieprasa konsultēšanos ar „29. pantā minēto darba grupu”.
- (16) Ir būtiski, lai dalībvalstis izstrādātu tiesību aktus, kas nodrošina, ka dati, kuri saglabāti saskaņā ar šo direktīvu, tiek sniegti vienīgi kompetentām valstu iestādēm saskaņā ar valstu tiesību aktiem, pilnībā ievērojot attiecīgo personu pamattiesības; minētie tiesību akti ietver atbilstošus nosacījumus, ierobežojumus un drošības pasākumus, lai nodrošinātu saglabāto datu sniegšanas atbilstību pamattiesībām, ko jo īpaši garantē Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencija.
- (17) Pasākumi, kas nepieciešami šīs direktīvas izpildei, ir jāpieņem saskaņā ar Padomes 1999. gada 28. jūnija Lēmumu 1999/468/EK, ar ko nosaka Komisijai piešķirto ieviešanas pilnvaru īstenošanas kārtību⁶.
- (18) Dalībvalstis nevar pietiekamā mērā sasniegt darbības mērķus, proti, saskaņot pakalpojumu sniedzēju saistības attiecībā uz konkrētu datu saglabāšanu un šo datu pieejamības nodrošināšanu tādu nopietnu kriminālnoziedzumu kā terorisms un organizētā noziedzība novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, un šīs darbības mēroga un ietekmes dēļ šos mērķus var labāk sasniegt Kopienas līmenī. Tāpēc Kopiena var pieņemt tiesību aktus saskaņā ar subsidiaritātes principu, kas noteikts Līguma 5. pantā. Saskaņā ar minētajā pantā izklāstīto proporcionālītātes principu direktīva nosaka tikai to, kas ir vajadzīgs, lai sasniegtu minētos mērķus.
- (19) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti Eiropas Savienības Pamattiesību hartā; jo īpaši šīs direktīvas un Direktīvas 2002/58/EK mērķis ir pilnībā nodrošināt pamattiesības, lai ievērotu pilsoņu privātās dzīves un komunikācijas un personas datu aizsardzību (hartas 7. un 8. pants),

⁶ OV L 184, 17.7.1999., 23. lpp.

IR PIENĒMUSI ŠO DIREKTĪVU.

1. pants

Priekšmets un darbības joma

1. Šīs direktīvas mērķis ir saskaņot dalībvalstu noteikumus attiecībā uz publiski pieejamu elektronisko sakaru pakalpojumu sniedzēju vai publiskā sakaru tīkla operatoru saistībām, kas attiecas uz noteiktu datu apstrādi un saglabāšanu, lai nodrošinātu, ka šī informācija ir pieejama tādu nopietnu noziegumu kā terorisms un organizētā noziedzība novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.
2. Šo direktīvu piemēro gan informācijai par privātpersonu, gan juridisku personu datu plūsmu un atrašanās vietas datiem, kā arī ar tiem saistītiem datiem, kas ir nepieciešami abonenta vai reģistrēta lietotāja identificēšanai. To nepiemēro elektronisko sakaru saturam, tai skaitā informācijai, kura skatīta, izmantojot elektronisko sakaru tīklu.

2. pants

Definīcijas

1. Šajā direktīvā piemērojamas Direktīvā 95/46/EK, Direktīvā 2002/21/EK ⁷, kā arī Direktīvā 2002/58/EK lietotās definīcijas.
2. Šajā direktīvā
 - a) „dati” ir informācija par datu plūsmu un atrašanās vietas dati, kā arī ar tiem saistīti dati, kas ir nepieciešami abonenta vai lietotāja identificēšanai;
 - b) „lietotājs” ir jebkura fiziska persona, kas izmanto publiski pieejamu elektronisko sakaru pakalpojumu personīgiem vai uzņēmējdarbības mērķiem, ne vienmēr būdama šā pakalpojuma abonents.

3. pants

Pienākums saglabāt datus

1. Atkāpjoties no Direktīvas 2002/58/EK 5., 6. un 9. panta, dalībvalstis pieņem pasākumus, lai nodrošinātu, ka dati, kurus iegūst un apstrādā publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji vai publiskā sakaru tīkla operatori, sniedzot sakaru pakalpojumus savā jurisdikcijā, tiek saglabāti atbilstoši šīs direktīvas noteikumiem.
2. Dalībvalstis pieņem pasākumus, lai nodrošinātu, ka dati, kuri saglabāti atbilstoši šai direktīvai, tiek sniegti vienīgi kompetentām valsts iestādēm īpašos gadījumos un

⁷ OV L 108, 24.4.2002., 33. lpp.

saskaņā ar valsts tiesību aktiem tādu nopietnu noziegumu kā terorisms un organizētā noziedzība novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

4. pants

Saglabājamo datu kategorijas

Dalībvalstis nodrošina šādu datu kategoriju saglabāšanu atbilstoši šai direktīvai:

- (a) dati, kuri ir nepieciešami, lai izsekotu un identificētu komunikācijas avotu;
- (b) dati, kuri ir nepieciešami, lai izsekotu un identificētu komunikācijas galamērķi;
- (c) dati, kuri ir nepieciešami, lai noteiktu komunikācijas datumu, laiku un ilgumu;
- (d) dati, kuri ir nepieciešami, lai noteiktu komunikācijas veidu;
- (e) dati, kuri ir nepieciešami, lai identificētu sakaru ierīci vai ierīci, kas veic tās funkcijas;
- (f) dati, kuri ir nepieciešami, lai noteiktu mobilo sakaru iekārtas atrašanās vietu.

Datu veidi, kuri ir jā saglabā atbilstoši iepriekš minētajām datu kategorijām, norādīti pielikumā.

5. pants

Pielikuma pārskatīšana

Pielikums tiek pēc vajadzības regulāri pārskatīts atbilstoši 6. panta 2. punktā minētajai procedūrai.

6. pants

Komiteja

1. Komisijai palīdz dalībvalstu pārstāvju komiteja, ko vada Komisijas pārstāvis.
2. Ja ir atsauce uz šo punktu, tad piemēro Lēmuma 1999/468/EK 5. un 7. pantu, ņemot vērā šī lēmuma 8. panta noteikumus.
3. Lēmuma 1999/468/EK 5. panta 6. punktā paredzētais laika posms ir trīs mēneši.

7. pants

Saglabāšanas periodi

Dalībvalstis nodrošina, lai 4. pantā minētās datu kategorijas tiktu saglabātas vienu gadu no komunikācijas datuma, izņemot datus, kas attiecas uz elektroniskajiem sakariem, kuri notiek, pilnībā vai galvenokārt izmantojot interneta protokolu. Šie dati tiek saglabāti 6 mēnešus.

8. pants
Saglabāto datu uzglabāšanas prasības

Dalībvalstis nodrošina, lai saskaņā ar šo direktīvu dati tiktu saglabāti tā, ka saglabātos datus un jebkuru citu nepieciešamo informāciju, kas saistīta ar minētajiem datiem, būtu iespējams nekavējoši nodot kompetentajām iestādēm.

9. pants
Statistika

Dalībvalstis nodrošina, lai Eiropas Komisijai katru gadu tiktu iesniegta statistika par saglabātajiem datiem, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu. Šī statistika ietver

- gadījumus, kad informācija sniegta kompetentām iestādēm saskaņā ar piemērojamiem valsts tiesību aktiem;
- laiku, kas pagājis kopš datu saglabāšanas datuma līdz datumam, kad kompetentā iestāde ir pieprasījusi šo datu nosūtīšanu;
- gadījumus, kad nav bijis iespējams izpildīt pieprasījumus pēc datiem.

Minētā statistika neietver personas datus.

10. pants
Izmaksas

Dalībvalstis nodrošina, lai publiski pieejamu elektronisko sakaru pakalpojumu sniedzējiem vai publisko sakaru tīklu operatoriem tiktu atlīdzinātas pierādītās papildu izmaksas, kuras tiem radušās sakarā ar saistību izpildi, ko uzliek šī direktīva.

11. pants
Direktīvas 2002/58/EK grozījums

Lēmuma 2002/58/EK 15. pantā iekļauj šādu 1.a punktu:

„1a. 1. punkts neattiecas uz saistībām, kuras izriet no Direktīvas 2005/..../EK attiecībā uz datu saglabāšanu tādu nopietnu noziegumu kā terorisms un organizētā noziedzība novēršanai, izmeklēšanai, atklāšanai un kriminālvajāšanai. ** OV L,”.

12. pants
Vērtēšana

1. Ne vēlāk kā trīs gadus pēc 13. panta 1. punktā minētā datuma, ņemot vērā statistikas datus, kuri iesniegti Komisijai atbilstoši 9. pantam, Komisija iesniedz Eiropas Parlamentam un Padomei šīs direktīvas piemērošanas vērtējumu un vērtējumu par tās ietekmi uz ekonomiskā procesa dalībniekiem un patērētājiem, lai noteiktu, vai ir

nepieciešams grozīt šīs direktīvas nosacījumus, jo īpaši attiecībā uz 7. pantā paredzēto saglabāšanas periodu.

2. Tādēļ Komisija pārbauda visus apsvērumus attiecībā uz personas datu apstrādi, kurus sniedz dalībvalstis vai darba grupa personu aizsardzībai, kas izveidota atbilstoši Direktīvas 95/46/EK 29. pantam.

13. pants

Transponēšana

1. Dalībvalstīs stājas spēkā likumi, noteikumi un administratīvie akti, kas vajadzīgi, lai izpildītu šīs direktīvas prasības [vēlākais 15 mēnešu laikā pēc direktīvas pieņemšanas]. Dalībvalstis tūlīt dara Komisijai zināmus minēto noteikumu tekstus, kā arī minēto noteikumu un šīs direktīvas atbilstības tabulu. Kad dalībvalstis pieņem minētos noteikumus, tajos ietver norādi uz šo direktīvu vai šādu norādi pievieno to oficiālajai publikācijai. Dalībvalstis nosaka, kā izdarāma šāda atsauce.
2. Dalībvalstis dara Komisijai zināmus valsts tiesību aktu galvenos noteikumus, ko tās pieņem jomā, uz kuru attiecas šī direktīva.

14. pants

Stāšanās spēkā

Šī direktīva stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

15. pants

Adresāti

Šī direktīva ir adresēta dalībvalstīm.

Briselē,

*Eiropas Parlamenta vārdā
priekšsēdētājs*

*Padomes vārdā
priekšsēdētājs*

PIELIKUMS

Datu veidi, kuri ir jāsaglabā atbilstoši šīs direktīvas 4. pantā norādītajām kategorijām.

- a) Dati, kuri ir nepieciešami, lai izsekotu un identificētu komunikācijas avotu.
- (1) Attiecībā uz fiksētā tīkla telefoniju:
 - (a) izsaucēja tālruņa numurs;
 - (b) abonenta vai reģistrētā lietotāja uzvārds un adrese.
 - (2) Attiecībā uz mobilo telefoniju:
 - (a) izsaucēja tālruņa numurs;
 - (b) abonenta vai reģistrētā lietotāja uzvārds un adrese.
 - (3) Attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:
 - (a) interneta protokola (IP) dinamiskā vai statiskā adrese, kuru komunikācijai piešķīris interneta piekļuves nodrošinātājs;
 - (b) komunikācijas avota lietotāja ID;
 - (c) pieslēguma marķējums vai tālruņa numurs, kas piešķirts visai komunikācijai, kura ienāk publiskajā telefonu tīklā;
 - (d) abonenta vai reģistrētā lietotāja uzvārds un adrese, kuram komunikācijas laikā piešķirta IP adrese, pieslēguma marķējums vai lietotāja ID.
- b) Dati, kuri ir nepieciešami, lai izsekotu un identificētu komunikācijas galamērķi.
- (1) Attiecībā uz fiksētā tīkla telefoniju:
 - (a) izsauktais tālruņa numurs vai numuri;
 - (b) abonenta(-u) vai reģistrētā(-o) lietotāja(-u) uzvārds(-i) un adrese(-s).
 - (2) Attiecībā uz mobilo telefoniju:
 - (a) izsauktais tālruņa numurs vai numuri;
 - (b) abonenta(-u) vai reģistrētā(-o) lietotāja(-u) uzvārds(-i) un adrese(-s).
 - (3) Attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:
 - (a) paredzētā(-o) komunikācijas saņēmēja(-u) pieslēguma marķējums vai lietotāja ID;
 - (b) tā(-o) abonenta(-u) vai reģistrētā(-o) lietotāja(-u) uzvārds(-i) un adrese(-s), kurš(-i) ir paredzētais(-ie) komunikācijas saņēmējs(-i).

- c) Dati, kuri ir nepieciešami, lai noteiktu komunikācijas datumu, laiku un ilgumu.
- (1) Attiecībā uz fiksētā tīkla telefoniju un mobilo telefoniju:
 - (a) komunikācijas sākuma un beigu datums un laiks.
 - (2) Attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:
 - (a) interneta sesiju pieteikuma un atteikuma datums un laiks, pamatojoties uz konkrētu laika zonu.
- d) Dati, kuri ir nepieciešami, lai noteiktu komunikācijas veidu.
- (1) Attiecībā uz fiksētā tīkla telefoniju:
 - (a) izmantotais tālruņa pakalpojums, piemēram, balss pakalpojums, konferences zvans, faksa un ziņojumapmaiņas pakalpojumi.
 - (2) Attiecībā uz mobilo telefoniju:
 - (a) izmantotais tālruņa pakalpojums, piemēram, balss pakalpojums, konferences zvans, īsziņu pakalpojums, pastiprinātais mediju pakalpojums vai multivides pakalpojums.
- e) Dati, kuri ir nepieciešami, lai identificētu sakaru ierīci vai ierīci, kas veic tās funkcijas.
- (1) Attiecībā uz mobilo telefoniju:
 - (a) izsauceja un izsauktā starptautiskā mobilā abonenta identitāte (IMSI);
 - (b) izsaucejas un izsauktās starptautiskās mobilās iekārtas identitāte (IMEI);
 - (2) Attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:
 - (a) izsaucejs tālruņa numurs iezvanpieejas piekļuvei;
 - (b) komunikācijas ierosinātāja ciparu abonenta līnija (DSL) vai cits nobeiguma punkta identifikācijas numurs;
 - (c) komunikācijas ierosinātāja mediju piekļuves kontroles (MAC) adrese vai cita identifikācijas iekārta.
- f) Dati, kuri ir nepieciešami, lai noteiktu mobilo sakaru iekārtas atrašanās vietu:
- (1) Atrašanās vietas marķējums (šūnas ID) komunikācijas sākumā un beigās;
 - (2) Datu kartēšana starp šūnu ID un to ģeogrāfisko atrašanās vietu komunikācijas sākumā un beigās.