

## **29 STRAIPSNIO duomenų apsaugos darbo grupė**

**11885/04/EN  
WP 99**

### **Nuomonė 9/2004**

**dėl sprendimo projekto dėl viešojo elektroninio ryšio paslaugų teikimo tikslais tvarkomų ir išsaugomų duomenų arba viešojo ryšio tinkluose prieinamų duomenų saugojimo nusikalstamų veiksmų, įskaitant terorizmą, prevencijos, tyrimo, nustatymo ir patraukimo baudžiamojon atsakomybėn tikslais.**

**[Pasiūlymai pateikti Prancūzijos, Airijos, Švedijos ir Didžiosios Britanijos (Tarybos 8958/04 2004 m. balandžio 28 d. dokumentas)]**

**Priimta 2004 m. lapkričio 9 d.**

Ši Darbo grupė buvo sudaryta pagal Direktyvos 95/46/EC 29 straipsnį. Ji yra Europos savarankiška patariamoji duomenų apsaugos ir privatumo institucija. Jos tikslai nubrėžti Direktyvos 95/46/EC 30 straipsnyje ir Direktyvos 2002/58/EC 15 straipsnyje.

Sekretoriatas yra išlaikomas Europos Komisijos E direktorato (paslaugos, autorių teisės, pramoninė nuosavybė ir duomenų apsauga), Vidaus rinkos pagrindinis direktoratas, B-1049 Briuselis, Belgija, įstaigos Nr. C100-6/136.

Tinklapis: [www.europa.eu.int/comm/privacy](http://www.europa.eu.int/comm/privacy)

## DARBO GRUPĖ DĖL ASMENŲ APSAUGOS TVARKANT ASMENS DUOMENIS

Sudaryta pagal Europos Parlamento ir Tarybos 1995 m. spalio 24 d.<sup>1</sup> direktyvą 95/46/EB,

atsižvelgdama į šios Direktyvos 29 straipsnį ir 30 straipsnio 1(a) ir 3 dalis bei Europos Parlamento ir Tarybos 2002 m. liepos 12 d. Direktyvos 2002/58/EC 15 straipsnio 3 dalį,

atsižvelgdama į jos Procedūrų taisykles ir ypač į 12 ir 14 straipsnius,

### **priėmė šią Nuomonę:**

Pastaraisiais metais Darbo grupė ne kartą komentavo klausimus, susijusius su komunikacijos srauto duomenų<sup>2</sup> išsaugojimu, o Europos duomenų apsaugos įgaliotinių konferencija išleido kelis bendrus pareiškimus ta pačia tema<sup>3</sup>. Siūlymai Sprendimo projektui dėl tokių srauto duomenų išsaugojimo, pateikti keturių valstybių narių Europos Sąjungos Taryboje, dar kartą reikalauja Darbo grupės nuomonės. Atsižvelgiant į tai, kad Tarybos darbo grupėje diskusija tik prasideda, ši nuomonė yra pirminio pobūdžio. Darbo grupė ketina dar kartą apsvarstyti šią temą, peržiūrėjusi projektą vėlesniame etape.

Darbo grupė patikrino, ar šis projektas atitinka Europos žmogaus teisių konvencijos 8 straipsnio normas.

Šiame kontekste itin svarbu atkreipti dėmesį į tai, jog piliečiai vis dažniau kasdieniškai veiklai ir operacijoms naudojami elektroninio ryšio tinklu ir paslaugomis. Šiais ryšiais generuojami duomenys - vadinamieji „srauto duomenys“ - galimas dalykas, apimantys detales apie laiką, vietą ir numerius, naudojami fiksuoto ar judriojo ryšio balso (telefonijos) paslaugoms, faksui, elektroniniam paštui, SMS - trumpiems tekstiniams pranešimams ir kitokiam interneto naudojimui, todėl atspindi vis daugiau detalių, susijusių su piliečių kasdienio gyvenimo aspektais.

*Rekomendacijoje 2/99 dėl pagarbos privatumui slapto ryšių perėmimo kontekste, priimtoje 1999 m. gegužės 3 d., Darbo grupė apibrėžė slaptą pasiklausymą ir duomenų perėmimą kaip trečiųjų šalių veiksmą, kuriuo gaunama žinių apie turinį ir (arba) duomenis, susijusius su privačiu dviejų ar daugiau asmenų bendravimu ryšio priemonėmis, ypač apie srauto duomenis, susijusius su elektroninių ryšių paslaugų naudojimu. Šioje situacijoje Darbo grupė nurodė, jog kiekvienas slaptas*

---

<sup>1</sup> Official Journal no.L 281, 23.11.1995, p. 31, galima rasti:

<http://europa.eu.int/comm/internal-market/privacy/law-fr.htm>

<sup>2</sup> Žr: Rekomendacija 3/97 dėl anonimiškumo internete; Rekomendacija 2/99 dėl pagarbos privatumui slapto telefoninių pokalbių pasiklausymo kontekste; Rekomendacija 3/99 dėl interneto paslaugų teikėjų srauto duomenų išsaugojimo įstatymo priežiūros tikslais; Nuomonė 7/2000 dėl Europos Komisijos pasiūlymo Europos Parlamento ir Tarybos direktyvai ryšium su asmens duomenų tvarkymu ir privatumo apsauga elektroninių ryšių sektoriuje 2000 COM 385, liepos 12 d.; Nuomonė 4/2001 dėl Europos Tarybos Konvencijos projekto dėl elektroninių nusikaltimų; Nuomonė 10/2001 dėl suderinto požiūrio poreikio kovojant su terorizmu; Nuomonė 5/2002 dėl Europos duomenų apsaugos įgaliotinių pareiškimo tarptautinėje konferencijoje Kardife (2002 m.rugsėjo 9-11) dėl privalomo sistemiško telekomunikacijų srauto duomenų išsaugojimo; Nuomonė 1/2003 dėl srauto duomenų išsaugojimo atsiskaitymų už paslaugas tikslais. Šių nuomonių ir pasisakymų santrauką rasite šio dokumento priede. Visi išvardinti dokumentai taip pat randami:

[http://europa.eu.int/comm/internal\\_market/privacy](http://europa.eu.int/comm/internal_market/privacy).

<sup>3</sup> Žr. teiginius, priimtus Stokholme (2000 m. balandis) ir Kardife (2002 m.)

elektroninių ryšių pasiklausymas ir perėmimas (įskaitant monitoringą ir duomenų išrinkimą iš srauto duomenų) sudaro asmens teisės į privatumą bei korespondencijos konfidencialumo pažeidimą. Iš to išplaukia išvada, jog slapti pasiklausymai ir informacijos perėmimas yra nepriimtini, nebent tokie veiksmai atitinka pagrindinius tris kriterijus, išdėstytus Europos konvencijos 8 straipsnio 2 dalyje, bei Europos žmogaus teisių teismo šios nuostatos aiškinimą: teisinis pagrindas, vertinimo poreikis demokratinėje visuomenėje ir suderinamumas su vienu iš Konvencijoje išvardintų teisėtų tikslų.

Darbo grupė supranta ir tai, kad tie patys pagrindiniai kriterijai turi būti taikomi srauto duomenų išsaugojimui, išskyrus kai tai reikalinga ryšių paslaugoms teikti bei kitiems teisėtiems verslo tikslams vykdyti ar bet kokiai paskesnei prieigai prie tokių duomenų teisėsaugos tikslais<sup>4</sup>.

Darbo grupė turi rimtų abejonų, ar atsižvelgiama į tuos pagrindinius kriterijus sprendimo projekte. Aptariant pirmąjį kriterijų (teisinį pagrindą), atsižvelgiant į preliminarų šios diskusijos pobūdį Taryboje, darbo grupė laikosi nuomonės, kad šis momentas nėra tinkamas jam nagrinėti. Atsižvelgiant į trečiąjį kriterijų (atitikimą teisėtam ir įvardintam tikslui), darbo grupei abejonų kelia pats projekto tikslas. Ar šis tikslas iš tikrųjų bus vien tik užkirsti kelią, tirti, nustatyti ir patraukti baudžiamojon atsakomybėn už kriminalinius pažeidimus, kaip teigiama projekte (Pagrindas 7), tuo pačiu nepaisant kitų 8 straipsnyje išvardintų tikslų? Pirmiausia būtina aiškiai nusistatyti tikslą.

Nagrinėjant antrąjį kriterijų (demokratinės visuomenės poreikį), remiantis EŽTT (Europos žmogaus teisių teismo) aiškinimu, kišimasį privalo diktuoti „neatidėliotinas socialinis poreikis“ (pvz., 1977 m. lapkričio 18 d. teismo sprendimas byloje Klass prieš Vokietijos Federacinę Respubliką, Europos žmogaus teisių teismas, serija A Nr. 28). Žmogaus teisių teismas pripažino susitariančiųjų šalių teisę slapta sekti asmeninę korespondenciją ir telefoninius pokalbius išskirtiniais atvejais ir ypatingomis aplinkybėmis. Be to, teigiama: „...tai nereiškia, jog susitariančiosios šalys naudojasi neribota veiksmų laisve dėl asmenų, esančių jų jurisdikcijoje, slauto sekimo. Teismas, suprasdamas pavojų, kad įstatymas galėtų pakenkti ar net naikinti demokratiją ją gindamas, patvirtina, jog susitariančiosios šalys negali vardan kovos su špionažu ir terorizmu imtis bet kokių priemonių, kurias tik jos laiko tinkamomis“ (Klass, p. 3).

Dėl rutiniško išsamaus visų srauto duomenų, naudotojo ir dalyvio duomenų kaupimo, kaip siūloma sprendimo projekte, išskirtinėmis sąlygomis leidžiamas stebėjimas taptų taisykle. O tai neabejotinai būtų neproporcinga. Į projekte numatytus rėmus patektų ne tik tie asmenys, kurie būtų kontroliuojami pagal konkrečius įstatymus, bet ir visi fiziniai asmenys, besinaudojantys elektroniniu ryšiu. Be to, tai apimtų visas siuntimo ir gavimo komunikacijas. Ne visa, kas galėtų atrodyti naudinga teisėsaugai, yra pageidautina arba galėtų būti laikoma būtina priemone demokratinėje visuomenėje, ypač jeigu tai lemia sistemišką visų elektroninių ryšių registravimą. Sprendimo projekte nepateikta jokių įtikinamų argumentų, kad srauto duomenų išsaugojimas tokiu

---

<sup>4</sup> Tai yra pagrįsta Europos žmogaus teisių teismo precedentų teise. Pavyzdžiui, pagal Amman nutartį (p.30), institucijų vien tik informacijos saugojimas buvo laikomas kišimusi į privatų gyvenimą, nepaisant to fakto, ar tie duomenys yra naudojami prieš asmenį, ar ne. Rotaru nutartyje slaptųjų tarnybų istorinės informacijos saugojimas taip pat buvo laikomas kišimusi į privatų gyvenimą. Byloje PG prieš Jungtinę Karalystę teismas nutartyje paskelbė (42 p.), jog matavimas „per se“ nesudaro 8 straipsnio pažeidimo, pavyzdžiui, jei jis atliekamas telefonų kompanijos atsiskaitymų už paslaugas tikslais. Teikėjo informacijos apie numerius, kuriais skambinta perdavimas policijai, vis dėlto yra kišimasis į korespondentų privatų gyvenimą ar korespondenciją. Malone byloje (84 p.) teismas taip pat nusprendė, jog operatoriaus duomenų perdavimas policijai buvo kišimasis į „korespondenciją“ pagal 8 straipsnį. Remiantis šiomis bylomis galima būtų daryti išvadą, jog privalomas srauto duomenų saugojimas elektroninių ryšių teikėjų pats savaime nėra 8 straipsnio pažeidimas, o tokių duomenų perdavimas valdžios organams ar tolesniam tvarkymui jį pažeidžia. Tokia išvada būtų klaidinga. Byloje MM prieš Nyderlandus teismas pripažino, kad valdžios organai negali išvengti atsakomybės pasinaudodami privačiais asmenimis, kurie atlieka pagrindinį vaidmenį vykdamas stebėjimo planą. Vadinasi, tai reikštų, pavyzdžiui, kad telekomunikacijų operatorių vykdomas duomenų išsaugojimas ir duomenų išrinkimas jų pačių sistemose viešosios tvarkos tikslais taip pat bus laikomas kišimusi į privatų gyvenimą.

plačiu mastu tėra vienintelis realus pasirinkimas kovojant su nusikalstamumu ar ginant nacionalinį saugumą. Reikalavimas operatoriams išsaugoti srauto duomenis, kurių jiems nebereikia jų pačių tikslams, sudarytų precedento neturintį menkinimą, nukrypimą nuo baigiamumo ir (arba) tikslo principo.

Europos telekomunikacijų kompanijų atliktas tyrimas atskleidė, jog teisėsaugos institucijos daugiausiai reikalavė duomenų, ne senesnių kaip šešių mėnesių. Tai rodo, jog ilgesnis saugojimo periodas yra aiškiai neproporcingas.

Pažymėtina tai, kad teisėsaugos atstovams nepavyko pateikti kokių nors tokių kraštutinių priemonių reikalingumo įrodymų. Iš esmės, apie tokias priemones išvis nebuvo kalbama neseniai vykusiuose seminaruose, organizuotuose siekiant apsvarstyti šio pasiūlymo sprendimo projektui pagrindą ir pasekmes.

Konvencija dėl elektroninių nusikaltimų numato tik „greito užšaldymo - greito atšildymo“ duomenų kaupimo modelį asmeniniam saugumui, kuris, skirtingai nuo keturių siūlančių vyriausybės požiūrio, yra visiškai tinkamas kriminalinių pažeidimų prevencijai ar patraukimui baudžiamojon atsakomybėn už kriminalinius pažeidimus. Dabartinėms teisinėms diskusijoms svarbu tai, kad dabartinis pasiūlymas yra rimtai svarstomas, kol Konvencija dėl elektroninių nusikaltimų dar neišsigaliojo daugumoje pasirašiusių šalių ir jos realiosios pasekmės negali būti įvertintos. 29 straipsnio darbo grupė jau yra pareiškusi (Nuomonėje 5/2002), kad srauto duomenų išsaugojimas teisėsaugos tikslais turi griežtai atitikti sąlygas, numatytas Direktyvos 2002/58/EC 15 straipsnio 1 dalyje, t.y. visais atvejais tik ribotam laikotarpiui ir kai tai yra būtina, tinkama ir suderinama demokratinėje visuomenėje. Be to, Europos duomenų apsaugos įgaliotiniai tarptautinėje konferencijoje Kardife (2002 m. rugsėjo 9-11 d.) padarė pareiškimą dėl sistemiško srauto duomenų išsaugojimo. Jame konstatuota, kad sisteminis visų tipų srauto duomenų išsaugojimas vieneriems metams ar ilgesniam laikui būtų aiškiai neproporcingas ir todėl nepriimtinas.

Sprendimo projekte ne tik neapimamos visos šios sąlygos, bet dar ir specialiai siekiama jas panaikinti, nereikalaujant apibrėžto pagrindo įtarimui ir patikimos bazės atskirais atvejais bei numatant platų duomenų kaupimą kaip atsargumo priemonę ateities teismo procesams prieš bet kuriuos elektroninių ryšių sistemų naudotojus.

Darbo grupė yra tos nuomonės, kad privalomas visų tipų duomenų išsaugojimas kiekvieną kartą naudojantis telekomunikacijų paslaugomis viešosios tvarkos tikslais, remiantis Sprendimo projekte išdėstytomis sąlygomis, yra nepriimtinos pagal 8 straipsnį.

Atlikta Briuselyje, 2004 m. lapkričio 9 d.

*Už darbo grupę*

Pirmininkas  
Peter Schaar

## **PRIEDAS**

### **29 straipsnio darbo grupės pasisakymų komunikacijos srauto duomenų išsaugojimo klausimu santrauka**

#### **REKOMENDACIJA 3/97 DĖL ANONIMIŠKUMO INTERNETE**

Rekomendacijoje 3/97 dėl anonimiškumo internete 29 straipsnio darbo grupė pareiškė, kad nors duomenys apie transakcijas tam tikrose jurisdikcijose yra apsaugoti vadovaujantis korespondencijos konfidencialumo taisyklėmis, vis dėlto masinis tokių duomenų apimtis augimas kelia pagrįstą susirūpinimą. Kadangi tiesioginio prisijungimo (ryšio) paslaugos tampa vis modernesnės ir populiarnesnės, problema dėl transakcijų duomenų vis aštrės. Kadangi vis daugiau mūsų kasdienės veiklos aspektų vykdoma internetu, vis daugiau mūsų veiksmų bus fiksuojama.

Atpažįstami transakcijų duomenys taps įrankiu, kuriuo naudojantis asmens elgseną bus įmanoma stebėti ir kontroliuoti iki šiol neregėtu mastu. Remiantis 29 straipsnio darbo grupe, vyriausybių ir viešųjų institucijų galimybės riboti asmens teises ir stebėti potencialiai neteisėtą elgseną internete neturėtų būti didesnės, negu (išoriniame pasaulyje) neryšinėje aplinkoje.

#### **REKOMENDACIJA 2/99 DĖL PAGARBOS PRIVATUMUI SLAPTO RYŠIŲ PERĖMIMO KONTEKSTE, PRIIMTA 1999 M. GEGUŽĖS 3 D.**

Kaip žmogaus teisių principai yra susiję su elektroninių ryšių sekimo (įskaitant monitoringą ir duomenų išrinkimą iš srauto duomenų), priemonėmis buvo išdėstyta 29 straipsnio darbo grupės Rekomendacijoje 2/99 dėl pagarbos privatumui slapto ryšių perėmimo kontekste, priimtoje 1999 m. gegužės 3 d. 29 straipsnio darbo grupė apibrėžė slaptą pasiklausymą ir perėmimą kaip trečiųjų šalių veiksmą, kuriuo gaunama žinių apie turinį ir (arba) duomenis, susijusius su privačiu dviejų ar daugiau asmenų bendravimu ryšio priemonėmis, ir ypač srauto duomenis, susijusius su elektroninių ryšių paslaugų naudojimu. 29 straipsnio darbo grupė nurodė, jog kiekvienas elektroninių ryšių slapto perėmimas pažeidžia asmens teisę į privatumą ir į korespondencijos konfidencialumą.

Iš to išplaukia išvada, jog slapto pasiklausymas ir perėmimas yra nepriimtinas, nebent atitinka tris pagrindinius kriterijus, pagal Europos konvencijos 8 straipsnio 2 dalį ir Europos žmogaus teisių teismo šios nuostatos išaiškinimą: teisinis pagrindas, priemonės būtinybė demokratinėje visuomenėje ir suderinamumas su vienu iš teisėtų tikslų, išvardintų Konvencijoje.

Šiame teisiniame kontekste, tiriamasis ar bendro pobūdžio plataus masto stebėjimas turi būti oficialiai uždraustas. 29 straipsnio darbo grupė ypač rėmėsi Leander ir Klass bylomis: reikalingos veiksmingos garantijos nuo piktnaudžiavimo, atsižvelgiant į riziką, kad slapto sekimo sistema, sukurta nacionaliniam saugumui ginti, galėtų pakenkti ar net sunaikinti demokratiją, užuot ją gynusi. Klass byloje, Vokietijos įstatymai neprieštaravo 8 straipsniui, nes „inter alia“ sekti buvo galima tik konkretų įtariamąjį arba jo tikėtinius „kontaktinius asmenis“. Šioje rekomendacijoje (9 skirsnis) darbo grupė sudarė reikalavimų, kuriuos turėtų tenkinti nacionalinė teisė ryšium su slapto telefoninių pokalbių pasiklausymu, sąrašą.

## **REKOMENDACIJA 3/99 DĖL INTERNETO PASLAUGŲ TEIKĖJŲ TEISĖSAUGOS TIKSLAIS IŠSAUGOMŲ SRAUTO DUOMENŲ, PRIIMTA 1999 M. RUGSĖJO 7 D.**

Įsipareigojimas ištrinti srauto duomenis ar padaryti juos anoniminiais yra padiktuotas ypatingo srauto duomenų pobūdžio, atskleidžiančio asmeninius ryšio profilius, įskaitant fiksuoto arba judriojo ryšio telefonus, naudotojo informacijos šaltinius ir geografinę buvimo vietą, ir galimų privatumo pažeidimų dėl tokio šių duomenų rinkimo, atskleidimo ar tolesnio jų naudojimo. Dėl laikotarpio, per kurį srauto duomenys gali būti saugomi, 29 straipsnio darbo grupė pastebėjo reikšmingą laikotarpio, per kurį srauto duomenys gali būti saugomi, nevienodumą valstybėse narėse. 29 straipsnio darbo grupė rekomendavo, kad srauto duomenys neturėtų būti saugomi vien tik teisėsaugos tikslui ir kad nacionaliniai įstatymai neturėtų versti saugoti srauto duomenis ilgiau negu būtina atsiskaitymo už paslaugas tikslams. Tokio laikotarpio trukmė galėtų būti toliau derinama ES .

## **NUOMONĖ 7/2000 DĖL EUROPOS KOMISIJOS SIŪLYMO 2000 M. LIEPOS 12 D. EUROPOS PARLAMENTO IR EUROPOS TARYBOS DIREKTYVAI DĖL ASMENS DUOMENŲ TVARKYMO IR PRIVATUMO APSAUGOS ELEKTRONINIŲ RYŠIŲ SEKTORIUJE, COM (2000) 385, PRIIMTA 2000 M. LAPKRIČIO 2 D.**

Tokie srauto duomenys, kaip, pavyzdžiui, URL (anglų k. - Universal Records Location), gali atskleisti asmens interesus, pvz., duomenis, apie religinius įsitikinimus, politines pažiūras, sveikatos būklę ar lytinį gyvenimą. Šiems duomenims turėtų papildomai būti taikomas komunikacijos nustatytas konfidencialumas.

29 straipsnio darbo grupės teigimu, reikėtų aptarti dar vieną papildomą aspektą - dalis šių duomenų gali būti priskiriami prie ypatingų duomenų pagal Duomenų apsaugos direktyvą 95/46/EB 8 straipsnį, kuriuos tvarkyti iš esmės yra draudžiama.

Atsižvelgiant į platų srauto duomenų apibrėžimą, 29 straipsnio darbo grupė nemano, jog visus duomenis reikia traktuoti vienodai . Kai kuriems srauto duomenų tipams reikalinga stipresnė apsauga negu kitiems.

## **NUOMONĖ 4/2001 DĖL EUROPOS TARYBOS KONVENCIJOS PROJEKTO DĖL ELEKTRONINIŲ NUSIKALTIMŲ, PRIIMTA 2001 M. KOVO 22 D.**

Jei procesinė teisė turi būti suderinta, turi būti apsvaistytas numatytoms priemonėms taikytinų saugumo priemonių ir sąlygų suderinimas. Ir vėl 29 straipsnio darbo grupė pabrėžė, jog bendra sekimo prievolė, apimanti rutinišką srauto duomenų išsaugojimą, kaip pradžioje buvo siūlyta Konvencijoje dėl elektroninių nusikaltimų (versija Nr. 25), būtų neprideramas išibrovimas, pažeidžiantis pagrindines teises, garantuojamas asmenims pagal Europos žmogaus teisių konvencijos 8 straipsnį.

Be to, verslo atstovams gali prireikti teisinio aiškumo tuo atveju, kai yra neaišku, kada ir kam turi būti leidžiama susipažinti su konfidencialia informacija bei ryšiais.

## **NUOMONĖ 10/2001 DĖL SUDERINTO POŽIŪRIO POREIKIO KOVOJANT SU TERORIZMU, PRIIMTA 2001 M. GRUODŽIO 14 D.**

*Nuomonėje 10/2001 dėl suderinto požiūrio poreikio kovojant su terorizmu, priimtoje 2001 m. gruodžio 14 d., 29 straipsnio darbo grupė pareiškė, kad demokratinių visuomenių tikslas išsitraukti į kovą su terorizmu yra ir būtinas, ir vertingas. Vis dėlto šioje kovoje reikia paisyti tam tikrų sąlygų, sudarančių demokratinių visuomenių pagrindą. Visiškai suprantant terorizmo problemos rimtumą, kadangi šis reiškinys egzistuoja Europoje jau kurį laiką, būtinas ilgalaikis priemonių, kurios yra*

tiesiog „naudingos“ ar „pageidaujamos“, apsvaistymas, pvz., išankstinis ir apibendrintas elektroninių ryšių duomenų išsaugojimas. Priemonės, kurių privaloma imtis, neturi apriboti pagrindinių teisių ir laisvių. Svarbiausias dalykas kovoje su terorizmu yra užtikrinti pagrindinių vertybių išsaugojimą, o tai sudaro mūsų demokratinių visuomenių pagrindą, ir būtent tų vertybių, kurias siekia sunaikinti smurto naudojimo šalininkai.

**NUOMONĖ 5/2002 DĖL EUROPOS DUOMENŲ APSAUGOS ĮGALYBŲ PAREIŠKIMO TARPTAUTINĖJE KONFERENCIJOJE KARDIFE (2002 M. RUGSĖJO 9-11 D.) DĖL PRIVALOMO SISTEMINIO TELEKOMUNIKACIJŲ SRAUTO DUOMENŲ IŠSAUGOJIMO, PRIIMTA 2002 M. SPALIO 11 D.**

29 straipsnio darbo grupė rimtai abejoja pagrįstumu ir teisėtumu privalomo sisteminio srauto duomenų išsaugojimo, kad teisėsaugos ir saugumo organai galėtų su šiais duomenimis susipažinti.. Gana ilgų ir detalių šio klausimo svarstymų rezultatas atsispindi Direktyvoje 2002/58/EB, kuri nustato, jog srauto duomenų išsaugojimas teisėsaugos tikslais turi atitikti griežtas sąlygas, numatytas šios Direktyvos 15 straipsnyje: t.y., bet kuriuo atveju tik ribotam laikotarpiui ir kai tai yra būtina, tinkama ir suderinama demokratinėje visuomenėje. 29 straipsnio darbo grupė pabrėžė, kad sisteminis visų tipų srauto duomenų saugojimas vienerius ir daugiau metų būtų visiškai neproporcingas ir todėl jokia būdu nepriimtinas.

Be to, 29 straipsnio darbo grupė tikisi, jog su ja bus konsultuojamasi dėl priemonių, kurios gali atsirasti trečiojo ramsčio diskusijose prieš jas patvirtinant.

**NUOMONĖ 1/2003 DĖL SRAUTO DUOMENŲ SAUGOJIMO ATSISKAITYMO UŽ PASLAUGAS TIKSLAIS, PRIIMTA 2003 M. SAUSIO 29 D.**

*Nuomonėje 1/2003 dėl srauto duomenų saugojimo atsiskaitymo už paslaugas tikslais, priimtoje 2003 m. sausio 29 d., 29 straipsnio darbo grupė pateikė gaires, kaip suderinti laikotarpį, per kurį srauto duomenys gali būti teisėtai tvarkomi atsiskaitymo už paslaugas tikslais. Duomenys atsiskaitymo už paslaugas tikslais paprastai turi būti saugomi ilgiausiai nuo 3 iki 6 mėnesių. Gali būti tvarkomi tik tie srauto duomenys, kurie atitinka atsiskaitymo už paslaugas ir ryšio teikimo temą, tikslą ir apimtį. Kiti srauto duomenys privalo būti ištrinti arba anonimiški.*

Veikla, prieštaraujanti šiems principams, kaip ir veikla, kuri nėra aiškiai leistina pagal nuostatas, remiantis Direktyvos 2002/58/EC 15 straipsnyje išdėstytomis sąlygomis yra „prima facie“ (akivaizdžiai) nesuderinama su EB duomenų apsaugos įstatymo reikalavimais.

Vertė A.Gobienė  
2005- 03 -15.