ISSN 1392-6195

JURISPRUDENCIJA
Mokslo darbai
2006 9(87); 69–75

PRIVATAUS GYVENIMO ELEKTRONINIUOSE RYŠIUOSE RIBOJIMAS NUSIKALTIMŲ TYRIMO TIKSLAIS

Darius Štitilis *

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedra
Ateities g. 20, LT-083030 Vilnius
Telefonas 271 45 71
Elektroninis paštas stitilis@mruni.lt

Pateikta 2005 m. lapkričio 11 d., parengta spausdinti 2006 m. liepos 10 d.

Santrauka. Kaip pažymima 2005 m. žmogaus teisių įgyvendinimo Lietuvoje apžvalgoje [20], 2005 metais viena iš pagrindinių teisės į privataus gyvenimo neliečiamumą problemų buvo susijusi su teisėsaugos institucijų vykdoma elektroninių ryšių kontrole. 2005 metais atliktas elektroniniais ryšiais perduodamos informacijos kontrolės ir teisės į privataus gyvenimo gerbimą tyrimas [21] parodė, kad Lietuvoje turinio ir srauto duomenų kontrolės klausimas yra labai aktualus. Šios srities svarbą įrodo ir tai, jog 2006 metais Europos Sąjungoje buvo priimta duomenų saugojimo direktyva, kuri reglamentuoja srauto duomenų, kaupiamų teikiant elektroninių ryšių paslaugas ar tinklus, saugojimo terminus.

Straipsnyje nagrinėjama teisėsaugos institucijų nusikaltimų tyrimo ir prevencijos tikslais vykdoma elektroninių ryšių kontrolė. Šio straipsnio objektas – privataus gyvenimo ribojimo elektroniniuose ryšiuose teisinis reguliavimas nusikaltimų tyrimo tikslais. Straipsnio tikslas – išanalizuoti privataus gyvenimo ribojimo elektroniniuose ryšiuose teisinį reguliavimą Lietuvoje nusikaltimų tyrimo tikslais. Straipsnyje naudojamas analizės, lyginamasis bei kiti metodai. Nagrinėjant privataus gyvenimo ribojimo elektroniniuose ryšiuose teisinius aspektus nusikaltimų tyrimo tikslais, naudojamasi užsienio valstybių doktrina bei periodine literatūra. Straipsnyje atskleidžiama tiek buvusi elektroninių ryšių kontrolė, tiek elektroninių ryšių kontrolė, vykdoma dabar. Taip pat analizuojamas tokios kontrolės priežiūros mechanizmas.

Straipsnyje atlikta analizė leidžia teigti, kad teisėsaugos institucijų vykdomos elektroninių ryšių kontrolės reglamentavimas nėra pakankamas ir, atsižvelgiant į užsienio valstybių praktiką bei remiantis žmogaus teises reglamentuojančių teisės aktų nuostatomis, yra tobulintinas.

Pagrindinės sąvokos: privatus gyvenimas, elektroniniai ryšiai, teisėsaugos institucijų vykdoma elektroninių ryšių kontrolė.

ĮVADAS

Elektroniniai ryšiai, komunikacijų ir ryšio priemonių konvergencija[1] suteikia ne tik neabejotinų pranašumų, bet ir kelia vis didelę grėsmę žmogaus privačiam gyvenimui. Neabejotina, kad elektroninės komunikacijos labiausiai gali daryti poveikį asmenų santykiams su kitais asmenimis elektroninių ryšių tinklų pagalba. Asmens susirašinėjimas ir kita veikla gali būti itin pažeidžiama.

Paminėtina, jog teisė į privatų gyvenimą nėra absoliuti. Tiek Lietuvos Respublikos Konstitucijos 22 straipsnis, tiek Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnio 2 dalis numato, kad ši teisė gali būti ribojama, esant tam tikroms aplinkybėms. Pažymėtina, jog teisės į privataus gyvenimo neliečiamybę ribojimas turi būti paremtas tam tikrais principais. Šioje vietoje svarbi Europos Žmogaus Teisių Teismo praktika. Bylose *Amann prieš Šveicariją, Armstrong prieš Jungtinę Karalystę, Khan prieš Jungti-*

* Socialinių mokslų daktaras, Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Informatikos ir statistikos katedros docentas.

[1] Konvergencija – žiniasklaidos, telekomunikacijų ir informacijos technologijų sektorių susiliejimas, įskaitant fiksuotų, judriųjų, antžeminių ir palydovinių ryšių, ryšių ir vietos nustatymo, lokacijos sistemų susiliejimą. Konvergencija lemia technologijų pažangą, suteikia galimybę tas pačias paslaugas teikti, perduoti bet kuriuo tinklu: bevieliu, laidiniu, televizijos, įskaitant kabelinę televiziją, palydoviniais ir antžeminiais tinklais / Elektroninių ryšių įstatymo projekto aiškinamasis raštas // http://www3.lrs.lt/cgi-bin/preps2?Condition1=226267& Condition2=.

nę Karalystę ir kt.[2] Europos Žmogaus Teisių Teismas suformavo šias pagrindines žmogaus teisių ribojimo sąlygas: 1) teisėtumo sąlygą, nurodančią, kad ribojimai gali būti nustatomi tik viešai paskelbtu ir aiškiai suformuluotu įstatymu; 2) būtinumo sąlygą, nurodančią, kad ribojimai gali būti nustatomi tik tuomet, kai tai reikalinga demokratinėje visuomenėje. Žmogaus teisių ribojimo klausimu pasisakė ir Lietuvos Respublikos Konstitucinis Teismas. 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime teigiama, jog pagal Konstituciją riboti konstitucines žmogaus teises ir laisves galima, jeigu yra laikomasi šių sąlygų: tai daroma įstatymu; ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; ribojimais nėra paneigiama teisių ir laisvių prigimtis bei jų esmė; yra laikomasi konstitucinio proporcingumo principo.

Teisės į privatų gyvenimą ribojimas elektroniniuose ryšiuose[3] taip pat turėtų būti vykdomas vadovaujantis aukščiau išvardintais principais ir sąlygomis. Elektroninių ryšių kontrolę (plačiąja prasme), vykdomą operatyviniais ar kitais nusikaltimų tyrimo tikslais, galima skirstyti į dvi grupes, tai: 1) buvusių elektroninių ryšių įvykių kontrolė – informacijos apie buvusius elektroninių ryšių įvykius (srauto duomenis)[4] gavimas iš elektroninių ryšių paslaugų teikėjų; 2) elektroninių ryšių tinklais perduodamos informacijos kontrolė (kompetentingų teisėsaugos institucijų vykdoma elektroninių ryšių turinio ar kitos elektroninių ryšių tinklais perduodamos informacijos kontrolė).

1. BUVUSIŲ ELEKTRONINIŲ RYŠIŲ ĮVYKIŲ KONTROLĖ

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnio 1 dalį „ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo kompetentingoms institucijoms – operatyvinės veiklos subjektų pagrindinėms institucijoms, Vyriausybės nurodytoms ikiteisminio tyrimo įstaigoms, prokurorui, teismui ar teisėjui – pateikti turimą informaciją“. Šiai informacijai priklauso ir informacija apie elektroninių ryšių įvykius, t. y. srauto duomenys.

Jei informacija renkama operatyvinės veiklos tikslais, pagal Lietuvos Respublikos operatyvinės veiklos įstatymą yra būtina teismo nutartis. Šiame įstatyme nustatyta, jog „operatyviniam tyrimui reikalingą konkrečią informaciją apie buvusius telekomunikacijų įvykius iš telekomunikacijų operatorių ir telekomunikacijų paslaugų teikėjų operatyvinės veiklos subjektai turi teisę gauti motyvuota apylinkės teismo teisėjo nutartimi, priimta pagal operatyvinės veiklos subjektų vadovų ar jų įgaliotų vadovų pavaduotojų motyvuotus teikimus“ [10, 10 str.]. Pagal įstatymo 10 straipsnio 13 dalį „telekomunikacijų operatoriams ar telekomunikacijų paslaugų teikėjams turi būti pateikiamas pranešimas, kuriame nurodomi teikimo numeris, nutarties priėmimo data ir nutartį priėmęs teismas“. Pagal įstatymą už tokio pranešimo turinio atitikimą teismo nutarčiai įstatymų nustatyta tvarka atsako pranešimą teikiantis pareigūnas.

Svarbu paminėti užsienio valstybių praktiką, nustatant reikalavimus buvusių elektroninių ryšių kontrolei. Atitinkamų teisės aktų analizė parodė, kad JAV (Elektroninių ryšių privatumo įstatyme) nustatyta bendra taisyklė, jog buvusių elektroninių ryšių kontrolė galima tik nustatyta tvarka pateikus teismo sankciją [6; 2 (a) (ii) (A)]. Buvę elektroninių ryšių įvykiai gali būti kontroliuojami ir nustatyta tvarka pateikus specialių įstatyme numatytų subjektų išduotą pažymėjimą (angl. *Certification*), kuriame nustatyti terminai ir kitos kontrolės sąlygos [6; 2 (a) (ii) (B)]. Panašias taisykles nustato ir Federalinis perėmimo įstatymas, kuriame nurodyta, kad visoms elektroninių ryšių perėmimo rūšims taikomas teismo leidimo principas. Ta pati procedūra kaip ir buvusių elektroninių ryšių kontrolei JAV taikoma ir elektroninių ryšių kontrolei esamuoju laiku, t. y. pokalbių pasiklausymui ir pan.

Lenkijos baudžiamajame kodekse taip pat nustatyta, jog bet kokia elektroninių ryšių kontrolė prokuroro teikimu turi būti sankcionuota teismo [12]. Lenkijos teisingumo ministerija taip pat yra priėmusi išsamias taisykles, kurios reglamentuoja elektroninių ryšių perėmimo procedūrą ir naudojamas technines priemones.

Estijoje elektroninių ryšių kontrolę (įskaitant buvusių elektroninių ryšių kontrolę ir elektroninių ryšių kontrolę esamuoju laiku) reglamentuoja Priežiūros įstatymas [17]. Elektroninių ryšių priežiūrą motyvuotu sprendimu gali sankcionuoti elektroninių ryšių priežiūros institucijos vadovas. Kai elektroninių ryšių kontrolė būtina tiriant sunkius nusikaltimus, reikia gauti Talino vyriausiojo administracinio teismo teisėjo sankciją [13]. Autoriaus nuomone, tokie elektroninių ryšių kontrolės sankcionavimo procedūros skirtumai yra nepagrįsti. Kiekvienu atveju sankcionuojamas tam tikro asmens teisės į privatų gyvenimą ribojimas ir sankcionavimo tvarka neturėtų priklausyti nuo to, koks nusikaltimas tiriamas.

Latvijoje elektroninių ryšių kontrolė galima tik su teismo sankcija – tai nustatyta Latvijos baudžiamojo proceso kodekse [14].

---

[2] Teismo sprendimai yra skelbiami interneto tinklapyje adresu http://www.echr.coe.int.

[3] Šis ribojimas taip pat gali būti vadinamas elektroninių ryšių kontrole.

[4] 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas“. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 3 str. 52 p. srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje Nr. 2002/58/EB preambulėje paminėta, kad „srauto duomenys gali *inter alia* apimti duomenis, nurodančius pranešimo maršrutą, trukmę, laiką ar apimtį, naudojamą protokolą, siuntėjo ar gavėjo galinio įrenginio vietą, tinklą, kuriame pranešimas atsirado ar pasibaigė, ryšio pradžios bei pabaigos laiką“. Remiantis šiomis sąvokomis, galima teigti, kad tradicinės telefonijos atveju srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, skambinančiojo telefono numerį ir pan., o elektroninio pašto atveju srauto duomenimis gali būti laikomi šie duomenys: siuntėjo IP adresas ir elektroninio pašto adresas, elektroninio pašto žinutės dydis, elektroninio pašto žinutės pavadinimas, elektroninio pašto žinutės priedų dydis, tipas ir pan.

Suomijos baudžiamoji teisė taip pat reglamentuoja elektroninių ryšių kontrolę. Elektroninių ryšių kontrolė pagal Baudžiamojo tyrimo įstatymą galima tik tada, jei padarytas nusikaltimas, už kurį baudžiama laisvės atėmimo bausme. Elektroninių ryšių kontrolė taip pat galima tik turint teismo sankciją [15].

Švedijoje elektroninių ryšių kontrolė taip pat galima tik turint teismo sankciją [16]. 1996 metais įstatymai, reglamentuojantys elektroninių ryšių kontrolę, buvo pakeisti, kad apimtų visas elektroninių ryšių kontrolės rūšis, įskaitant internetą.

Svarbu atkreipti dėmesį į tai, jog nuo 2003 m. gegužės 1 d. įsigaliojus naujajam Lietuvos Respublikos baudžiamojo proceso kodeksui, nebereikalaujama motyvuotos teismo nutarties ikiteisminio tyrimo pareigūnams norint gauti informacijos apie buvusius elektroninių ryšių įvykius, kai šios informacijos reikia ikiteisminio tyrimo stadijoje[5]. Galima paminėti tik vieną išimtį – šio Kodekso 155 straipsnį, kuriame yra bendra nuostata, jog informaciją iš įmonės prokuroras gali gauti tik turėdamas ikiteisminio tyrimo teisėjo leidimą. Todėl galima teigti, kad pagal minėtą kodeksą kiti ikiteisminio tyrimo pareigūnai neprivalo pateikti teismo sprendimą, kai prašo informacijos apie buvusius elektroninių ryšių įvykius. Tokia situacija, reglamentuojant informacijos apie buvusius elektroninių ryšių įvykius kontrolę, prieštarauja konstitucinėms normoms dėl privataus gyvenimo apsaugos ir praktikoje gali sukelti problemų. Ikiteisminio tyrimo pareigūnai didžiaja dalimi vadovaujasi Lietuvos Respublikos baudžiamojo proceso kodeksu ir formaliai minėtą informaciją gali reikalauti pateikti be sankcijos. Kita vertus, egzistuoja Lietuvos Respublikos Konstitucija, taip pat ir minėtas Lietuvos Respublikos Konstitucinio Teismo nutarimas, kuriuose yra motyvuotos teismo nutarties reikalavimas norint gauti minėtą informaciją. Todėl elektroninių ryšių paslaugų teikėjai, pateikdami informaciją apie buvusius elektroninių ryšių įvykius, turėtų reikalauti teismo sprendimo, kitu atveju kiltų grėsmė pažeisti asmenų, apie kuriuos teikiama informacija, privataus gyvenimo neliečiamybę. Taip pat svarbu nedelsiant užtikrinti įstatyminį tokios tvarkos pagrindą ir pakeisti Lietuvos Respublikos baudžiamojo proceso kodeksą.

Trūkumų yra ir elektroninių ryšių srauto duomenų kontrolės poįstatyminiame reglamentavime. Lietuvos Respublikos elektroninių ryšių įstatymo 77 straipsnyje nurodyta, jog „Vyriausybės nurodytos ikiteisminio tyrimo įstaigos Vyriausybės nustatyta tvarka organizuoja ir sudaro galimybę gauti šią informaciją savo padaliniams ir (ar) kitoms ikiteisminio tyrimo įstaigoms“ [9, 77 str. 1 d.]. Srauto duomenų kontrolės, kurios metu ribojama asmens teisė į privatų gyvenimą, atveju turi būti nustatyta griežta procedūra. Tačiau minima Vyriausybės tvarka iki šiol nepatvirtinta, tai sudaro prielaidas piktnaudžiauti iš elektroninių ryšių paslaugų teikėjų gauta privačia informacija, šią informaciją paskirstant pavaldžioms įstaigoms ir pareigūnams. Ši padėtis turi būti ištaisyta patvirtinant minimą tvarką.

Svarbią reikšmę kontroliuojant buvusius elektroninius ryšius turės 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, gautų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti direktyvą 2002/58/EB [5], kurioje informacijos apie srauto duomenis teikimo teisėsaugos institucijoms tikslais numatyta pareiga elektroninių ryšių paslaugų teikėjams srauto duomenis privalomai kaupti ir saugoti nuo 6 mėnesių iki 2 metų nuo jų užfiksavimo. Kadangi, kaip parodė praktika, norėdami užtikrinti ūkinę veiklą elektroninių ryšių paslaugų teikėjai informaciją apie srauto duomenis kaupia ne ilgiau kaip kelis mėnesius, nustačius reikalavimą duomenis kaupti iki dvejų metų, duomenys, sudarantys privataus gyvenimo paslaptį, tam tikrą laikotarpį teisėsaugos tikslais būtų kaupiami be teismo leidimo. Kaip minėta, pagal Lietuvos Respublikos Konstitucijos 22 straipsnį informacija apie privatų gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Taip pat teigia ir Lietuvos Respublikos Konstitucinis Teismas. Todėl toks įpareigojimas be motyvuoto teismo sprendimo saugoti informaciją ilgiau negu reikia ūkinei veiklai užtikrinti įsiterpia į žmogaus privatų gyvenimą ir gali prieštarauti Konstitucijos 22 straipsnio nuostatoms. Dėl galimo direktyvos nuostatų, susijusių su duomenų saugojimo laikotarpiu, prieštaravimo žmogaus teises reglamentuojantiems tarptautinės teisės aktams, diskutuojama ir mokslinėje literatūroje [19; p. 49], tačiau diskusijos tik prasideda. Lietuvos įstatymo leidėjui reikėtų įvertinti minėtos direktyvos įtaką ir santykį su Lietuvos Respublikos Konstitucija bei pasiruošti atlikti veiksmus (įskaitant teisės aktų pakeitimus), kuriais būtų išvengta direktyvos normų prieštaravimo Lietuvos Respublikos konstitucinėms normoms.

2. ELEKTRONINIŲ RYŠIŲ TURINIO IR SRAUTO DUOMENŲ KONTROLĖ ESAMUOJU LAIKU

Kas yra elektroninių ryšių turinys ar kita elektroninių ryšių tinklais perduodama informacija? Teisės aktuose nėra nustatyta, kas laikoma turinio duomenimis. Tačiau teisės literatūroje nurodoma, kad turinio duomenimis (ang. *communication*) laikoma bet kokia informacija, kuria keičiasi šalys viešųjų elektroninių ryšių paslaugų teikimo atveju, t. y. turinio duomenimis laikomas pokalbio telefonu ar susirašinėjimo elektroniniu paštu turinys [11, p. 10]. Prie kitos elektroniniais ryšiais perduodamos informacijos priskirtina informacija apie srauto duomenis ir pan.

Manoma, jog procesiniai reikalavimai srauto ir turinio duomenų rinkimui turėtų skirtis [4, p. 10], kadangi turinio duomenys atskleidžia komunikacijų turinį ir jų neteisėtas atkleidimas daro didesnę žalą, palyginus su srauto duomenų neteisėtu atkleidimu. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis (11, p. 10). Tačiau reikėtų paminėti, jog nors tradici-

[5] 1961 m. Lietuvos Respublikos baudžiamojo proceso kodekse 2002 metais įvestas naujas 198-3 straipsnis reglamentavo informacijos iš telekomunikacijų operatorių ir telekomunikacijų paslaugų teikėjų gavimą. Šio straipsnio 2 dalyje buvo nurodyta, jog informacija apie buvusius telekomunikacijų įvykius gaunama teismo nutartimi.

nėse telekomunikacijose gana lengva atskirti turinio duomenis nuo srauto duomenų, kitos susižinojimo formos, pvz., internetas, kuris priskiriamas prie elektroninių ryšių, tokį atskyrimą padaro gana komplikuotą. Turinio ir srauto duomenų atskyrimas buvo nulemtas tradicinių telekomunikacijų procesų, kur takoskyra tarp srauto duomenų (kas skambino, kur skambino, kiek truko skambutis) ir turinio duomenų (pokalbio turinio) buvo gana aiški, tačiau toks atskyrimas interneto atveju yra gana sudėtingas, jei iš viso įmanomas. Nėra aišku, ar turinio duomenimis laikytinas visas elektroninių paketų turinys, ar srauto duomenys yra tik elektroninių paketų antraštės, taip pat ar srauto duomenimis laikytini *clickstreams* (ang.) ar http užklausos. Tokiu atveju užklausa „http:///searchengine/com/++aids++homosexuality++symptoms“ būtų laikoma srauto duomeniu, kai tuo tarpu minima užklausa susijusi su susižinojimo turiniu [3]. Taip pat galima pateikti ir kitą pavyzdį – DTMF kodų rinkimą elektroninių komunikacijų metu. Pavyzdžiui, surinkus atitinkamą telefoninės bankininkystės numerį po įvykusio sujungimo atsiranda galimybė paslaugas valdyti DTMF kodų pagalba. Kadangi DTMF kodai renkami jau įvykus sujungimui, galima teigti, kad tai yra elektroninių ryšių turinys. Tačiau, kita vertus, DTMF kodais siekiama inicijuoti tam tikras paslaugas/veiksmus, todėl šios komandos gali turėti ir srauto duomenų požymių. Kai kurie telekomunikacijų operatoriai Valstybinės duomenų apsaugos inspekcijos tinklapyje adresu http://www.ada.lt skelbiami deklaravę technines komandas pradėti sujungimus kaip tvarkomus asmens, t. y. srauto duomenis. Šie pavyzdžiai verčia atkreipti dėmesį į tolesnių diskusijų sritį – minėtų dviejų kategorijų (turinio duomenų ir srauto duomenų) sujungimo, šias kategorijas kartu pavadinant komunikacijomis (elektroniniais ryšiais), problemą. Uoliau domėtis šiuo klausimu turėtų ir Valstybinė duomenų apsaugos inspekcija, kurios vienas iš svarbiausių tikslų pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 29 straipsnį yra prižiūrėti duomenų valdytojų veiklą tvarkant asmens duomenis [7, 29 str. 2 d.].

Reikia paminėti, jog skirtingai nuo informacijos apie buvusius elektroninių ryšių įvykius gavimo iš elektroninių ryšių paslaugų teikėjų, elektroniniais ryšiais perduodamos informacijos kontrolę esamuoju laiku atlieka patys kontroliuojantys subjektai. Pagal Lietuvos Respublikos elektroninių ryšių įstatymo 77 str. „kai yra motyvuota teismo nutartis, ūkio subjektai, teikiantys elektroninių ryšių tinklus ir (ar) paslaugas, privalo sudaryti techninę galimybę operatyvinės veiklos subjektams įstatymų nustatyta tvarka, ikiteisminio tyrimo įstaigoms – Lietuvos respublikos baudžiamojo proceso kodekso nustatyta tvarka, kontroliuoti elektroninių ryšių kanalais perduodamos informacijos turinį“ [9, 77 str. 3 d.]. Atkreiptinas dėmesys, jog elektroninių ryšių paslaugų teikėjams nenustatyta pareiga užtikrinti kitos elektroniniais ryšiais perduodamos informacijos kontrolę.

Diskutuotinos ir Lietuvos Respublikos operatyvinės veiklos įstatyme nustatytos elektroninių ryšių tinklais perduodamos informacijos kontrolės galimybės laiko atžvilgiu. Nors įstatyme nustatyta sankcionuoto termino pratęsimo procedūra, maksimalus terminas nenustatytas. Tai reiškia, kad nustatyta tvarka pratęsiant sankcionuotą laikotarpį, galima neribotą laiką kontroliuoti žmogaus privataus gyvenimo dalį, susijusią su elektroniniais ryšiais. Tokia padėtis gali būti vertinama kaip prieštaraujanti žmogaus teisės į privataus gyvenimo neliečiamumą ribojimo proporcingumo principui. Kaip teigiamą pavyzdį galima paminėti Lietuvos Respublikos baudžiamojo proceso kodeksą, kuris maksimalų elektroninių ryšių tinklais perduodamos informacijos ribojimo terminą riboja iki 9 mėnesių [8, 154 str., 3 d.]. Todėl Lietuvos Respublikos operatyvinės veiklos įstatyme taip pat siūlytina nustatyti maksimalų elektroninių ryšių tinklais perduodamos informacijos kontrolės terminą.

Elektroniniais ryšiais perduodamos informacijos kontrolė pagal Lietuvos Respublikos įstatymus gali būti vykdoma operatyvinio tyrimo ar baudžiamojo proceso metu, todėl šie procesai nagrinėtini atskirai.

2.1. Elektroniniais ryšiais perduodamos informacijos kontrolė vykdant operatyvinę veiklą

Lietuvos Respublikos operatyvinės veiklos įstatymo 10 str. 10 d. nustatyta, jog „telekomunikacijų operatorius ar telekomunikacijų paslaugų teikėjas privalo sudaryti techninę galimybę vykdyti telekomunikacijos priemonėmis perduodamos informacijos kontrolę“. Šioje dalyje, aprašant procedūrą, minimas terminas – techninių priemonių panaudojimas specialia tvarka. Pagal įstatymo 3 str. 8 d. „techninių priemonių panaudojimas specialia tvarka – motyvuota teismo nutartimi sankcionuotas techninių priemonių panaudojimas operatyvinėje veikloje kontroliuojant ar fiksuojant asmenų pokalbius, kitokį susižinojimą ar veiksmus [...]“. Frazė „ar veiksmus“ iš esmės turėtų apimti techninių priemonių panaudojimą renkant srauto duomenis, nes būtent srauto duomenys susiję su tam tikrais telekomunikacijų paslaugų vartotojų veiksmais. Remiantis šia sąvoka, galima teigti, jog Lietuvos Respublikos operatyvinės veiklos įstatymas numato kompiuterinių duomenų surinkimo esamuoju laiku procedūras tiek turinio, tiek srauto duomenų atžvilgiu. Tačiau paminėtinas vienas šio įstatymo trūkumas. Įstatyme vartojamos sąvokos, kurios buvo svarbios galiojant Lietuvos Respublikos telekomunikacijų įstatymui. Tuo tarpu Lietuvos Respublikos elektroninių ryšių įstatyme naudojamos šiek tiek kitokios sąvokos, pavyzdžiui, vietoje telekomunikacijos – elektroniniai ryšiai ir pan. Dėl šios priežasties minimas sąvokas patartina suvienodinti, atitinkamai pakeičiant Lietuvos Respublikos operatyvinės veiklos įstatymą.

2.2. Elektroniniais ryšiais perduodamos informacijos kontrolė baudžiamojo proceso metu

Elektroniniais ryšiais perduodamos informacijos kontrolę ikiteisminio tyrimo institucijos atlieka pagal Lietuvos Respublikos baudžiamojo proceso kodekso taisykles. Deja, išsami tokios kontrolės tvarka kodekse

nenustatyta, išskyrus, pvz., reikalavimą[6], jog telekomunikacijų operatoriai privalo sudaryti sąlygas klausytis telefoninių pokalbių ar kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją. Lietuvos Respublikos baudžiamojo kodekso 154 straipsnyje nustatyta, jog „[...] ikiteisminio tyrimo pareigūnas gali klausytis telefoninių pokalbių, kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją ar daryti įrašus [...]“. To paties straipsnio 4 dalyje nurodyta, jog „telekomunikacijų operatoriai privalo sudaryti sąlygas klausytis telefoninių pokalbių ar kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją ar daryti įrašus“. Toks neapibrėžtumas gali sąlygoti situaciją, kai telekomunikacijų operatorius nežinos apie jo tinkle vykdomą konkrečių asmenų perduodamos informacijos kontrolę.

Pažymėtina, jog pagal Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnį, kuriame numatyta, kad pagal teisėjo nutartį gali būti kontroliuojama „kita telekomunikacijų tinklais perduodama informacija“, internetu perduodamos informacijos kontrolei taip pat reikalinga teismo nutartis. Lietuvos Respublikos baudžiamojo kodekso 154 straipsnyje naudojama telekomunikacijų tinklais perduodamos informacijos kategorija, todėl atrodo, kad problemų dėl turinio ir srauto duomenų atskyrimo neturėtų kilti, nes minima kategorija apima tiek srauto, tiek turinio duomenis, kuriuos elektroninėje erdvėje, kaip jau minėta, dažnai sunku atskirti. Tačiau kodekso 154 str. 2 d. numato telekomunikacijų tinklais perduodamos informacijos kontrolės ir fiksavimo galimybę tik srauto duomenų atžvilgiu, todėl komunikacijų internetu atveju dėl šios normos įgyvendinimo gali kilti problemų. Tačiau, kita vertus, tai pateisinama tuo, jog turinio ir srauto duomenų kontrolės sąlygos gali skirtis.

Lietuvos Respublikos baudžiamojo proceso kodekse kitos (ne turinio) elektroniniais ryšiais perduodamos informacijos kontrolei nustatytos platesnės galimybės – šią informaciją galima kontroliuoti ir tais atvejais, „jeigu yra pagrindas manyti, kad tokiu būdu galima gauti duomenų apie nesunkius nusikaltimus, numatytus Lietuvos Respublikos baudžiamojo kodekso 166, 196, 197, 198(1) straipsniuose, 309 straipsnio 1 ir 2 dalyse“ [8, 154 str. 2 d.]. Taigi kodeksas įgyvendina skirtingų reikalavimų nustatymo turinio ir srauto duomenų kontrolei principą, nors, kaip minėta, šį principą sunku įgyvendinti interneto aplinkoje.

Be to, Lietuvos Respublikos baudžiamojo proceso kodekso atžvilgiu išsakytina kritika dėl vartojamų sąvokų Operatyvinės veiklos įstatyme, todėl pageidautini atitinkami (nors ir formalūs) šio kodekso pakeitimai.

3. ELEKTRONINIAIS RYŠIAIS PERDUODAMOS INFORMACIJOS KONTROLĖS PRIEŽIŪRA

Lietuvos Respublikos Vyriausybė ilgai delsė įgalioti specialią instituciją – konkretų operatyvinės veiklos subjektą. Tik 2000 metų gruodį Vyriausybės nutarime [1] buvo įvardinta, jog valstybės įgaliota institucija – Valstybės saugumo departamentas. Deja, iki šiol nenustatyta tvarka, pagal kurią Valstybės saugumo departamentas kiekvienam operatyvinės veiklos subjektui, o baudžiamajame procese – ir ikiteisminio tyrimo įstaigai, sudarytų technines galimybes savarankiškai kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį. Tokios tvarkos nebuvimas gali sudaryti prielaidas operatyvinės veiklos subjektui ar ikiteisminio tyrimo įstaigai piktnaudžiauti suteikta teise vykdyti turinio kontrolę. Europos Žmogaus Teisių Teismo praktika dėl Europos žmogaus teisių konvencijos teigia, kad valstybės turi užtikrinti, kad jų teisės aktai numatytų garantijas ir apsaugą nuo galimo piktnaudžiavimo kontroliuojant elektroninių ryšių turinį. Kadangi Lietuva ratifikavo minėtą konvenciją ir prisiėmė atitinkamus įsipareigojimus, taip pat privalo užtikrinti minimų garantijų užtikrinimą nacionaliniuose teisės aktuose.

Valstybės įgaliota institucija įvardijus Valstybės saugumo departamentą, tapo aišku, kad elektroninių ryšių tinklu siunčiamos techninės komandos „pradėti“ ar „nutraukti“ pasiklausymą ar kitą elektroninių ryšių tinklais perduodamos informacijos kontrolę bus saugomos šio departamento patalpose. Tai reiškia, kad ta pati institucija tam tikrais atvejais ir organizuos perduodamos informacijos kontrolės vykdymą, ir saugos šios kontrolės įrodymus. Manytina, jog technines komandas pradėti ar pabaigti pasiklausymą ar kitos elektroniniais ryšiais perduodamos informacijos kontrolę turi saugoti ne pati operatyvinę veiklą vykdanti institucija, nes tokiu atveju, kai ta pati institucija ir vykdo operatyvinę veiklą, ir kontroliuoja tokios veikos vykdymą, negalima užtikrinti tokios veiklos skaidrumo. Taigi tam, kad būtų galima garantuoti asmenų teisę į privatų gyvenimą, apriboti galimybes keisti saugomą informaciją apie elektroninių ryšių kontrolę, minėtos informacijos saugojimas turi būti pavestas ne Valstybės saugumo departamentui, o Generalinei prokuratūrai, nebent prokuratūra užtikrintų tinkamą tokio saugojimo kontrolę.

Kita galima elektroninių ryšių turinio ar kitos elektroniniais ryšiais perduodamos informacijos perėmimo proceso kontrolės forma – parlamentinė kontrolė. Paminėtina, jog pagal Operatyvinės veiklos įstatymą asmenų konstitucinių teisių ir laisvių apsaugą vykdant operatyvinę veiklą kontroliuoja Operatyvinės veiklos parlamentinės kontrolės komisija [10, 23 str. 2 d. 1 p.]. Ši komisija buvo sukurta tik 2003 m. pabaigoje, kilus Prezidentūros skandalui, o komisijos nuostatai buvo patvirtinti tik 2004 metais [2]. Tačiau ar vienintelei Seimo komisijai būdinga politinė operatyvinės veiklos kontrolė gali užtikrinti konkrečių asmenų teisės į privatų gyvenimą apsaugą? Be abejo, komisijos nuostatuose įtvirtintos teisės sudaro tam tikras prielaidas kontroliuoti teisėsaugos institucijas. Tačiau turint omenyje, jog komisijos nariai – išimtinai tik parlamentarai[7], t. y. politikai, kai kuriais at-

[6] Be to, šis reikalavimas pagal savo prigimtį turėtų būti išdėstytas ne Lietuvos Respublikos baudžiamojo proceso kodekse, o Lietuvos Respublikos elektroninių ryšių įstatyme.

[7] 2005 m. kovo 15 d. Lietuvos Respublikos Seimo nutarimu Nr. X-132 „Dėl Seimo operatyvinės parlamentinės kontrolės komisijos sudarymo“, Lietuvos Respublikos Seimas, vadovaudamasis Seimo statuto 80-1 straipsniu ir Operatyvinės veiklos įstatymo 23 straipsnio 1

vejais sunku išvengti politinių sprendimų. Manytina, jog šios komisijos kontrolę reikia derinti su specialios ir nuo politinės valdžios nepriklausomos institucijos (komisijos) vykdoma operatyvinės veiklos kontrole. Pagal šiuo metu galiojantį Lietuvos Respublikos operatyvinės veiklos įstatymą parlamentinei komisijai suteikta teisė tirti tik šiurkščius Operatyvinės veiklos įstatymo pažeidimo bei operatyvinės veiklos subjektų nustatytų veiklos ribų peržengimo atvejus [10, 23 str. 2 d. 5 p.]. Tuo tarpu speciali institucija galėtų nagrinėti ir paprastus skundus dėl teisės į privatų gyvenimą pažeidimo (įskaitant jau įvykusios elektroninių ryšių kontrolės teisėtumo įvertinimą). Tokia komisija taip pat turėtų teikti ir periodines ataskaitas apie vykdytas „sekimo" priemones (elektroninių ryšių kontrolės skaičius, kokiems nusikaltimams tirti buvo panaudotos elektroninio sekimo priemonės, elektroninių sekimo priemonių panaudojimo tęstinumas (laikas) ir pan.)[8]. Pavyzdžiui, JAV ataskaitos apie vykdytas elektroninių ryšių kontrolės priemones ir mastus publikuojamos viešai internete [18]. Tačiau, pavyzdžiui, Lenkijoje, kaip ir Lietuvoje, Vyriausybė viešai neskelbia ataskaitų apie vykdytos elektroninių ryšių kontrolės mastus, teigdama, jog tai yra valstybės paslaptis. Reikia pripažinti, jog tokios praktikos mažėja. Manytina, kad visuomenė turi žinoti statistinę informaciją apie vykdomą elektroninių ryšių kontrolę bei jos mastus. Štai Švedijoje generalinis prokuroras parlamentui teikia kasmetines ataskaitas apie elektroninių ryšių priežiūrą, pavyzdžiui, 2003 metais pateiktos ataskaitos už 2002 metus duomenimis, 2002 metais elektroninių ryšių kontrolės mastai padidėjo – teismai atmetė tik du prašymus vykdyti elektroninių ryšių kontrolę, o 553 prašymai buvo patenkinti. Ataskaitoje taip pat pateikiama informacija, kad 50 proc. visų elektroninių ryšių kontrolės atvejų nebuvo gauta jokios naudingos įrodomąją vertę turinčios informacijos.

Švedijoje 2003 metais Švedų-Helsinkio komitetas, nevyriausybinė organizacija, kuri prižiūri, kaip gerbiamos žmogaus teisės, pasiūlė Švedijoje stiprinti parlamentinę elektroninių ryšių sekimo kontrolę bei užtikrinti nepriklausomą elektroninių ryšių sekimo mechanizmą [16]. Vienas iš variantų – kurti nepriklausomą priežiūros instituciją.

Specialios institucijos galimybė Lietuvoje numatyta ir naujos Operatyvinės veiklos įstatymo redakcijos projekte, tačiau šis projektas Seimo nebuvo priimtas, nors buvo pateiktas svarstyti. Atkreiptinas dėmesys, jog panašios institucijos jau veikia Vokietijoje, Prancūzijoje, Jungtinėje Karalystėje ir kitose valstybėse. Be to, kaip alternatyva, svarstytinas variantas minimos specialiosios komisijos funkcijas suteikti Valstybinei duomenų apsaugos inspekcijai.

IŠVADOS

1. Lietuvos Respublikos baudžiamojo proceso kodekso galiojanti redakcija nenumato reikalavimo sankcionuoti informacijos apie buvusius elektroninių ryšių įvykius gavimą iš elektroninių ryšių paslaugų teikėjų. Tai prieštarauja Lietuvos Respublikos Konstitucijoje numatytai asmenų teisei į privataus gyvenimo neliečiamumą.

2. Siekiant užtikrinti pagarbą privačiam gyvenimui elektroniniuose ryšiuose kontroliuojant elektroninius ryšius teisėsaugos tikslais, šiuo metu stinga ir kai kurių poįstatyminių teisės aktų, kurie turėtų būti nedelsiant priimti.

3. Elektroninių ryšių paslaugų teikėjų tvarkomos informacijos, sudarančios srauto duomenis, saugojimo laikotarpį gali iš esmės keisti ES direktyva dėl privalomo srauto duomenų saugojimo. Šios direktyvos nuostatos galbūt prieštarauja Lietuvos Respublikos Konstitucijai tiek, kiek yra nustatytas reikalavimas informaciją apie srauto duomenis kaupti daugiau, negu reikia ūkinei veiklai užtikrinti. Įgyvendinant minimą direktyvą, kompetentingos institucijos turėtų imtis priemonių įvertinti šį galimą prieštaravimą.

4. Internete sunku atskirti srauto duomenis nuo turinio duomenų, tai gali apsunkinti teisės kontroliuoti ir fiksuoti telekomunikacijų tinklais perduodamus srauto duomenis įgyvendinimą, remiantis Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio 2 dalimi, todėl svarstytina turinio duomenų ir srauto duomenų kategorijų sujungimo galimybė kontroliuojant elektroninius ryšius.

5. Abejotinas sprendimas įgalioti Valstybės saugumo departamentą savo patalpose saugoti elektroninių ryšių tinklu siunčiamas technines komandas „pradėti" ar „nutraukti" pasiklausymą ar kitą elektroninių ryšių tinklais perduodamos informacijos kontrolę taip, kad komandų duomenų nebūtų galima pakeisti, nes departamentas kartu yra ir operatyvinės veiklos subjektas. Tokia situacija neatitinka demokratinės valstybės principų, kadangi ta pati institucija negali ir vykdyti operatyvinę veiklą, ir ją kontroliuoti. Turėtų būti nustatyta tokia tvarka, kad saugotų ne operatyvinės veiklos subjektas arba bent jau būtų įgyvendinta reikiama tokio saugojimo kontrolė.

6. Vienas iš pagarbos privačiam gyvenimui elektroniniuose ryšiuose užtikrinimo būdų – elektroninių ryšių kontrolės priežiūra. Dabar akivaizdu, kad elektroninių ryšių priežiūros kontrolė turėtų būti sugriežtinta. Esamoms tokios priežiūros kontrolės institucijoms turėtų būti suteikta daugiau teisių. Be to, siūlytina įkurti specialią nepriklausomą elektroninių ryšių kontrolės priežiūros instituciją.

7. Lietuvos Respublikos operatyvinės veiklos įstatyme bei Lietuvos Respublikos baudžiamojo proceso kodekse aprašytose elektroniniais ryšiais perduodamos informacijos kontrolės procedūrose vartojamos sąvokos keistinos.

---

dalimi, nutarė patvirtinti Seimo Operatyvinės veiklos parlamentinės kontrolės komisiją iš 7 narių: Vytautas Čepas, Kęstutis Daukšys, Gediminas Jakavonis, Juozas Palionis, Viktoras Rinkevičius, Vidmantas Žiemelis, Zita Žvikienė.

[8] Metinės ataskaitos, kuriose nurodyti elektroninių ryšių kontrolės mastai, trukmė ir kita informacija, jau leidžiamos tokiose valstybėse kaip Prancūzija, Švedija, Australija, Kanada, JAV ir kt.

LITERATŪRA

1. **2004 m. gruodžio 6 d.** Lietuvos Respublikos Vyriausybės nutarimas Nr. 1593 „Dėl įgaliojimų suteikimo įgyvendinant Lietuvos Respublikos elektroninių ryšių įstatymą“ // http://www.lrs.lt.
2. **2004 m. vasario 12 d.** Lietuvos Respublikos Seimo nutarimas Nr. IX-2022 „Dėl Seimo operatyvinės veiklos komisijos nuostatų patvirtinimo“ // http://www.lrs.lt.
3. **Banisar D. A.** Commentary on he Council of Europe Cybercrime Convention // http://privacy.openflows.org/pdf/coe_analysis.pdf.
4. **Broadhurst R.** Content crimes: criminality and sencorship in Asia. Conference on „The Challenge of Cybercrime“. 15–17 September, 2004. Palais de l`Europe, Strasbourg, France // http://www.coe.int.
5. **Directive 2006/24/EC** of the European Parliament and of the Council of Europe of 15 March 2006 on the retention of data processed and storedgenerated or processed in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism and amending Directive 2002/58/EC // OJ L 105/54.
6. **Electronic Communications** privacy Act. United States Code. Title 18 – Crimes and Criminal Procedure. Part I - Crimes. Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications // http://floridalawfirm.com/privacy.html.
7. **Lietuvos Respublikos** asmens duomenų teisinės apsaugos įstatymas // Valstybės žinios. 1996. Nr. 63-1479.
8. **Lietuvos Respublikos** baudžiamojo proceso kodeksas // Valstybės žinios. 2002. Nr. 37-1341.
9. **Lietuvos Respublikos** elektroninių ryšių įstatymas // Valstybės žinios. 2004. Nr. 69-2382.
10. **Lietuvos Respublikos** operatyvinės veiklos įstatymas // Valstybės žinios. 2002. Nr. 65-2633.
11. **Maxwell W.** Electronic Communications: the New EU Framework. Part I, Booklet 1.5. – New York: Oceana Publications, Inc., 2002.
12. **Privacy International** – Republic of Poland. 2004 // http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83774.
13. **Privacy International Survey** – Republic of Estonia. 2003 // http://www.privacyinternational.org/survey/phr2003/countries/estonia.htm.
14. **Privacy International Survey** – Republic of Latvia. 2003 // http://www.privacyinternational.org/survey/phr2003/countries/latvia.htm.
15. **Privay international Survey** – Finland. 2004 // http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83553.
16. **Privay international Survey** – Sweden. 2004 // http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-83530.
17. **Surveillance Act of Estonia** (February 22, 1994) // http://vlf.juridicum.su.se/master99/library2/teste/Surv.htm.
18. **The Nature and Scope** of Governmental Electronic Surveillance Activity // http://www.cdt.org/wiretap/wiretap_overview.html.
19. **The New Data Retention Directive** // European Media, IP & IT Law Review, 2006 No. 1.
20. **Žmogaus teisių** įgyvendinimas Lietuvoje: 2005 m. apžvalga. Žmogaus teisių stebėjimo institutas. 2005 // http://www.hrmi.lt.
21. **Žmogaus teisių** stebėjimo institutas: Privataus gyvenimo ribojimas elektroninių ryšių srityje nusikaltimų tyrimo ir prevencijos tikslais. 2005 // http://www.hrmi.lt.

RESTRICTION OF PRIVATE LIFE IN ELECTRONIC COMMUNICATIONS FOR CRIMINAL INVESTIGATION PURPOSES

Dr. Darius Štitilis [*]
Mykolas Romeris University

S u m m a r y

The main purpose of the article – to analyze legal problems related to the restriction of private life in electronic communications for law enforcement purposes. The present work deals with some legal regulation problems of both control of electronic communications according to Law on operative acrivities and Criminal procedure law.

In the first part of the present work legal problems, related to the control of traffic data, retained by electronic communication operators and service providers, are studied. The main problem is a lack of secondary legislation acts, related to control of private life for criminal investigation purposes. Significant importance in Lithuanian electronic communication control process also may have a proposal for a Directive on the retention of communications traffic data that would see internet data held for six months, phone data held for one year, and ISPs and telcos compensated for their compliance costs. The proposed Directive would not be applicable to the actual content of the communications.

In the second part the legal aspects of real-time collection of content and traffic data are studied. The line drawn between traffic data (who someone calls, when, for how long) and communication data (the content of telephone call) is drawn from the traditional telephone infrastructure. Adapting this ti the Internet is particular quite different, if at all possible. Is communication the content of packages? Is traffic data just packets headers? O is traffic data clickstreams, or http-requests? A possible step forward would be to define the notion of communication. Subpart 2.1 deals with the control of electronic communications during operational activities. Also subart 2.2 deals with the control of electronic communications during criminal procedure.

In the third part, the need of special institution is discussed. At that moment acredited institution, related to black boxes is State Security Department. But this department also provides operational activities and controls electronic communications itself. Another form of supervision of electronic communication control for criminal investigalion purposes is Parliamentary control, which in Lithuania is weak and should be strenghtened.

At the end of the present work the conclusions are presented.

Keywords: private life, electronic communications, control of electronic communications for criminal investigalion purposes.

[*] Mykolas Romeris University, Faculty of Economics and Finance Management, Informatics and Statistics Department, Assoc. Prof. Dr.