ISSN 2029–2236 (print)
ISSN 2029–2244 (online)
SOCIALINIŲ MOKSLŲ STUDIJOS
SOCIAL SCIENCES STUDIES
2009, 1(1), p. 205–221

IP TELEFONIJA – IŠŠŪKIS ELEKTRONINIŲ RYŠIŲ KONTROLĖS, SIEKIANT IŠTIRTI NUSIKALTIMUS, TEISINIAM REGULIAVIMUI

Darius Štitilis

Mykolo Romerio universiteto Socialinės informatikos fakulteto
Elektroninio verslo katedra
Ateities g. 20, LT-08303, Vilnius, Lietuva
Telefonas (+370 5) 2714 572
Elektroninis paštas stitilis@mruni.eu

Marius Laurinaitis

Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto
Bankininkystės ir investicijų katedra
Ateities g. 20, LT-08303 Vilnius, Lietuva
Telefonas (+370 5) 2714 572
Elektroninis paštas laurinaitis@mruni.eu
Pateikta 2008 m. gegužės 28 d., parengta spausdinti 2009 m. balandžio 14 d.

Anotacija. *Straipsnyje analizuojami IP (Interneto protokolas) telefonijos kontrolės nusikaltimų tyrimo tikslais teisinio reguliavimo, susijusio su IP telefonijos kontrole, aspektai. Straipsnį sudaro 3 dalys. Pirmoje straipsnio dalyje IP telefonija ir jos savybės analizuojamos atsižvelgiant į elektroninių ryšių kontrolės nusikaltimų tyrimo tikslus. Antroje straipsnio dalyje aptariami elektroninių ryšių kontrolės reguliavimo siekiant tirti nusikaltimus ir IP telefonijos kontrolės aspektai. Trečia straipsnio dalis skirta aptarti pagrindinėms IP telefonijos kontrolės teisinio reguliavimo problemoms, susijusioms su IP telefonijos kontrole. Atlikus analizę galima teigti, kad technologijos plėtojasi greičiau nei teisinis atitinkamų visuomeninių santykių, kontroliuojant balso telefoniją, reguliavimas, ir tai teisėsaugos institucijoms*

sudaro kliūčių kontroliuoti IP telefoniją. Straipsnyje pateikiamos IP telefonijos kontrolės siekiant ištirti nusikaltimus tobulinimo kryptys, priemonės, taip pat atitinkami pasiūlymai.

***Reikšminiai žodžiai**: informatikos teisė, IP telefonija, elektroninių ryšių kontrolė, siekiant ištirti nusikaltimus, elektroninių ryšių reguliavimas.*

Įvadas

Daug pokyčių plėtojantis elektroniniams ryšiams atsirado pradėjus diegti IP telefoniją, galutiniams paslaugų gavėjams suteikiančią judėjimo laisvę (netgi nepaisant konkrečių valstybių sienų) ir galimybę balso telefonija naudotis visur, kur yra internetas, t. y. bet kuriame pasaulio krašte esant prieinamam interneto ryšiui.

Tačiau IP telefonija ne tik suteikia neabejotinų privalumų balso paslaugų gavėjams, bet sukuria problemų teisėsaugos institucijoms siekiant tirti nusikaltimus kontroliuoti susižinojimą, paremtą minima technologija. Tuo tarpu IP telefonija dėl savo savybių tam tikrais atvejais tampa nekontroliuojama arba labai sunkiai kontroliuojama. Jau šiuo metu teisėsaugos institucijoms, atliekančioms IP telefonijos kontrolę, kyla problemų iš bendrojo interneto srauto skiriant atitinkamą turinį, dėl užsienyje esančio galutinio IP technologija paremtų balso paslaugų gavėjo kontrolės ir kt. Šie klausimai yra labai aktualūs, nes nusikaltėliai tampa vis mobilesni, ir konkretaus asmens susižinojimo kontrolė negali baigtis ties konkrečios valstybės siena. Teisėsaugos institucijų pastangos kontroliuoti nusikaltimais įtariamųjų asmenų susižinojimą taikant IP telefoniją turi atitikti naująsias IP telefonijos realijas. Tikėtina, kad dideles kliūtis tinkamai ir efektyviai kontroliuoti IP telefoniją sudaro ne tik technologiniai aspektai, tačiau ir istoriškai pasenęs teisinis elektroninių ryšių kontrolės nusikaltimų tyrimo tikslais reguliavimas.

Tad straipsnis skirtas išnagrinėti IP telefonijos kontrolės nusikaltimų tyrimo tikslais teisinį reguliavimą, sudarantį prielaidas kontroliuoti IP telefoniją, kylančias problemas bei pasiūlyti galimus jų sprendimų būdus. Straipsnio objektas – elektroninių ryšių kontrolės nusikaltimų tyrimo tikslais reguliavimas, sudarantis prielaidas IP telefonijos kontrolei nusikaltimų tyrimo tikslais. Straipsnio tikslas – išanalizuoti elektroninių ryšių kontrolės nusikaltimų tyrimo tikslais teisinį reguliavimą, susijusį su kliūtimis kontroliuoti IP telefoniją. Straipsnyje taikomas lyginamasis, analizės ir kiti metodai. Aptariami pagrindiniai teisės aktai. Analizuojant užsienio valstybių IP telefonijos kontrolės teisinį reguliavimą naudojamasi užsienio valstybių teisinių dokumentų duomenų bazėmis, statistine informacija bei kitais šaltiniais.

Tiriama tema nei Lietuvos teisės moksle, nei užsienio mokslininkų darbuose iš esmės nenagrinėta.

1. IP telefonija bei jos savybės, turinčios įtakos elektroninių ryšių kontrolei nusikaltimų tyrimo tikslais

Elektroniniai ryšiai apima ne tik balso telefoniją, bet ir interneto paslaugas. Nepaisant to, šiame straipsnyje bus nagrinėjama tik balso telefonijos kontrolė.

Elektroninių ryšių kontrolę[1] (plačiąja prasme), vykdomą taikant operatyvinius ar kitus nusikaltimų tyrimus, galima skirstyti į dvi grupes: 1) buvusių elektroninių ryšių įvykių kontrolė – informacijos apie buvusius elektroninių ryšių įvykius (srauto duomenis)[2] 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, t. y. srauto duomenų kontrolė)[3].

Šiai elektroninių ryšių kontrolei įtakos turi elektroninių ryšių sektoriaus pokyčiai. Atsiranda būtinybė kontroliuoti taikant IP telefoniją technologiją vykstantį susižinojimą vis dažniau pakeičiantį tradicinę telefoniją[4]. IP telefonija (angl. *Internet Telephony*, arba *Voice over IP, VoIP*) – balso ryšys, perduodamas duomenų perdavimo tinklais naudojant interneto protokolą[5]. Tokiuose tinkluose informacija nepriklausomai nuo jos pobūdžio (vaizdinė, garsinė, tekstinė) yra suskaidoma į individualius skaitmeninius paketus, kurie į savo tikslą juda visiškai nepriklausomai vienas nuo kito. Internetu telefono pokalbius galima perduoti be tradicinių telefono ryšio paslaugų teikėjų (t. y. centralizuotų jų duomenų/apskaitos bazių). Šiuo atveju teikėjas tiesiogiai nevaldo balsu perduodamos informacijos. Tai įmanoma naudojant tris pagrindines įrangos konfigūracijas: kompiuteris-kompiuteris, kompiuteris-telefonas bei telefonas-telefonas[6]. Taigi IP telefonijos atveju paslaugų teikimas gali būti atskirtas nuo infrastruktūros teikimo. Visais anksčiau minėtais atvejais elektroninių ryšių paslaugų teikėjai papildomai neapmokestina sujungimo, todėl nekaupiami su sujungimais susiję srauto duomenys, įvykę pokalbiai neįtraukiami į paslaugų teikėjų apskaitos sistemas.

---

1 Elektroninių ryšių kontrolę (angl. *Lawful interception*) galima apibrėžti kaip laikantis įstatymo reikalavimų bei gavus atitinkamus kompetentingų institucijų leidimus teisėsaugos institucijų vykdomą elektroninių ryšių perėmimą.

2 Pagal ERĮ 3 str. 52 p. srauto duomenimis laikytini „duomenys, tvarkomi siekiant perduoti informaciją elektroninių ryšių tinklu ir (arba) tokio perdavimo apskaitai“. Detalesnis srauto duomenų aprašymas pateikiamas Direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje Nr. 2002/58/EB preambulės 15 p.: „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“.

3 Štitilis, D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais. *Jurisprudencija*. 2006, 9(87).

4 *Common Position on VoIP* [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.erg.eu.int/doc/publications/erg_07_56rev2_cp_voip_final.pdf>.

5 *Ibid.*

6 Du telefonus galima sujungti per internetą, naudojant VoIP tinklo sąsajas.

Labai svarbi IP telefonijos ypatybė ta, jog dažnai yra sunku atskirti informacijos srautus: pokalbių srautą nuo kitų duomenų srauto, nes balsinis paketas IP pakete nėra specialiai pažymėtas[7]. Tai taip pat gerokai apsunkina galimybę kontroliuoti IP telefoniją.

IP telefonijos atveju galinis įrenginys gali būti ne tik telefonas, bet ir kompiuteris, kurio vieta gali būti nesusieta su konkrečiu geografiniu adresu. Dėl to, kad nepaprastai plačiai galima naudotis internetu, IP telefonijos paslauga gali būti teikiama netgi už valstybės teritorijos ribų, dėl to itin sunku tampa „sekti“ IP abonentus.

Manoma, jog įdiegus reikiamas programines šifravimo priemones, IP telefonijos praktiškai neįmanoma pasiklausyti (jei vienas IP telefonijos abonentas skambina kitam)[8]. IP telefonijos ypatybė ta, jog papildomą šifravimą savo galiniuose įrenginiuose gali įsidiegti du tarpusavyje bendraujantys asmenys. Tai skiriasi nuo centralizuotos pokalbių šifravimo sistemos, kurią elektroninių ryšių paslaugų teikėjai yra įgyvendinę tradiciniame telefono ryšyje. Esant centralizuotai pokalbių šifravimo sistemai paslaugų teikėjas teisėsaugos institucijoms atskleisdamas šifravimo raktus sudaro galimybę iššifruoti visų per paslaugų teikėjo sistemas centralizuotai perduodamų pokalbių turinį. Kai pokalbius šifruoja atskiri vartotojai, elektroninių ryšių paslaugų teikėjas neturi nei raktų, nei kitos galimybės iššifruoti užšifruotą informaciją. Tačiau tokius raktus gali turėti IP telefonijos paslaugų teikėjas.

2. Pagrindiniai elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, teisinio reguliavimo principai ir IP telefonija

Toliau šiame straipsnyje bus nagrinėjama, kaip reguliuojama elektroninių ryšių kontrolė, siekiant ištirti nusikaltimus, ir bus vertinama šio reguliavimo mastas bei santykis su IP telefonijos savybėmis.

2.1. Pagrindinės tarptautinio bei ES elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, reguliavimo nuostatos

Tarptautiniai dokumentai dėl ryšių kontrolės, siekiant ištirti nusikaltimus, – Europos Tarybos 1995 m. sausio 17 d. sprendimas dėl teisėto telekomunikacijų perėmimo[9] bei 2001 m. lapkričio 23 d. Konvencija dėl elektroninių nusikaltimų[10]. Pirmasis doku-

7 Gelvanovska, N. IP telefonijos reguliavimo aspektai. Pranešimas 2004 m. gruodžio 7 d. seminare „Elektroninių ryšių plėtros tendencijos ir reguliuojančios institucijos vaidmuo“, Vilnius [interaktyvus]. 2004 [žiūrėta 2009-04-06]. <http://www.rrt.lt/conferences/files/EC_2004_12_07_Gelvanovska.pdf; 16 sk.>.

8 *Fiksuoto ryšio telefonija* [interaktyvus]. [žiūrėta 2009-04-06]. <http://elekta.lt/article/archive/133/>.

9 Council Resolution of January 17, 1995 on the Lawful Interception of Telecommunications [interaktyvus]. [žiūrėta 2009-04-06] <http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html>; < http://www.interlex.it/testi/eu95lawf.htm>.

10 *Convention on Cybercrime* [interaktyvus]. 2001 [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

mentas yra rekomendacinio pobūdžio, o Konvencija yra privaloma prie jos prisijungusioms valstybėms[11].

1995 m. priimant sprendimą dėl teisėto telekomunikacijų perėmimo telekomunikacijos buvo atskirtos nuo interneto, IP telefonija nebuvo naudojama asmenims susižinoti. Tačiau sprendime nurodoma, jog turi būti sudaryta galimybė teisėsaugos institucijoms perimti visus telekomunikacijomis siunčiamus duomenis[12]. Taip pat nurodoma, jog telekomunikacijų operatoriai turi sudaryti technines programines galimybes (sąsajas) kontroliuoti telekomunikacijas. Dėl šių sąsajų telekomunikacijų operatoriai ir teisėsaugos institucijos tariasi atsižvelgdami į atitinkamoje valstybėje susiklosčiusią patirtį[13]. Tačiau atkreiptinas dėmesys jog sprendimo nuostatos susijusios su telekomunikacijų operatorių – teisėsaugos institucijų santykiais, kai pokalbių srautas nukreipiamas per konkretų telekomunikacijų operatorių, ir jis užtikrina skambučio/pokalbio srautų valdymą, šifravimą bei kitas technines operacijas ir taip pat turi galimybę valdyti bei pritaikyti technines sąlygas siekdamas teisėtai kontroliuoti.

Konvencija, kaip pirmasis tarptautinio pobūdžio dokumentas, skirtas spręsti nusikalstamų veikų kompiuteriniuose tinkluose problemoms[14], technologiškai yra daug pažangesnis teisės aktas. Konvencijos priėmimo metu elektroninių ryšių bei telekomunikacijų konvergavimo tendencijos buvo aiškiai apibrėžtos. Tai liudija ir Konvencijos normos, susijusios su kompiuterinių duomenų kontrole siekiant ištirti nusikaltimus. Konvencijoje reguliuojamas kompiuterinių duomenų surinkimas tuo pat metu, apimantis tiek turinio, tiek srauto duomenis. Konvencijoje teigiama, jog kiekviena šalis priima tokius teisės aktus, kurie kompetentingoms institucijoms sudarytų galimybę surinkti srauto ir/ar turinio duomenis, perduodamus naudojantis kompiuterine sistema[15]. Konvencijos paaiškinamojoje ataskaitoje patikslinama, jog kompiuterinių duomenų perėmimo, siekiant ištirti nusikaltimus, reguliavimas dėl telekomunikacijų ir elektroninių ryšių konvergencijos turėtų būti taikomas visoms technologijoms, kuriomis taikant kompiuterines sistemas komunikuojama panaudojant elektronines komunikacijas – elektroninių ryšių tinklus[16]. Taigi tai turėtų apimti ir IP telefoniją.

Šiame straipsnyje nagrinėjamos aktualiausios Konvencijos Proceso teisės skirsnio normos, o ypač:

1. Normos dėl operatyvioje darbo atmintyje laikomų kompiuterinių duomenų išsaugojimo, susijusios su srauto duomenimis.

---

11 Konvencija įsigaliojo 2004 m. liepos 1 d. 2008 m. sausio 1 dienai prie konvencijos buvo prisijungusios 22 valstybės. Lietuva prie konvencijos prisijungė 2004 m**.** (2004 m. sausio 22 d. Įstatymas dėl Konvencijos dėl elektroninių nusikaltimų ratifikavimo. *Valstybės žinios*. 2004, Nr. 36-1178).

12 *Council Resolution of January 17, 1995 on the Lawful Interception of Telecommunications* [interaktyvus]**.** [žiūrėta 2009-04-06]. < http://www.interlex.it/testi/eu95lawf.htm>.

13 *Ibid.*

14 Kiškis, M., *et al. Teisės informatika ir informatikos teisė.* Vilnius: Mykolo Romerio universiteto leidybos centras, 2006, p. 233.

15 *Convention on Cybercrime* [interaktyvus]. 2001 [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

16 *Explanatory Report to Convention on Cybercrime* [interaktyvus]. [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Šios normos susijusios su jau išsaugotų srauto duomenų tolesniu saugojimu, siekiant juos pateikti kompetentingoms institucijoms. Remiantis Konvencija „šalys narės privalo <...> užtikrinti, kad toks operatyvus srauto duomenų išsaugojimas yra galimas, nepaisant to, ar tokią informaciją perdavė vienas ar daugiau paslaugos teikėjų <...>, taip pat <...> užtikrinti, kad <...> būtų operatyviai atskleista pakankamai srauto duomenų, leidžiančių Šaliai nustatyti paslaugos teikėjus ir tos informacijos perdavimo kelią.“[17] Atkreiptinas dėmesys, kad šios normos gali būti veiksmingos tik tuo atveju, kai paslaugos teikėjas fiksuoja ir saugo informaciją apie srauto duomenis, tačiau tais atvejais, kai IP telefonijos srauto duomenys nėra fiksuojami (nes jų nereikia siekiant apmokestinti), minimos normos neturi prasmės.

2. Normos dėl kompiuterinių duomenų surinkimo realiuoju laiku (atitinkamai skirstytinos į srauto duomenų ir turinio duomenų surinkimą).

Remiantis Konvencija „<...> Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas: a) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti; b) priversti paslaugos teikėją pagal jo technines galimybes: i) tos Šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba ii) bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti realiuoju laiku srauto duomenis/turinio duomenis, susijusius su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema.“[18]

Anksčiau minėtos nuostatos labai svarbios atliekant IP telefonijos kontrolę, tačiau paremtos nacionaline valstybių jurisdikcija. Tuo tarpu IP telefonija gali būti už valstybės teritorijos ribų, ir dėl to gali atsirasti tam tikrų kliūčių[19] kontroliuoti susižinojimą susijusį su IP telefonija, kuriam nacionalinių valstybių sienos nėra aktualios.

Svarbu paminėti tai, jog normos suteikia galimybę pačioms teisėsaugos institucijoms rinkti ir įrašinėti srauto bei turinio duomenis[20], o tai labai aktualu kontroliuojant IP telefoniją. Taip pat svarbu paminėti ir tai, jog normos leidžia įpareigoti paslaugų teikėją pagal technines galimybes rinkti srauto bei turinio duomenis. Deja, konvencija neįpareigoja paslaugų teikėjų užtikrinti papildomas technines galimybes[21]. Kitaip tariant, jei paslaugos teikėjo sistema nefiksuoja tam tikrų srauto ar turinio duomenų, teisėsaugos institucijos pagal konvenciją negali įpareigoti paslaugos teikėją pradėti fiksuoti atitinkamus duomenis. Tai gerokai riboja galimybę IP telefoniją kontroliuoti.

17 *Convention on Cybercrime* [interaktyvus]. 2001 [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

18 *Ibid.*

19 Rašydami apie kliūtis autoriai turi omenyje bendradarbiaujančių subjektų skaičių (remiantis nustatyta procedūra, kuri dažnai yra biurokratinė, turi bendradarbiauti bent dviejų valstybių teisėsaugos institucijos, atitinkami operatoriai ar paslaugų teikėjai) bei laiko tarpą, per kurį informacija gaunama (uždelsus, informacija gali būti prarasta).

20 Deja, kaip rodo kai kurių valstybių praktika, dažnai teisėsaugos institucijos, kontroliuodamos srauto ar turinio duomenis, neveikia savarankiškai, o yra susijusios su konkrečiais paslaugų teikėjais.

21 *Explanatory Report to Convention on Cybercrime* [interaktyvus]. [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Paminėtina taip vadinama ES duomenų saugojimo direktyva.[22] Siekiant teisėsaugos institucijoms teikti informaciją apie srauto duomenis šioje Direktyvoje numatyta pareiga elektroninių ryšių paslaugų teikėjams srauto duomenis kaupti ir saugoti nuo 6 mėnesių iki 2 metų nuo jų užfiksavimo. Saugotini duomenys susiję su telefono ryšio bei interneto paslaugomis, įskaitant ir IP telefoniją, tačiau Direktyva netaikoma elektroninių ryšių turiniui. Atkreiptinas dėmesys, kad pagal Direktyvą, pareiga elektroninių ryšių paslaugų ar viešųjų ryšių tinklų teikėjams išsaugoti atitinkamus duomenis kyla tik tuomet, kai tokie duomenys generuojami arba tvarkomi. Atkreiptinas dėmesys, kad su IP telefonija susiję srauto duomenys tam tikrais atvejais paslaugų teikėjų duomenų bazėse dažnai net nėra generuojami/fiksuojami.

2.2. Dabartinis elektroninių ryšių kontrolės teisinis reguliavimas Lietuvoje

Lietuvos Respublikoje elektroninių ryšių kontrolę nusikaltimų tyrimo tikslais reglamentuoja trys pagrindiniai teisės aktai: Lietuvos Respublikos baudžiamojo proceso kodeksas (toliau – BPK)[23], Lietuvos Respublikos operatyvinės veiklos įstatymas (toliau – OVĮ)[24] bei Lietuvos Respublikos elektroninių ryšių įstatymas (toliau – ERĮ)[25].

BPK normos numato elektroninių ryšių tinklais perduodamos informacijos kontrolę, jos fiksavimą ir kaupimą baudžiamojo proceso metu. BPK 154 straipsnyje numatyta, jog galima „<…> klausytis asmenų pokalbių, perduodamų elektroninių ryšių tinklais, daryti jų įrašus, kontroliuoti kitą elektroninių ryšių tinklais perduodamą informaciją ir ją fiksuoti bei kaupti <...>“[26]. Iki 2007 m. BPK normos reglamentavo ne elektroninių ryšių, o telekomunikacijų tinklais perduodamos informacijos kontrolę, tačiau po 2007 m. atliktų BPK 154 straipsnio pakeitimų, reguliavimas apima ir internetu perduodamų duomenų kontrolę, taigi ir IP telefoniją.

Pagal OVĮ operatyvinės veiklos subjektai turi teisę vadovaudamiesi specialia tvarka naudoti technines priemones ir gauti informaciją iš telekomunikacijų operatorių bei telekomunikacijų paslaugų teikėjų[27]. OVĮ taip pat palieka diskrecijos teisę turinio kontrolę vykdyti nepriklausomai nuo technologijos. Srauto duomenų kontrolė, kaip numatyta OVĮ 10 straipsnio 12 dalyje, gali būti vykdoma gaunant duomenis iš telekomunikacijų operatorių ir telekomunikacijų paslaugų teikėjų. Tai reiškia, kad pagal OVĮ, teisėsaugos institucijos operatyviniams tikslams gali gauti tik tuos duomenis, kuriuos operatoriai fiksuoja ir nustatytą laikotarpį saugo.

Tokią tvarką numato ir ERĮ, kuriame numatytas įpareigojimas atskleisti teisėsaugos institucijoms turimą informaciją apie srauto duomenis. Tačiau, kaip jau minėta, IP

22 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti direktyvą 2002/58/EB.

23 Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios*. 2002, Nr. 37-1341.

24 Lietuvos Respublikos operatyvinės veiklos įstatymas. *Valstybės žinios*. 2002, Nr. 65-2633.

25 Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.

26 Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios*. 2002, Nr. 37-1341; 154 str.

27 Lietuvos Respublikos operatyvinės veiklos įstatymas. *Valstybės žinios*. 2002, Nr. 65-2633.

telefonijos atveju paslaugos teikėjas tokios informacijos gali neturėti, nors įgyvendinus papildomas technines programines priemones minima informacija vis dėlto gali būti fiksuojama. Reikia paminėti tai, jog dabartinė ERĮ 77 straipsnio redakcija netgi draudžia paslaugų teikėjams fiksuoti papildomus duomenis.

Dėl turinio duomenų kontrolės ERĮ nustatyta pareiga „sudaryti techninę galimybę operatyvinės veiklos subjektams įstatymų nustatyta tvarka, o ikiteisminio tyrimo įstaigoms – BPK nustatyta tvarka, kontroliuoti elektroninių ryšių tinklais perduodamos informacijos turinį“[28]. Labai svarbi nuostata, jog „tam reikalinga įranga įsigyjama ir išlaikoma valstybės lėšomis“[29]. Ši nuostata gali būti panaudota įsigyjant įrangą, reikalingą kontroliuoti ir IP telefoniją.

2007 m. į nacionalinę teisę turėjo būti perkelta jau minėta duomenų saugojimo direktyva, tačiau kilus diskusijoms dėl duomenų saugojimo bei pateikimo išlaidų operatoriams kompensavimo direktyvą įgyvendinantis ERĮ pakeitimo ir papildymo projektas kol kas galutinai nepatvirtintas[30]. Atkreiptinas dėmesys į tai, jog Lietuvoje aktuali duomenų saugojimo ir pateikimo išlaidų paskirstymo konstitucingumo problema. Pirminiame ERĮ papildymo ir pakeitimo projekte, įgyvendinančiame duomenų saugojimo direktyvą, duomenų saugojimo ir pateikimo išlaidų kompensavimo klausimas iš viso nebuvo sprendžiamas. Tačiau Lietuvos Respublikos Konstitucinis Teismas 2002 m. rugsėjo 19 d. nutarime yra konstatavęs, kad „nusikaltimų užkardymas, tyrimas, nustatymas yra valstybės nuolatinė funkcija, kuri turi būti finansuojama valstybės lėšomis“[31]. Lietuvos Respublikos Konstitucinis Teismas nurodė, kad „Konstitucijos 23 straipsnyje įtvirtintas nuosavybės neliečiamumas ir apsauga reiškia tai, kad negali būti nustatyta tokio teisinio reguliavimo, kuriuo ne valstybės nuosavybės subjektai būtų įpareigoti nuolat savo nuosavybę naudoti valstybės funkcijoms, finansuojamoms valstybės lėšomis, vykdyti. Ne valstybės nuosavybės subjektai gali būti įpareigoti savo nuosavybe prie visuomenės ypatingų reikmių užtikrinimo prisidėti tiek, kiek pareiga prisidėti prie šių reikmių užtikrinimo esant nepaprastoms sąlygoms išplaukia iš Konstitucijos“[32]. Tokia pozicija pagrįsta Lietuvos Respublikos Konstitucijos 23 straipsnyje įtvirtinta nuosavybės nelie-

28 Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*. 2004, Nr. 69-2382.

29 *Ibid.*

30 2007 m. pabaigoje Lietuvos Respublikos Seimas minimą projektą priėmė, tačiau Lietuvos Respublikos Prezidentas 2007 m. gruodžio 18 d. dekretu įstatymą grąžino Seimui svarstyti pakartotinai iškeldamas duomenų saugojimo kompensavimo problemą.

31 Lietuvos Respublikos Konstitucinio Teismo nutarimas „Dėl Lietuvos Respublikos telekomunikacijų įstatymo“ (2000 m. liepos 11 d. redakcija) 27 straipsnio 2 dalies, Lietuvos Respublikos telekomunikacijų įstatymo 27 straipsnio pakeitimo įstatymo 2 straipsnio 1 dalies, Lietuvos Respublikos telekomunikacijų įstatymo (2002 m. liepos 5 d. redakcija) 7 straipsnio 3 dalies 4 punkto, Lietuvos Respublikos operatyvinės veiklos įstatymo (2002 m. birželio 20 d. redakcija) 7 straipsnio 3 dalies 6 punkto, Lietuvos Respublikos baudžiamojo proceso kodekso 48 straipsnio 1 dalies (1961 m. birželio 26 d. redakcija) ir 75 straipsnio 1 dalies (1975 m. sausio 29 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai“. <http://www.lrkt.lt/dokumentai/2002/n020919.htm>. III sk. 3.1.

32 2007 m gruodžio 28 d. Lietuvos Respublikos Prezidento dekretas Nr. 1K-1215 „Dėl Lietuvos Respublikos Seimo priimto Lietuvos Respublikos elektroninių ryšių įstatymo 1, 3, 7, 12, 34, 77 straipsnių, devintojo skirsnio ir priedo pakeitimo ir papildymo nauju priedu įstatymo gražinimo Lietuvos Respublikos Seimui pakartotinai svarstyti“. *Valstybės žinios*. 2008, Nr. 1-7.

čiamumo koncepcija[33]. Autorių nuomone, ši koncepcija turėtų būti taikoma sprendžiant duomenų saugojimo direktyvos įgyvendinimo klausimus. Deja, Lietuvos Respublikos Seime 2008 m. antrąjį pusmetį užregistruota antroji ERĮ pakeitimo ir papildymo projekto redakcija numato dalies duomenų saugojimo išlaidų (nereikalingų elektroninių ryšių operatorių ūkinei veiklai užtikrinti) kompensavimą ir todėl kelia abejonių dėl atitikimo tiek Lietuvos Respublikos Konstitucijos 23 straipsnio nuostatų, tiek 2002 m. rugsėjo 19 d. Lietuvos Respublikos Konstitucinio Teismo nutarimo.

3. Elektroninių ryšių IP telefonijos kontrolės, siekiant ištirti nusikaltimus, teisinio reguliavimo problemos

3.1. Įpareigojimo generuoti ir atskleisti IP telefonijos duomenis, taip pat sudaryti papildomas technines sąlygas kontroliuoti perduodamus duomenis problema

Bene didžiausia problema, susijusi su IP telefonijos kontrole, nusikaltimų tyrimo tikslais yra ta, jog dabartinis teisinis reguliavimas įpareigoja elektroninių ryšių paslaugų teikėjus atskleisti tik tuos duomenis, kuriuos šie subjektai generuoja arba sudaryti sąlygas kontroliuoti tik tokią perduodamą informaciją, kuri gali būti fiksuojama paslaugų teikėjų ūkinės veiklos metu.

Daugelio užsienio valstybių teisės aktuose yra tik bendrojo pobūdžio nuostatos dėl elektroninių ryšių perėmimo. Pavyzdžiui, Jungtinės Karalystės 2000 m. Tyrimo teisių reguliavimo įstatymas telekomunikacijų operatoriams nustato pareigą suteikti perėmimo galimybę šių operatorių sistemose, taip pat teikti tam tikrus srauto duomenis[34]. Panaši situacija kitose valstybėse: Olandijoje, Šveicarijoje, Australijoje, Naujojoje Zelandijoje[35]. Tačiau, kaip jau minėta, įdiegus IP telefoniją nemažai duomenų, reikalingų teisėsaugai, iš viso nėra generuojami/fiksuojami[36]. Nors minimų valstybių teisės aktuose kol kas nėra specialiųjų nuostatų, įpareigojančių operatorius imtis tam tikrų papildomų techninių priemonių, siekiant generuoti su IP telefonija susijusius duomenis, tačiau atlikus kai kurių užsienio valstybių praktikos analizę taip pat pastebėta, jog šiose valstybėse stebimi procesai, kai teisės aktais siekiama elektroninių ryšių paslaugų teikėjus įpareigoti užtikrinti papildomas, su ūkine veikla nesiejamas, technines priemones siekiant užtikrinti kuo geresnes galimybes kontroliuoti IP telefoniją (srauto ir turinio duomenis).

---

33 Lietuvos Respublikos Konstitucija. *Valstybės žinios.* 1992, Nr. 33-1014.

34 Regulation of Investigatory Powers Act, 2000 [interaktyvus]. 2000 [žiūrėta 2009-04-06]]. <http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1>, chapter. 2.>.

35 Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Surveillance of Communications. Legal and Technical Standards for Surveillance: Building in Big Brother [interaktyvus]. Privacy and Human Rights, 2006 [žiūrėta 2009-04-06]]. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559085&als[theme]=Privacy%20and%20Human%20Rights>.

36 Tačiau gali būti generuojami įgyvendinus papildomas technines priemones.

Minėtinas Jungtinės Karalystės pavyzdys. Šioje valstybėje IP telefonijos kontrolė kelia ypač didelį teisėsaugos susirūpinimą. Jungtinėje Karalystėje kol kas nėra specialaus teisinio reguliavimo, susijusio su IP telefonijos kontrole. Manoma, jog dėl to Jungtinės Karalystės teisėsaugos institucijos negali perimti IP telefonijos duomenų. Yra žinoma, kad policija ir saugumo tarnybos stengėsi paveikti vyriausybę baimindamosi dėl potencialios IP technologijos. Jų tikslas – gauti papildomą atitinkamų paslaugų teikėjų pagalbą ir taip kontroliuoti pasiklausymus bei surasti būdą identifikuoti vartotojus, nustatyti kas skambina, kam, įrašyti juos[37].

Teisėsaugos institucijos kreipėsi į Ofcom[38] pabrėždamos susirūpinimą IP telefonija. Kreipimesi buvo pažymėta, kad teisėsaugos institucijos susiduria su sunkumais, kuriuos sukelia IP telefonijos kontrolė, ir kad šie sunkumai kelia realią grėsmę jų demokratinei visuomenei, dėl to privalu paslaugų teikėjams išsaugoti tinkamas ataskaitas apie suteiktas paslaugas taikant IP technologiją[39].

JAV daugelis paslaugų tiekėjų neatsisakydavo perduoti bet kokią informaciją apie IP telefonijos klientus, tačiau tam tikrais atvejais to padaryti jie negalėdavo dėl sunkumų atskirti, pavyzdžiui, balso perdavimą nuo kitų duomenų internete[40]. Tam reikalingos papildomos investicijos. Daugelis paslaugų tiekėjų JAV neprieštarauja bendradarbiauti su teisėsaugos institucijomis, tačiau yra ir kitų atvejų, pavyzdžiui, Skype. Todėl vis dažniau pasisakoma dėl atitinkamų įpareigojimų teisės aktuose. JAV Federalinė susisiekimo komisija pastaruoju metu svarstė nemažai klausimų, kaip bendradarbiavimo su teisėsaugos institucijomis įstatymo (CALEA[41]) reikalavimus pritaikyti naujoms technologijos, tokioms kaip IP telefonija[42]. Vienas probleminis aspektas dėl principinio interneto paslaugų teikėjų bendradarbiavimo vis dėlto išspręstas. 2006 m. buvo įgyvendinti FTB siūlymai atitinkamai papildyti teisės aktus, jog interneto paslaugų teikėjai pritaikytų savo tinklus taip, kad atitiktų vyriausybinę specifikaciją CALEA, o tai galbūt suteiktų policijai prieigą kontroliuoti IP telefoniją[43]. Deja, šis įpareigojimas yra bendro pobūdžio,[44] ir nesprendžiama problema, kai interneto paslaugų teikėjai nors ir nefiksuoja tam tikros su

37 *UK police pressure Voip companies to yield customer data.* Security agencies [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.futureintelligence.co.uk/content/view/34/63>.

38 OFCOM – Jungtinės Karalystės elektroninių ryšių sektorių reguliuojanti institucija. [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.ofcom.org.uk/>.

39 *UK police pressure Voip companies to yield customer data.* Security agencies [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.futureintelligence.co.uk/content/view/34/63>.

40 *VoIP: It's not so easy to listen in.* CNET News [interaktyvus]. [žiūrėta 2008-05-06]. <http://www.news.com/VoIP-Its-not-so-easy-to-listen-in/2100-7352_3-5159159.html>.

41 CALEA – The Communications Assistance for Law Enforcement Act. [interaktyvus]. [žiūrėta 2009-04-06]. <http://epic.org/privacy/wiretap/calea/calea_law.html>.

42 CRS *Report for Congress. Digital surveillance: The Communications Assistance for law Enforcement Act.* [interaktyvus]. 2007 [žiūrėta 2009-04-06]. <http://fas.org/sgp/crs/intel/RL30677.pdf>.

43 Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Surveillance of Communications. Legal and Technical Standards for Surveillance: Building in Big Brother [interaktyvus]. Privacy and Human Rights, 2006 [žiūrėta 2009-04-06] <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559085&als[theme]=Privacy%20and%20Human%20Rights>.

44 Nustatyta bendroji pareiga bendradarbiauti su teisėsauga, bet ne specialioji pareiga diegti specialias techninės programines priemones, suteikiančias galimybes fiksuoti daugiau duomenų nei reikia ūkiniams poreikiams.

IP telefonija susijusios informacijos, tačiau panaudojus tam tikrą papildomą programinę techninę įrangą tokia informacija galėtų būti fiksuojama.

Kaip rodo atlikta analizė, rinkoje jau pasirodė daugelis IP telefonijos perėmimo programinės įrangos produktų, kurie suteiktų galimybę operatoriams generuoti daugiau IP telefonijos duomenų nei tai daroma iki šiol. Autorių nuomone, elektroninių ryšių paslaugų teikėjai diegdami IP platformas turėtų būti įpareigoti įdiegti galimybę visiškai kontroliuoti IP telefoniją. Tačiau pagrindinė problema – tokios funkcijos finansavimas. Išanalizavus tarptautinį ir ES elektroninių ryšių kontrolės reguliavimą paaiškėjo, jog Konvencija dėl elektroninių nusikaltimų neįpareigoja operatorių užtikrinti papildomų techninių programinių priemonių negu jų reikia ūkinei veiklai vykdyti. Autorių nuomone, nepaisant to, iš principo nėra kliūčių tokiems įpareigojimams, turint omenyje bendrąjį tikslą – nusikaltimų tyrimą ir kontrolę. Tik svarbu paminėti vieną aspektą, jog elektroninių ryšių kontrolės, siekiant ištirti nusikaltimus, finansavimas – nacionalinės teisės objektas. Reguliavimo praktika atitinkamose nacionalinėse valstybėse yra labai skirtinga: vienose valstybėse (pvz., Australijoje[45]) išlaidas, susijusias su bendrąja elektroninių ryšių kontrole, turi padengti patys operatoriai. Kitose valstybėse taikoma praktika buvo pripažinta kaip antikonstitucinė. Pavyzdžiui, 2003 m. Austrijos Konstitucinis Teismas savo sprendime nurodė, kad įstatymas, įpareigojantis telekomunikacijų operatorius savo lėšomis užtikrinti telekomunikacijų perėmimo galimybę, yra antikonstitucinis[46]. Kaip parodė Lietuvos teisinės praktikos analizė, tokia funkcija pagal Lietuvos Respublikos Konstituciją taip pat turėtų būti finansuojama iš Lietuvos Respublikos biudžeto. Lietuvos teisės aktuose galėtų būti nustatytas įpareigojimas elektroninių ryšių paslaugų teikėjams užtikrinti papildomas technines programines IP telefonijos kontrolės priemones (daugiau srauto duomenims), ir tokia papildoma funkcija turėtų būti finansuojama valstybės. Kitose nacionalinėse valstybėse atitinkami įpareigojimai galėtų būti nustatomi atsižvelgiant į nacionalinės teisės ypatumus.

3.2. IP telefonijos kontrolė, siekiant ištirti nusikaltimus, ir šifravimo problema

Daugelyje nacionalinių valstybių centralizuotai užšifruoto bendrojo telekomunikacijų srauto iššifravimo problemos jau sprendžiamos įpareigojant operatorius atskleisti šifravimo raktus/imtis priemonių iššifruoti turinį (Jungtinėje Karalystėje, Naujoje Zelandijoje ir kt.[47]). Tačiau teisėsaugos institucijoms kyla problemų iššifruoti necentralizuotai užšifruotą IP telefonijos srautą. Teisėsaugai galėtų pagelbėti IP telefonijos pas-

45 Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Surveillance of Communications. Legal and Technical Standards for Surveillance: Building in Big Brother [interaktyvus]. Privacy and Human Rights, 2006 [žiūrėta 2009-04-06]. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559085&als[theme]=Privacy%20and%20Human%20Rights>.

46 Austrian Federal Constitutional Court. VfGH, G 37/02 ua, February 27, 2003 [interaktyvus]. [žiūrėta 2009-04-06]. <http://epic.org/privacy/intl/austrian_vfgh-022703.html>.

47 Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Surveillance of Communications. Legal and Technical Standards for Surveillance: Building in Big Brother [interaktyvus]. Privacy and Human Rights, 2006 [žiūrėta 2009-04-06]. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559085&als[theme]=Privacy%20and%20Human%20Rights>.

laugų teikėjai, tačiau šie neturi jokių pareigų kontroliuoti elektroninius ryšius. Situaciją sunkina ir tai, jog dažnai IP telefonijos paslaugos teikėjai – užsienio kompanijos, kurių veiklą reguliuoja užsienio valstybių įstatymai, ir nacionalinės teisėsaugos institucijos neturi reikiamų teisinių svertų įpareigoti šias kompanijas bendradarbiauti.

Autorių nuomone, vienas iš galimų problemos sprendimo būdų – nustatyti pareigą tam tikromis techninėmis priemonėmis suteikti prieigą (atitinkamus šifravimo raktus) prie necentralizuotai užšifruoto IP telefonijos srauto. Tačiau tokia pareiga turėtų būti taikoma ne elektroninių ryšių paslaugų teikėjams[48], o atitinkamos IP telefonijos programinės įrangos gamintojams – IP telefonijos paslaugų teikėjams. Taigi galėtų būti nustatytas įpareigojimas bendradarbiauti su teisėsaugos institucijomis arba, kitaip tariant, atitinkamose IP telefonijos programose palikti galimybę (taip vadinamos „užpakalinės durys“) iššifruoti užšifruotą IP telefonijos srautą. Būtent įpareigojimas palikti „užpakalines duris“ sudarytų teisėsaugos institucijoms vienintelę galimybę „apeiti“ šifravimo užkardą.

Kol kas ši užkarda yra pakankamai neįveikiama netgi JAV teisėsaugai. Pavyzdžiui, JAV teisėsaugos institucijos bandė perimti IP telefonijos srautą naudodamos savo policijos skaitmenines sekimo sistemas, bet negalėjo jų visiškai panaudoti dėl atitinkamų trūkumų – kuoduotės. Tad JAV svarstoma IP telefoniją kontroliuoti atitinkamose programose paliekant „užpakalines duris“.

Paminėtina Vokietijos praktika, kai šios valstybės teisėsauga siekdama iššifruoti necentralizuotai užšifruotą IP telefonijos srautą pati ėmėsi priemonių kontroliuoti atskirų vartotojų kompiuterius. Tačiau 2007 m. tokie veiksmai Vokietijos teismų buvo įvertinti nepalankiai ir traktuotini kaip žmogaus teisių pažeidimas[49]. Vokietijos Aukščiausiasis Teismas nusprendė, kad policija negali slaptai įsibrauti į įtariamųjų asmenų kompiuterius, nes nėra nustatytos jokios teisėtos tvarkos slaptos policijos padaliniams prasiskverbti į kompiuterines sistemas. Vokietijos federalinio teismo sprendimu pripažįstama, kad įtariamojo asmens kompiuterį be jo žinios policija jai priimtinais tyrinėjimo metodais tyrinėti negali, nes taip pažeidžiamas privatumas[50]. Nors ši byla daugiau susijusi su sankcionavimo problema, patys neteisėtos kontrolės faktai rodo, jog Vokietijos teisėsauga siekdama kontroliuoti IP telefoniją ieško iššifravimo būdų. Todėl Vokietijoje taip pat svarstoma, jog suteikti galimybę iššifruoti užšifruotą IP telefonijos srautą galėtų IP telefonijos paslaugų teikėjai.

Autorių nuomone, siekiant tirti ir kontroliuoti nusikaltimus neturėtų būti kliūčių atitinkamų valstybių teisės aktuose įvesti įpareigojimą prieš teikiant į rinką IP telefonijos produktus įdiegti teisėtos kontrolės galimybę. Tai suteiktų galimybę teisėsaugos institucijoms „įveikti“ jau minėtą šifravimo užkardą ir įgyvendinti teisėtas susižinojimo kontrolės galimybės funkcijas. Tačiau tokia funkcija remiantis Lietuvos nacionalinės teisės ypatumais taip pat turėtų būti finansuojama valstybės. Taip pat labai svarbu, jog minimo įpareigojimo įgyvendinimas turėtų būti koordinuojamas tarptautiniu mastu.

---

48 Elektroninių ryšių paslaugų teikėjai tiesiog neturėtų techninių galimybių minimą pareigą įgyvendinti.

49 *German Court Shoots Down Computer Surveillance* [interaktyvus]. The Associated Press, 2008 [žiūrėta 2009-04-06]. < http://www.ibtimes.com/articles/20080227/german-court-shoots-down-pc-surveillance.htm>.

50 *Germany`s Highest Court Restricts Internet Surveillance* [interaktyvus]. 2008 [žiūrėta 2009-04-06]. <http://www.dw-world.de/dw/article/0,2144,3152627,00.html>.

3.3. Tarptautinis IP telefonijos kontrolės aspektas ir jurisdikcijos problema

IP telefonija tampa tarptautiniu reiškiniu (globalusis IP telefonijos paslaugų pobūdis), tuo tarpu IP telefonijos kontrolės reguliavimas įgyvendinamas vidaus reguliavimo įrankiais ir ribojamas nacionalinių valstybių jurisdikcijų. Naivu būtų tikėtis, jog dėl IP telefonijos kontrolės būtų koreguojami nacionalinės jurisdikcijos principai. Tad, autorių nuomone, operatyvios IP kontrolės galimybės turėtų būti gerinamos skatinant tarptautinį bendradarbiavimą bei diegiant efektyvesnį tarptautinio masto reguliavimą, atitinkamai turintį įtakos valstybių nacionalinės teisės normoms.

Atkreiptinas dėmesys, jog nepaisant to, kad Konvencija dėl elektroninių nusikaltimų skirta kriminalizuoti bei tirti elektroninius nusikaltimus, anksčiau šiame straipsnyje analizuotos konvencijos proceso teisės skirsnio nuostatos taikomos ir bet kokių kitų nusikaltimų įrodymams rinkti elektroniniu būdu[51]. Taigi konvencijos antrojo skirsnio nuostatos, skirtos valstybių savitarpio pagalbai, turėtų būti taikomos ir IP telefonijos, už nacionalinių valstybių ribų, kontrolei, netgi jei tiriami ir ne elektroniniai nusikaltimai. Todėl skirtingų valstybių teisėsaugos institucijų bendradarbiavimui gerinti kontroliuojant IP telefoniją turėtų būti aktyviau naudojamasi konvencijos suteikiamomis galimybėmis.

Tačiau netgi konvencijoje nurodytoms savitarpio pagalbos priemonėms dažnai būtinos neadekvačios laiko sąnaudos. Pavyzdžiui, nors pagal konvenciją, „skubiais atvejais kiekviena Šalis gali perduoti savitarpio pagalbos arba su tuo susijusios informacijos prašymus operatyviomis ryšio priemonėmis, tarp jų faksimiliniu ryšiu arba elektroniniu paštu“[52]. Ši tarptautinė sutartis nustato daug kitų biurokratinių suvaržymų, galinčių trukdyti operatyviai kontroliuoti IP telefoniją. Čia galima paminėti ir pareigą bendradarbiauti pasitelkiant atskiras institucijas[53]. Autorių nuomone, tarpinės institucijos ir kiti formalumai apsunkina IP telefonijos kontrolės galimybes už nacionalinės valstybės ribų.

Paminėtina, jog konvencijos 32 straipsnis dėl tarptautinės laikomųjų kompiuterinių duomenų prieigos nustato tam tikrą tvarką, kai gaunant reikiamus duomenis gali būti išvengiama tarpinių institucijų[54]. Tačiau šis straipsnis taikytinas daugiau tais atvejais, kai reikia gauti saugomas elektroninio pašto žinutes[55] ar kitą vartotojo išsaugotą informaciją, be to, būtinas informaciją teikiančios šalies teisiškai įgaliotas sutikimas.

Vis dėlto nepaisant jau galiojančių Konvencijos dėl elektroninių nusikaltimų proceso teisės ir savitarpio pagalbos normų (kurios, autorių nuomone, atskirose valstybėse dar nėra visiškai įgyvendintos), IP kontrolė turėtų būti paremta dar naujoviškesniais procesinio bendradarbiavimo bei savitarpio pagalbos principais. Vienas iš galimų variantų, jog tarptautinės IP telefonijos kontrolės mechanizmai galėtų būti įgyvendinti tai-

51 *Convention on Cybercrime,* 2001 [interaktyvus]. [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

52 *Ibid.*, 25 str. 3 d.

53 *Ibid.,* 27 str. 2 d. a.

54 *Ibid.*

55 Explanatory Report to Convention on Cybercrime [interaktyvus]. [žiūrėta 2009-04-06]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

kant „on-line“ duomenų bazių principą. Tačiau tokiam mechanizmui įgyvendinti reikia nuodugniai išanalizuoti bei įvertinti privatumo apsaugos, sankcionavimo, nacionalinės jurisdikcijos ir kitus aspektus.

Minėtasis naujoviškesnis panašaus pobūdžio bendradarbiavimo mechanizmas jau skatinamas Europos Tarybos rekomendacijose[56], tačiau kol kas šios rekomendacijos neprivalomos ir paremtos gera šalių valia bei noru bendradarbiauti. Nepaisant to, tai vienas pirmųjų žingsnių siekiant geresnės tarptautinės IP telefonijos kontrolės.

Išvados

1. IP telefonijos savybės turi įtakos elektroninių ryšių procesui, siekiant kontroliuoti nusikaltimų tyrimą. Jos apsunkina galimybę įgyvendinti elektroninių ryšių kontrolę (IP telefonijos globalumas, atsietumas nuo tradicinių telefonijos tinklų, decentralizuoto šifravimo galimybės).

2. Elektroninių ryšių kontrolės teisinis reguliavimas, siekiant ištirti nusikaltimus tarptautiniu mastu, beveik nekoordinuojamas, išskyrus Konvencijos dėl elektroninių nusikaltimų nuostatas. Šias nuostatas tinkamai įgyvendinus valstybėse narėse vis dėlto lieka iš dalies neišspręstos problemos dėl įpareigojimų operatoriams užtikrinti technines IP telefonijos kontrolės galimybes bei problemos dėl jurisdikcijos/IP telefonijos globalumo santykio bei operatyvios IP telefonijos kontrolės. Bendroji duomenų saugojimo direktyva taikoma tik fiksuojamiems/generuojamiems duomenims, o IP telefonijos duomenys tam tikrais atvejais iš viso nefiksuojami.

3. Elektroninių ryšių kontrolės Lietuvoje teisinis reguliavimas siekiant ištirti nusikaltimus (kaip ir daugelyje kitų valstybių) nukreiptas kontroliuoti/gauti operatoriaus valdomą informaciją. Tuo tarpu IP telefonijoje elektroninių ryšių paslaugų teikėjas tam tikrais atvejais nevaldo balsu perduodamos informacijos ir dėl to jos negali pateikti teisėsaugos institucijoms srauto duomenų arba sudaryti galimybę kontroliuoti perduodamą informaciją. Tačiau yra techninės galimybės, įgyvendinus papildomas priemones, kontroliuoti ar valdyti tokią informaciją.

4. Įgyvendinant Lietuvoje Duomenų saugojimo direktyvą Nr. 2006/24/EB aktualus ir duomenų saugojimo bei pateikimo teisėsaugos institucijoms išlaidų kompensavimo konstitucingumo aspektas.

5. ERI operatoriai/paslaugų teikėjai diegdami IP platformas turi būti įpareigoti įdiegti papildomos IP telefonijos kontrolės galimybę. Tokios funkcijos finansavimas turėtų būti sprendžiamas atsižvelgiant į Lietuvos nacionalinės teisės ypatumus – finansuojamas valstybės lėšomis.

6. Siekiant spręsti necentralizuoto IP telefonijos informacijos srauto iššifravimo problemą svarstytina galimybė įpareigoti IP telefonijos programose įgyvendinti „užpakalinių durų“ principą, t. y. teisėto informacijos iššifravimo, vykdomo teisėsaugos ins-

56 Tackling cybercrime: guidance on sharing internet data. International Herald Tribune. April 2Tech News Review, 2008 [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.iht.com/articles/2008/04/02/business/cybercrime.php>; <http://www.technewsreview.com.au/article.php?article=4472 >.

titucijų, galimybę. Lietuvoje tokios funkcijos įgyvendinimas turėtų būti finansuojamas valstybės lėšomis.

7. Kontroliuojant tarptautinio pobūdžio IP telefoniją pakankamai svertų suteikia Konvencija dėl elektroninių nusikaltimų, tačiau nustato ir tam tikrus suvaržymus. Tokio pobūdžio IP telefonijos kontrolės mechanizmai galėtų būti dar naujoviškesni ir užtikrinti „on-line“ prieigą prie kontroliuotinų duomenų.

Literatūra

Štitilis, D. Privataus gyvenimo elektroniniuose ryšiuose ribojimas nusikaltimų tyrimo tikslais. *Jurisprudencija*. 2006, 9(87).

ERG (07) 56rev2 Common Position on VoIP [interaktyvus]. [žiūrėta 2009-04-06]]. <http://www.erg.eu.int/doc/publications/erg_07_56rev2_cp_voip_final.pdf>.

Gelvanovska, N. Elektroninių ryšių plėtros tendencijos ir reguliuojančios institucijos vaidmuo, 2004 [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.rrt.lt/conferences/files/EC_2004_12_07_Gelvanovska.pdf>.

Fiksuoto ryšio telefonija [interaktyvus]. [žiūrėta 2009-04-06]. <http://elekta.lt/article/archive/133/>.

Council Resolution of January 17, 1995 on the Lawful Interception of Telecommunications [interaktyvus]. [žiūrėta 2009-04-06] <http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html>.

Convention on Cybercrime, Budapest, November, 23, 2001 [interaktyvus]. 2001 [žiūrėta 2009-04-06]]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

Kiškis, M.; Petrauskas, R.; Rotomskis, R.; Štitilis, D. *Teisės informatika ir informatikos teisė.* Vilnius: Mykolo Romerio universiteto leidybos centras, 2006.

Explanatory Report to Convention on Cybercrime [interaktyvus]. [žiūrėta 2009-04-06]]. <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti direktyvą 2002/58/EB [2002].

Lietuvos Respublikos baudžiamojo proceso kodeksas. *Valstybės žinios.* 2002, Nr. 37-1341.

Lietuvos Respublikos operatyvinės veiklos įstatymas. *Valstybės žinios.* 2002, Nr. 65-2633.

Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios.* 2004, Nr. 69-2382.

Lietuvos Respublikos Konstitucinio teismo nutarimas dėl Lietuvos Respublikos telekomunikacijų įstatymo (2000 m. liepos 11 d. redakcija) 27 straipsnio 2 dalies, Lietuvos Respublikos telekomunikacijų įstatymo 27 straipsnio pakeitimo įstatymo 2 straipsnio 1 dalies, Lietuvos Respublikos telekomunikacijų įstatymo (2002 m. liepos 5 d. redakcija) 7 straipsnio 3 dalies 4 punkto, Lietuvos Respublikos operatyvinės veiklos įstatymo (2002 m. birželio 20 d. redakcija) 7 straipsnio 3 dalies 6 punkto, Lietuvos Respublikos baudžiamojo proceso kodekso 48 straipsnio 1 dalies (1961 m. birželio 26 d. redakcija) ir 75 straipsnio 1 dalies (1975 m. sausio 29 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.lrkt.lt/dokumentai/2002/n020919.htm>.

2007 m gruodžio 28 d. Lietuvos Respublikos Prezidento dekretas Nr. 1K-1215 “Dėl Lietuvos Respublikos Seimo priimto Lietuvos Respublikos elektroninių ryšių įstatymo 1, 3, 7, 12, 34, 77 straipsnių, devintojo skirsnio ir priedo pakeitimo ir papildymo nauju priedu įstatymo grąžinimo Lietuvos Respub-

likos Seimui pakartotinai svarstyti. *Valstybės žinios*. 2008, Nr. 1-7.

Lietuvos Respublikos Konstitucija. *Valstybės žinios*. 1992, Nr. 33-1014.

Regulation of Investigatory Powers Act, [interaktyvus]. 2000 [interaktyvus]. [žiūrėta 2009-04-06] <http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1>.

Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Surveillance of Communications. Legal and Technical Standards for Surveillance: Building in Big Brother [interaktyvus]. Privacy and Human Rights, 2006 [žiūrėta 2009-04-06]. <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559085&als[theme]=Privacy%20and%20Human%20Rights>.

UK police pressure Voip companies to yield customer data. Security agencies [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.futureintelligence.co.uk/content/view/34/63/>.

VoIP: It's not so easy to listen in. CNET News [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.news.com/VoIP-Its-not-so-easy-to-listen-in/2100-7352_3-5159159.html>.

CRS Report for Congress. Digital surveillance: The Communications Assistance for law Enforcement Act. June 8, 2007 [interaktyvus]. [žiūrėta 2009-04-06]. <http://fas.org/sgp/crs/intel/RL30677.pdf>.

Austrian Federal Constitutional Court. VfGH, G 37/02 ua, February 27, 2003 [interaktyvus]. [žiūrėta 2009-04-06]. <http://epic.org/privacy/intl/austrian_vfgh-022703.html>.

German Court Shoots Down Computer Surveillance. The Associated Press. February 27, 2008 [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.nytimes.com/aponline/technology/AP-Germany-Computer-Surveillance.htm?_r=1&oref=sloginhttp://www.ibtimes.com/articles/20080227/german-court-shoots-down-pc-surveillance.htm>.

Germany`s Highest Court Restricts Internet Surveillance. DW-World.de, February 27, 2008 [interaktyvus]. [žiūrėta 2009-04-06]. <http://www.dw-world.de/dw/article/0,2144,3152627,00.html>.

Tackling cybercrime: guidance on sharing internet data. International Herald Tribune. April 2. Tech News Review, 2008 [interaktyvus]. [žiūrėta 2009-04-06] <http://www.iht.com/articles/2008/04/02/business/cybercrime.php>.

CALEA – The Communications Assistance for Law Enforcement Act. [interaktyvus]. [žiūrėta2009-04-06].<http://www.technewsreview.com.au/article.php?article=4472>.

The Communications Assistance for Law Enforcement Act [interaktyvus]. [žiūrėta 2009-04-06]. <http://epic.org/privacy/wiretap/calea/calea_law.html>.

INTERNET TELEPHONY – CHALLENGE FOR LEGAL REGULATION OF SURVEILLANCE OF ELECTRONIC COMMUNICATIONS

Darius Štitilis, Marius Laurinaitis

Mykolas Romeris University, Lithuania

Summary. *Lawful interception (wiretapping) is the interception of electronic communications by law enforcement agencies and intelligence services. However, Voice over IP (VoIP) technologies have introduced new challenges for law enforcement agencies and intelligence services. Whilst the detailed requirements for lawful interception differ from one jurisdiction*

to another, the general requirements are the same. However, these requirements are outdated for the new technologies, such as VoIP. The article analyzes legal regulation of lawful interception of VoIP. The subject of this article relates to legal regulation of lawful interception at both – international (regional) and national levels. The purpose of this article is to analyze the principles of legal regulation of lawful interception and to raise the main problems related to VoIP interception. The methods of comparison and analysis as well as some others have been applied in the article. International (regional) legal documents (Convention on Cybercrime, Data Retention directive, ect.), legal instruments in foreign countries (UK, Germany, USA, etc.) as well as periodicals and statistical information have been referred to in order to analyze the legal regulation of lawful interception of VoIP. Also the situation in Lithuania, related with the legal regulation of lawful interception of VoIP is analyzed.

The analysis provided in the article makes it possible to assert that international, as well as national regulation of lawful interception of VoIP (including Lithuania) needs to be improved. The authors have indicated the main problems, such as the extent of obligation to cooperate with law enforcement agencies and intelligence services, non-centralized encryption of VoIP (which encumbers lawful interception of VoIP) and exterritorial nature of VoIP (which contradicts with the principle of national jurisdiction). To this end, different ways and measures of improving the legal regulation of lawful interception of VoIP have been discussed in this article.

***Keywords**: internet telephony, surveillance of electronic communcations, regulation of electronic communications.*

Darius Štitilis, Mykolo Romerio universiteto Socialinės informatikos fakulteto Elektroninio verslo katedros docentas. Mokslinių tyrimų kryptis: informatikos teisė.

Darius Štitilis, Mykolas Romeris University, Faculty of Social Informatics, Department of Informatics and Statistics, associated professor. Research interests: IT law.

Marius Laurinaitis, Mykolo Romerio universiteto Ekonomikos ir finansų valdymo fakulteto Bankininkystės ir investicijų katedros lektorius. Mokslinių tyrimų kryptis: informatikos teisė.

Marius Laurinaitis, Mykolas Romeris University, Faculty of Social Informatics Department of Banking and Investments, lecturer. Research interests: IT law.