Jurisprudencija, 2005, t. 67(59); 20–28

BAUDŽIAMOJI TEISĖ, PROCESAS, KRIMINALISTIKA

KAI KURIE KONVENCIJOS DĖL ELEKTRONINIŲ NUSIKALTIMŲ PROCESO TEISĖS SKIRSNIO ĮGYVENDINIMO LIETUVOJE ASPEKTAI

Doc. dr. Darius Štitilis

Mykolo Romerio universiteto Valstybinio valdymo fakulteto Teisinės informatikos katedra
Ateities g. 20, LT–08303 Vilnius
Telefonas 271 45 71
Elektroninis paštas stitilis@mruni.lt

Dr. Rolandas Krikščiūnas

Mykolo Romerio universiteto Teisėsaugos fakulteto Kriminalistikos katedra
Ateities g. 20, LT–08303 Vilnius
Telefonas 271 46 11
Elektroninis paštas rolandkr@mruni.lt

Prof. dr. Rimantas Petrauskas

Mykolo Romerio universiteto Valstybinio valdymo fakulteto Teisinės informatikos katedra
Ateities g. 20, LT–08303 Vilnius
Telefonas 271 45 71
Elektroninis paštas rpetraus@mruni.lt

Pateikta 2004 m. gruodžio 2 d.
Parengta spausdinti 2005 m. gegužės 3 d.

Pagrindinės sąvokos: elektroniniai nusikaltimai, elektroninių nusikaltimų tyrimas.

Santrauka

Šio straipsnio objektas – Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimas Lietuvoje. Straipsnio tikslas – išanalizuoti kai kurias pagrindines Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvos Respublikos teisinėje sistemoje problemas. Straipsnio uždaviniai: įvertinti Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio pagrindinių nuostatų įgyvendinimo Lietuvoje būklę; identifikuoti pagrindines Konvencijos dėl elektroninių nusikaltimų proceso teisės skirsnio įgyvendinimo Lietuvoje problemas ir pateikti galimus šių problemų sprendimo būdus.

Straipsnyje taikomi lyginamosios analizės, lyginamasis ir kiti metodai, remiamasi užsienio valstybių doktrina bei periodine literatūra. Straipsnį sudaro įvadas, trys skyriai ir išvados. Pirmajame skyriuje analizuojamas Konvencijos dėl elektroninių nusikaltimų nuostatų dėl operatyvaus laikomųjų kompiuterinių duomenų išsaugojimo įgyvendinimas. Antrajame skyriuje analizuojamas Konvencijos dėl elektroninių nusikaltimų nuostatų dėl laikomųjų kompiuterinių duomenų paieškos ir poėmio įgyvendini-

mas. Trečiajame skyriuje analizuojamas Konvencijos dėl elektroninių nusikaltimų nuostatų dėl kompiuterinių duomenų surinkimo realiuoju laiku įgyvendinimas. Straipsnio pabaigoje formuluojamos išvados.

Įvadas

Lietuvos Respublikos prisijungimas prie Konvencijos dėl elektroninių nusikaltimų (toliau kai kur šiame straipsnyje – Konvencija) turėjo didelės įtakos Lietuvos nacionalinei baudžiamajai teisei. Nors dar prieš Konvencijos pasirašymą priimtame naujajame Lietuvos Respublikos baudžiamajame kodekse jau buvo įvestas naujas skirsnis „Nusikaltimai informatikai“[1], kuriame nustatyta atsakomybė už nusikaltimus, keliančius grėsmę saugiam kompiuterinės informacijos apdorojimui, svarbūs Lietuvos Respublikos baudžiamojo kodekso papildymai buvo atlikti 2004 m. pradžioje. Įgyvendinant Konvenciją, nuo 2004 m. vasario 14 d. įsigaliojo nauji Lietuvos Respublikos baudžiamojo kodekso papildymai, kuriais į minėtą skirsnį įvestos dvi naujos veikos: neteisėtas prisijungimas prie kompiuterio ar kompiuterių tinklo (198–1 str.) bei neteisėtas disponavimas įrenginiais, kompiuterinėmis programomis, slaptažodžiais, prisijungimo kodais ir kitais duomenimis, skirtais nusikaltimams daryti (198–2 str.). Buvo papildyti ir kiti „tradiciniai“ straipsniai, pavyzdžiui, 309 straipsnis, nustatantis atsakomybę už disponavimą pornografinio turinio dalykais.

Tačiau vienas iš pagrindinių Konvencijos tikslų – ne tik unifikuoti nacionalinius baudžiamuosius įstatymus dėl elektroninių nusikaltimų[2], bet ir tobulinti nacionalinę baudžiamojo proceso teisę. Tokie elektroninių nusikaltimų požymiai kaip globalumas, elektroninė veikos forma yra gana rimta kliūtis tirti minimus nusikaltimus. Vienos iš pagrindinių problemų kovojant su elektroniniais nusikaltimais yra nusikaltimo subjekto identifikavimas, taip pat nusikalstamos veikos masto ar poveikio įvertinimas [1, p. 133]. Taip pat iššūkį kelia elektroninės informacijos, kuri gali tapti nusikalstamos veikos įrodymu, pažeidžiamumas, galimybė ją pakeisti ar sunaikinti. Užsienio valstybių praktika rodo, kad dažnai neužtenka galiojančių procesinių normų, kurios istoriškai pritaikytos tradiciniams nusikaltimams tirti (pvz., kratos išplėtimo kompiuteriniuose tinkluose problema).

Konvencijoje išskirtas atskiras skirsnis, skirtas vienodinti valstybių nacionalinių įstatymų proceso normas. Šiuo 2 skirsniu siekiama tradicines procesines priemones, tokias kaip kratą ir poėmį, pritaikyti elektroninei aplinkai. Taip pat siekiant tradicines įrodymų rinkimo priemones, pavyzdžiui, kratą, poėmį, padaryti efektyviomis besikeičiančioje elektroninėje aplinkoje, nustatomos tokios naujos priemonės kaip operatyvus laikomųjų kompiuterinių duomenų išsaugojimas ir kitos. Išskirtinos šios toliau nagrinėtinos pagrindinės proceso teisės skirsnio nuostatos dėl procesinių priemonių: operatyvus laikomųjų kompiuterinių duomenų išsaugojimas, laikomųjų kompiuterinių duomenų paieška ir poėmis bei kompiuterinių duomenų surinkimas realiuoju laiku.

Konvencijos apžvalgoje teigiama, kad Lietuva, siekdama įgyvendinti Konvencijos nuostatas, pakeitė Lietuvos Respublikos baudžiamojo proceso kodeksą [2; 4]. Prisijungus prie Konvencijos Lietuvos Respublikos baudžiamojo proceso kodeksas buvo papildytas bei pakeistas (pvz., kodekso 154 str. papildytas antraja dalimi[3]). Tačiau ar įstatymo leidėjas identifikavo visas su elektroniniais nusikaltimais susijusias procesines problemas, kurias bandoma spręsti Konvencijos proceso teisės skirsnio nuostatomis? Taigi šis straipsnis skirtas atsakyti į minėtą klausimą ir įvertinti pagrindines Konvencijos proceso teisės skirsnio įgyvendinimo Lietuvos Respublikos teisinėje sistemoje problemas, kurios gali tapti rimta kliūtimi tiriant elektroninius nusikaltimus.

I. Operatyvus laikomųjų kompiuterinių duomenų išsaugojimas

Konvencijoje dėl elektroninių nusikaltimų teigiama, kad „*kiekviena šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti įgalinant jos kompetentingas institucijas nurodyti arba panašiai pasirūpinti operatyviu konkrečių kompiuterinių duomenų, įskaitant srauto duomenis, laikomus kompiuterinėje sistemoje, išsaugojimu, ypač kai yra pagrindo manyti, jog tie kompiuteriniai duomenys gali*

[1] Iki 2004 m. vasario mėn. šį skirsnį sudarė trys straipsniai, numatantys baudžiamąją atsakomybę už kompiuterinės informacijos sunaikinimą ar pakeitimą (196 str.), kompiuterinės programos sunaikinimą ar pakeitimą ir kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo sutrikdymą (197 str.) bei kompiuterinės informacijos pasisavinimą ar skleidimą (198 str.).

[2] Terminas „elektroniniai nusikaltimai“ šiame straipsnyje bus vartojamas atsižvelgiant į Elektroninių nusikaltimų konvencijoje siūlomą veikų sąrašą, ir kartu bus platesnis nei „informatikos nusikaltimų“ terminas.

[3] Žr. 2004 m. sausio 29 d. Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio pakeitimo ir papildymo įstatymą Nr. IX–1993 // Žin. 2002. Nr. 37–1341.

būti nesunkiai prarasti arba pakeisti“ [3, 16 str. 1 d.]. Konvencijos 17 straipsnyje taip pat reglamentuojamas minimų išsaugotų duomenų atskleidimo galimybės užtikrinimas, o 18 straipsnyje – nurodymas dėl duomenų pateikimo.

Poreikis išsaugoti kompiuterinius duomenis gali kilti tais atvejais, kai atliekant tyrimą nustatyta, jog tam tikri kompiuterių duomenys tarp kitų duomenų yra laikomi atitinkamo paslaugų teikėjo serveryje, kur teikėjas verslo tikslais kaupia tam tikro laikotarpio duomenis. Norint išskirti reikiamą informaciją iš duomenų srauto arba ją išimti, reikalinga laikina duomenų apsauga. Tai gali būti įmanoma įgyvendinti tik tuo atveju, jei tyrimo organai turės atitinkamas teises įpareigoti paslaugų teikėją išsaugoti saugomus kompiuterių duomenis [4, p. 207].

Ši priemonė taikytina tuo atveju, kai kompiuteriniai duomenys jau išsaugoti. Tačiau tyrimui svarbūs kompiuteriniai duomenys, nors ir išsaugoti, per trumpą laiką gali būti ištrinami. Pavyzdžiui, galimas atvejis, kad paslaugos teikėjo užfiksuoti kompiuteriniai duomenys kompiuterių sistemoje saugomi ne ilgiau nei kelios valandos ar kelios paros, nes tai numato teisės aktų reikalavimai. Tuo atveju, jei kompiuteriniai duomenys laikytini asmens duomenimis, asmens duomenų apsaugą reglamentuojantys teisės aktai reikalauja tokius duomenis sunaikinti (arba padaryti anonimiškus) iš karto, kai šie duomenys tampa nereikalingi ūkinei veiklai užtikrinti. Paminėtina, jog Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 3 straipsnyje numatyti bendrieji duomenų apsaugos principai reikalauja tam tikro tipo, t. y. asmens duomenis ištrinti, jei šie duomenys nereikalingi verslo tikslams. Panašūs principai taikytini pagal Lietuvos Respublikos elektroninių ryšių įstatymo 64 straipsnio nuostatas ir srauto duomenų saugojimo atvejams. Galima pamanyti, kad vadovaujantis šiais principais ūkio subjektams negalima nustatyti pareigos saugoti asmens duomenis ilgiau, nei reikia ūkinėms reikmėms. Tačiau minėtos nuostatos įgyvendina 95/46/EB ir 2002/58/EB direktyvų reikalavimus. Paminėtina, jog nors šios direktyvos nustato pareigą duomenis sunaikinti iš karto, kai jie tampa nereikalingi, šalys narės gali priimti teisės aktus, kuriuose nusikaltimų prevencijos bei tyrimo tikslais būtų nustatytos išimtys.

Daugelyje valstybių operatyvaus laikomųjų kompiuterinių duomenų išsaugojimo problema jau išspręsta įstatymo lygiu [4, p. 208]. Pavyzdžiui, JAV įstatymai numato įpareigojimo išsaugoti kompiuterinius duomenis, kurie gali būti įrodymais byloje, galimybę. Pagal JAV įstatymų sąvado 18 antraštės 2703 paragrafo (f) (1) dalį, telekomunikacijų operatoriai ir interneto paslaugų teikėjai pagal kompetentingų institucijų reikalavimus privalo imtis visų priemonių, siekiant išsaugoti jų žinioje esančius kompiuterinius duomenis, kol jie bus išimti pagal nustatytas procedūras. Antroje dalyje nustatyta, jog gali būti reikalaujama išsaugoti duomenis ne ilgiau kaip 90 dienų (numatant galimybę pratęsti terminą dar 90 dienų) [5, Title 18, Part 1, Chapter 121, par. 2703 (f) (2)]. Kai kuriose Europos valstybėse (Bulgarija ir kt.) baudžiamojo proceso įstatymų pakeitimai, susiję su operatyviu laikomųjų kompiuterinių duomenų išsaugojimu, buvo padaryti būtent įgyvendinant Konvenciją dėl elektroninių nusikaltimų [2; 12].

Paminėtina, jog Konvencijos rengėjų nuomone, tokia teisė įpareigoti subjektą išsaugoti laikomuosius kompiuterinius duomenis nacionalinėje teisėje turi būti įtvirtinta ir siekiant sudaryti galimybę padėti kitai valstybei tarptautiniu lygiu išsaugant aktualius kompiuterinius duomenis savo teritorijoje. Taip būtų užtikrinta, jog svarbūs kompiuteriniai duomenys nebūtų prarasti iki to laiko, kol bus nustatyta tvarka gautas teisinės pagalbos prašymas suteikti informaciją. Atsižvelgiant į tai, kad nusikaltimo tyrimo procese skirtingų valstybių teisėsaugos institucijos privalo bendradarbiauti viena su kita tiek oficialiai, tiek neoficialiai, gali kilti tam tikrų problemų. Jei vienos iš valstybių teisės normos nenustato konkrečių elektroninės informacijos rinkimo įgaliojimų tokia valstybė iš esmės gali būti nepajėgi reaguoti į prašymą suteikti pagalbą.

Ar nurodymas išsaugoti kompiuterinius duomenis, laikomus kompiuterių sistemoje, gali būti traktuojamas kaip nauja procesinė prievartos priemonė? Kaip rodo teisinė praktika, toks duomenų išsaugojimas daugelyje valstybių laikytinas nauja teisine priemone ar procedūra pagal nacionalinę teisę [1, p. 155].

Ar Lietuvoje anksčiau minėtų tikslų negalima pasiekti panaudojant jau esamas procesines prievartos priemones, įskaitant kitas teisės aktų normas? Kadangi Konvencijoje operatyvus laikomųjų kompiuterinių duomenų išsaugojimas traktuojamas daugiau kaip procesinė prievartos priemonė, numatyta nacionalinių valstybių baudžiamuosiuose procesiniuose įstatymuose, toliau nagrinėtinos tik Lietuvos Respublikos baudžiamojo proceso kodekso normos.

Lietuvos Respublikos baudžiamojo proceso 154 str. nustatyta procesinė prievartos priemonė – telekomunikacijų tinklais perduodamos informacijos kontrolė ir įrašų darymas. Minėtame kodekso straipsnyje nurodoma, jog „(*...) ikiteisminio skyriaus pareigūnas gali klausytis telefoninių pokalbių, kontroliuoti kitą telekomunikacijų tinklais perduodamą informaciją (...)*“ [6, 154 str. 1 d.]. Pagal Lietuvos

Respublikos baudžiamojo proceso kodekso komentarą, „telekomunikacijų tinklais perduodamos informacijos kontrolė bei įrašų darymas – procesinė prievartos priemonė, kurią taikant ikiteisminio tyrimo pareigūnas įstatymo nustatyta tvarka klausosi procese dalyvaujančių asmenų telefoninių pokalbių, kontroliuoja kitą telekomunikacijų tinklais perduodamą informaciją ir daro įrašus, siekdamas nustatyti reikšmingas aplinkybes nusikalstamai veikai tirti“ [7, p. 387]. Atkreiptinas dėmesys, jog ši prievartos priemonė taikoma kompiuteriniams duomenims perimti ateityje, tuo tarpu operatyvaus laikomųjų kompiuterinių duomenų išsaugojimo priemonė skirta jau išsaugotų kompiuterinių duomenų saugojimui užtikrinti. Be to, telekomunikacijų tinklais perduodama informacija yra daug siauresnė kategorija nei laikomi kompiuteriniai duomenys. Pavyzdžiui, elektroninių ryšių paslaugų teikėjas gali teikti kompiuterinių duomenų saugojimo (ang. *hosting*) paslaugas. Šie kompiuterių duomenys nebus susiję su telekomunikacijų tinklais perduodama informacija.

Kita vertus, ikiteisminio tyrimo pareigūnas vietoj oficialaus nurodymo išsaugoti laikomus kompiuterinius duomenis gali atlikti kratą ir taip paimti tyrimui svarbią kompiuterinę informaciją. Taip būtų pasiekti tie patys tikslai, kaip ir operatyvaus laikomųjų kompiuterinių duomenų išsaugojimo atveju – svarbi informacija elektroninė forma būtų išsaugota. Nustatyta tvarka kratai reikalinga sankcija ir tai gali apsunkinti reikiamų kompiuterinių duomenų paėmimą. Kita vertus, baudžiamojo proceso įstatymas leidžia ypatingais atvejais kratą atlikti ir neturint ikiteisminio tyrimo teisėjo sankcijos (numatant, kad tokia sankcija bus gauta per nustatytą laikotarpį). Tokiu atveju kratą galima atlikti taip pat greitai, kaip ir oficialiai nurodyti operatyviai išsaugoti laikomuosius kompiuterinius duomenis. Tačiau problema išlieka tais atvejais, kai, pavyzdžiui, kompiuteriniai duomenys nėra išskirti iš bendro duomenų masyvo ir atlikti kratą nerekomenduotina dėl to, jog reikiamų duomenų išskyrimas gali pareikalauti laiko. Tokiu atveju pasiruošimas kratai gali užimti tam tikrą laiką, per kurį gali būti prarasti tyrimui labai svarbūs duomenys. Tuo tarpu įpareigojimas operatyviai išsaugoti laikomuosius kompiuterinius duomenis užtikrintų laikomųjų kompiuterinių duomenų (galbūt didesnio duomenų srauto, nei reikia tyrimui) apsaugą, kol būtų atliekami kiti procesiniai veiksmai.

Kitas labai svarbus aspektas, susijęs su kratos ar poėmio atlikimu vietoj įpareigojimo išsaugoti laikomuosius kompiuterinius duomenis, yra atsižvelgimas į tam tikrus verslo interesus. Galima įsivaizduoti, kokį atgarsį visuomenėje gali sukelti kratos, pavyzdžiui, stambiausių telekomunikacijų operatorių patalpose. Stambiai verslo įmonei, kuri investuoja didžiules lėšas į gerą vardą (reputaciją), labai svarbu, kad jos klientai pasitikėtų įmone. Net neabejotina, kad kratos ir kiti panašūs procesiniai veiksmai gali sukelti rimtų įtarimų klientams, kad įmonė vykdo neteisėtą veiklą. Taigi įmonės prestižui gali būti padaryta didelė žala. Tuo tarpu įpareigojimas operatyviai išsaugoti laikomuosius kompiuterinius duomenis praktiškai neturėtų tokių žalingų pasekmių.

Dar vienas argumentas dėl kratos, kaip procesinio veiksmo, netinkamumo nagrinėjamu atveju yra tas, jog elektroniniai nusikaltimai dažnai susiję su tam tikrų duomenų siuntimu per kompiuterių sistemas (tinklus). Toks signalų siuntimas gali būti susijęs su neteisėtu turiniu, pavyzdžiui, vaikų pornografija, kompiuterių virusais ar kitais nusikaltimais, tokiais kaip sukčiavimas. Tokių buvusių komunikacijų šaltinio nustatymas gali padėti identifikuoti nusikaltėlį. Norint nustatyti „susekti“ tokias komunikacijas reikalingi srauto duomenys, kurie, kaip minėta, gali būti saugomi labai trumpą laiką. Taip pat kai elektroninės komunikacijos yra susijusios su neteisėtu turiniu ar kriminalinės veikos įrodymais ir šių komunikacijų „kopijos“ yra laikomos pas paslaugų teikėjus, pavyzdžiui, el. pašto žinutės, tokių duomenų išsaugojimas labai svarbus siekiant, kad šie svarbūs duomenys nebūtų prarasti. Vargu ar tokiais atvejais krata yra tinkama procesinė priemonė minėtiems duomenims paimti. Krata dažnai prilyginama asmens, pas kurį atliekama krata, apkaltinimui kriminaliniu nusikaltimu. Todėl tokie veiksmai pas paslaugos teikėją, kuris dažniausiai nesusijęs su nusikalstama veika, yra nepageidautini. Autorių nuomone, būtent tokiems atvejams ir yra skirta priemonė dėl operatyvaus saugomų kompiuterinių duomenų išsaugojimo. Todėl galima konstatuoti, jog atliekant kratą ar poėmį ne visais atvejais galima pasiekti tikslus, kurie keliami operatyvaus kompiuterinių duomenų išsaugojimo atveju.

Be kratos procesinio veiksmo atlikimo, egzistuoja galimybė pasinaudoti Lietuvos Respublikos baudžiamojo proceso kodekso 97 straipsnio suteikiamomis teisėmis, kad *„ikiteisminio tyrimo pareigūnas, prokuroras ir teismas turi teisę reikalauti iš fizinių ir juridinių asmenų pateikti daiktus ir dokumentus, turinčius reikšmės nusikalstamai veikai tirti ir nagrinėti*“. Tačiau ši priemonė taikytina daiktų ir dokumentų atžvilgiu ir negali būti nurodyta pateikti žinioje esančius kompiuterinius duomenis. Todėl taikant šią priemonę taip pat negalima pasiekti visų tikslų, numatytų operatyvaus laikomųjų kompiuterinių duomenų išsaugojimo atveju.

Todėl autorių nuomone, įgyvendinant Konvencijos dėl elektroninių nusikaltimų nuostatas, įstatymų leidėjas turėtų svarstyti galimybę tarp Lietuvos Respublikos baudžiamajame proceso kodekse

nustatytų procesinių prievartos priemonių įvesti naują priemonę, susijusią su įpareigojimu operatyviai išsaugoti laikomus kompiuterinius duomenis. Be abejo, ši priemonė turėtų būti aprašyta nustatant laikomųjų kompiuterinių duomenų laikino išsaugojimo maksimalų terminą, pavyzdžiui, 90 dienų (galbūt numatant galimybę šį terminą pratęsti). Bet kokiu atveju turėtų būti nustatytas maksimalus duomenų išsaugojimo terminas. Kadangi minima priemonė didžiąja dalimi susijusi su elektroninių ryšių paslaugų teikėjų veikla, svarstytina ir atitinkamų pakeitimų ir (ar) papildymų Lietuvos Respublikos elektroninių ryšių įstatyme būtinybė.

II. Laikomųjų kompiuterinių duomenų paieška ir poėmis

Konvencijoje dėl elektroninių nusikaltimų teigiama, jog „*kiekviena šalis priima tolius teisės aktus ir kitas priemones, kurių gali prireikti, įgalinant jos kompetentingas institucijas apieškoti ar panašiai ištirti:*

a) kompiuterinę sistemą arba jos dalį ir joje laikomus kompiuterinius duomenis;

b) *kompiuterinių duomenų atmeniąją terpę, kurioje tos Šalies teritorijoje gali būti laikomi kompiuteriniai duomenys*“ [3, 19 str. 1 d.].

Kaip nurodyta Konvencijos 19 straipsnio 2 dalyje, *„Kiekviena Šalis priima tokius teisės aktus ir kitas priemones, kurių gali prireikti užtikrinti, kad jos institucijoms pagal šio straipsnio 1 dalies a punktą apieškant ar panašiai tiriant konkrečią kompiuterinę sistemą arba jos dalį ir turint priežasčių manyti, kad ieškomi duomenys laikomi tos Šalies teritorijoje esančioje kitoje kompiuterinėje sistemoje arba jos dalyje ir kad tokie duomenys yra teisėtai prieinami naudojant pirmąją sistemą, tokios institucijos galėtų operatyviai išplėsti paiešką ar panašų tyrimą į kitą sistemą“.*

Vienas iš pagrindinių anksčiau minėtų Konvencijos normų tikslų – kad informacijos elektroninė forma paėmimas iš apieškomos vietos nebūtų diskriminuojamas kitų materialių daiktų ar dokumentų atžvilgiu. Kitaip tariant, krata turi būti vienodai veiksminga tiek materialių, tiek nematerialių objektų atžvilgiu.

Lietuvos Respublikos baudžiamojo proceso kodekso 145 straipsnio 1 dalyje numatyta, jog „*Kai yra pagrindas manyti, kad kokioje nors patalpoje ar kitokioje vietoje yra nusikalstamos veikos įrankių, nusikalstamu būdu gautų ar įgytų daiktų bei vertybių, taip pat daiktų ar dokumentų, galinčių turėti reikšmės nusikalstamai veikai tirti, arba kad koks nors asmuo jų turi, ikiteisminio tyrimo pareigūnas ar prokuroras jiems surasti ir paimti gali daryti kratą*“. Šioje normoje pateiktas baigtinis sąrašas atvejų, kai galima daryti kratą. Gali būti ieškoma tik daiktų, vertybių ar dokumentų. Kokiai iš šių kategorijų priskirtina informacija elektronine forma (kompiuteriniai duomenys)? Jei iš apieškomos vietos kartu su kompiuteriniais duomenimis bus paimamos kompiuterinės sistemos, tai galima priskirti daiktų kategorijai. Tačiau gali pasitaikyti atvejų, kai kompiuterinė technika, kurioje laikomi kompiuteriniai duomenys, yra susijusi su pagrindiniu, pavyzdžiui, telekomunikacijų operatoriaus verslu ir tokios technikos paėmimas gali sužlugdyti operatoriaus veiklą arba laikinai sutrikdyti paslaugų teikimą. Tada iškyla pačios informacijos elektronine forma paėmimo būtinybė (kompiuterinė technika paliekama jos buvimo vietoje). Minėtas kodekso straipsnis numato galimybę paimti dokumentus. Tačiau ne visa informacija elektronine forma gali būti prilyginta dokumentui. Pavyzdžiui, neteisėto turinio informacijos paėmimas turi būti vienodai galimas, lyginant su informacijos, laikomos dokumentu, paėmimu. Todėl siekiant, kad informacija elektronine forma atliekant kratą nebūtų diskriminuojama, svarstytinas minėto straipsnio papildymas, pavyzdžiui, „(...) *ar kitos informacijos“*. Kaip alternatyva paminėtinas prieš kelerius metus parengtas Lietuvos Respublikos elektroninės prekybos įstatymo projektas, kuriame buvo įtvirtintos normos dėl elektroninės informacijos nediskriminavimo. Remiantis šiomis normomis elektroninę informaciją būtų galima prilyginti dokumentui ir taip išvengti formalių reikalavimų neatitikimo. Tačiau minėtas projektas nebuvo priimtas, o analogiškų normų Lietuvos teisės aktuose kol kas nėra.

Labai aktuali nuostatų dėl kratos išplėtimo (19 str. 1 d. b)) įgyvendinimo problema. Konvencija nenurodo mechanizmo, kaip kratos išplėtimas turi būti vykdomas. Tai paliekama nacionaliniam reguliavimui.

Šiuo metu nesiginčijama, jog tyrėjas turi turėti teisę išplėsti paiešką į kitas sujungtas kompiuterių sistemas [4, p. 206]. Tačiau kaip tai turi būti įgyvendinama? Konvencijos rengėjų nuomone, nacionalinėje teisėje svarstytini keli kratos į kitą kompiuterių sistemą išplėtimo variantai:

1) išduotą sankciją papildo ją išdavusi institucija, t. y. „praplečiama“ apimant ir kompiuterių sistemą, kurioje yra informacija, prieinama iš tiriamosios kompiuterių sistemos;
2) suteikiami įgaliojimai sankciją papildyti sankciją gavusiai institucijai (pareigūnui).

Nors pirmuoju atveju nereikėtų kreiptis dėl naujos sankcijos, bet tyrėjas, prieš išplėsdamas kratos veiksmus į kitą kompiuterių sistemą, turėtų kreiptis dėl sankcijos papildymo[1]. Turint omenyje kitoje kompiuterių sistemoje saugomos informacijos pažeidžiamumą ir tai, jog sankcija negali būti išplėsta tiesiogiai (t. y. tyrėjas turėtų atlikti veiksmus, kurie, laiko sąnaudų prasme, prilygintini naujos sankcijos gavimui) būnant kratos vietoje, šis būdas atrodo nelabai taikomas.

Antruoju atveju tyrėjas nesikreiptų dėl sankcijos papildymo, o būtų traktuojama, jog išduota sankcija suteikia teisę tyrėjui savarankiškai išplėsti paiešką į su tiriamąja kompiuterių sistema sujungtą kompiuterių sistemą, esančią Lietuvos Respublikos teritorijoje, jei būtų manoma, kad toje kompiuterių sistemoje laikoma tyrimui svarbi informacija. Šiuo atveju būtų tiesiogiai „išplečiama" krata ir kiek įmanoma sumažinama galimybė pakeisti ar ištrinti informaciją iš atitinkamos kompiuterių sistemos, kol bus gauta nauja sankcija ar papildyta esama.

Ar galimas kratos „išplėtimas" pagal Lietuvos baudžiamojo proceso teisę? Pagal aktualią Lietuvos Respublikos baudžiamojo proceso kodekso redakciją, krata sankcionuojama ištirti ar apieškoti konkrečią fizinę vietą. Todėl pareigūnui aptikus, jog kompiuterinėje sistemoje, esančioje kitoje fizinėje vietoje, nei nurodyta sankcijoje, yra laikoma iš tiriamosios sistemos prieinama tyrimui aktuali kompiuterinė informacija, atsiranda sankcijos būtinybė naujos fizinės vietos atžvilgiu. Be abejo, remiantis Lietuvos Respublikos baudžiamojo proceso kodekso normomis, tyrėjas gali traktuoti, jog atsirado neatidėliotinas atvejis ir iš susijusios kompiuterių sistemos informaciją paimti darant kratą be ikiteisminio tyrimo teisėjo nutarties. Lietuvos Respublikos baudžiamojo proceso kodekso 145 straipsnio 3 dalyje nustatyta, jog „(*...) neatidėliotinais atvejais krata gali būti daroma ir ikiteisminio tyrimo pareigūno ar prokuroro nutarimu, tačiau šiuo atveju per tris dienas nuo kratos atlikimo gali būti gaunamas ikiteisminio tyrimo teisėjo patvirtinimas dėl kratos darymo teisėtumo*". Taip pat yra galimybė išvengti kratos išplėtimo sankcionavimo problemos, prieš kratą tiksliai išsiaiškinant ieškomų kompiuterinių duomenų buvimo vietą ir kreipiantis sankcijos dėl visų kompiuterinių sistemų, nors ir esančių skirtingose vietose, apieškojimo ar ištyrimo.

Paminėtina, jog Konvencijos paaiškinamajame rašte įvardijama, kad kratos išplėtimo galimybė nebūtinai turi būti reglamentuojama naujais teisės aktais pagal nacionalinę teisę. Jei egzistuojantys teisės aktai suteikia galimybę išplėsti kratą, nėra būtinybės priimti naujas teisės normas, reglamentuojančias kratos išplėtimą. Atkreiptinas dėmesys, jog Lietuvoje, kaip minėta, šiuo metu egzistuoja praktiniai egzistuojančiomis procesinėmis normomis paremti būdai, kaip nesant kratos išplėtimo instituto, atlikti kratą kitoje kompiuterių sistemoje, sujungtoje su tiriamąja kompiuterių sistema. Todėl galima teigti, kad nėra būtinybės svarstyti Konvencijos nuostatų dėl kratos išplėtimo įgyvendinimo naujais teisės aktais (teisės aktų pakeitimais).

III. Kompiuterinių duomenų surinkimas realiuoju laiku

Konvencijoje numatyta, jog „*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:

- *tos šalies teritorijoje surinkti arba techninėmis priemonėmis įrašyti arba*
- *bendradarbiauti su kompetentinga institucija ir padėti jai surinkti arba įrašyti realiuoju laiku srauto duomenis, susijusiu su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema*" (Konvencijos 20 str.) arba „*realiuoju laiku turinio duomenis, susijusiu su konkrečia informacija, jos teritorijoje perduodama naudojantis kompiuterine sistema*" (Konvencijos 21 str.).

Kai kalbama apie kompiuterinių duomenų surinkimą realiuoju laiku, turima omenyje įrodymų rinkimą iš dabartiniu metu vykdomų komunikacijų, kurios generuoja tam tikrus duomenis [1, p. 208]. Reikėtų atskirti, jog šiuo atveju galimi dviejų tipų duomenys: srauto duomenys[2] ir turinio duomenys[3].

[1] Tokio procesinio veiksmo galimybė Lietuvos Respublikos baudžiamajame proceso kodekse iš viso nėra numatyta.

[2] 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. 2002 m. rugsėjo 19 d. Konstitucinio Teismo nutarime telekomunikacijų įvykis apibūdinamas kaip „informacijos perdavimo, siuntimo, priėmimo telekomunikacijų tinklais faktas". Pavyzdžiui, srauto duomenimis laikytina informacija apie sujungimo laiką, trukmę, naudotus protokolus ir kita.

[3] Nei Konvencijoje, nei Lietuvos Respublikos teisės aktuose nėra apibrėžta, kas laikytina turinio duomenimis, tačiau šie duomenys susiję su susižinojimo (komunikacijų) turiniu (išskyrus srauto duomenis). Pagal 2002/58/EB direktyvos 2 (d) str., „pranešimas" – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai

Manoma, jog procesiniai srauto ir turinio duomenų surinkimo reikalavimai turėtų skirtis [8; 10], kadangi turinio duomenys atskleidžia komunikacijų turinį ir jų neteisėtas atkleidimas daro didesnę žalą nei srauto duomenų neteisėtas atkleidimas. Todėl turinio duomenų kontrolės sankcionavimas turėtų būti griežtesnis [9, 1.5–10]. Tačiau reikėtų paminėti, jog nors tradicinėse telekomunikacijose sąlyginai lengva atskirti turinio duomenis nuo srauto duomenų, kitos susižinojimo formos, pavyzdžiui, internetas tokį atskyrimą padaro gana komplikuotą. Autorių manymu, atskirti turinio ir srauto duomenis tradicinių telekomunikacijų procese nesunku – čia takoskyra tarp srauto duomenų (kas skambino, kur skambino, kiek truko skambutis) ir turinio duomenų (pokalbio turinio) gana aiški, tačiau šiuos dalykus atskirti internete gana sudėtinga arba iš viso neįmanoma. Nėra aišku, ar turinio duomenimis laikytinas visas elektroninių paketų turinys, ar srauto duomenys yra tik elektroninių paketų antraštės, taip pat ar srauto duomenimis laikytinos *clickstreams* ar http užklausos. Tokiu atveju užklausa „http:/// searchengine/com/++aids++homosexuality++symptoms“ būtų laikoma srauto duomenimis, o iš tikrųjų minima užklausa susijusi su susižinojimo turiniu [10]. Taip pat galima pateikti ir kitą pavyzdį – DTMF kodų rinkimą elektroninių komunikacijų metu. Pavyzdžiui, surinkus atitinkamą telefoninės bankininkystės numerį, sujungus atsiranda galimybė paslaugas valdyti naudojant DTMF kodus. Kadangi DTMF kodai renkami jau sujungus, galima teigti, kad tai yra telekomunikacijų 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. Todėl diskusija dėl minimų duomenų priskyrimo turinio arba srauto duomenų kategorijoms, arba šių kategorijų sutapatinimo, ypač aktuali.

Pateikti pavyzdžiai verčia atkreipti dėmesį į tolesnių tyrinėjimų sritį – minėtų dviejų kategorijų (turinio duomenų ir srauto duomenų) sujungimo, šias kategorijas kartu pavadinant komunikacijomis (elektroniniais ryšiais), problemą.

Kompiuterinių duomenų surinkimas realiuoju laiku pagal Lietuvos Respublikos įstatymus gali būti vykdomas operatyvinio tyrimo ar baudžiamojo proceso metu, todėl šie procesai nagrinėtini atskirai.

2002 m. birželio 20 d. Lietuvos Respublikos operatyvinės veiklos įstatymo Nr. IX–965 (toliau – Operatyvinės veiklos įstatymas) 10 straipsnio 10 dalyje nustatyta informacijos gavimo iš telekomunikacijų operatorių ir telekomunikacijų paslaugų gavėjų procedūra. Minimoje dalyje nurodoma, jog „telekomunikacijų operatorius ar telekomunikacijų paslaugų teikėjas privalo sudaryti techninę galimybę vykdyti telekomunikacijos priemonėmis perduodamos informacijos kontrolę“. Šioje dalyje, aprašant procedūrą, vartojamas terminas „techninių priemonių panaudojimas specialia tvarka“. Pagal Operatyvinės veiklos įstatymo 3 straipsnio 8 dalį, „techninių priemonių panaudojimas specialia tvarka – motyvuota teismo nutartimi sankcionuotas techninių priemonių panaudojimas operatyvinėje veikloje kontroliuojant ar fiksuojant asmenų pokalbius, kitokį susižinojimą ar veiksmus (...)“. Pasakymas „ar veiksmus“ iš esmės turėtų apimti techninių priemonių panaudojimą renkant srauto duomenis, nes būtent srauto duomenys yra susiję su tam tikrais telekomunikacijų paslaugų vartotojų veiksmais. Remiantis šia sąvoka galima teigti, jog Operatyvinės veiklos įstatymas numato kompiuterinių duomenų surinkimo realiuoju laiku procedūras tiek turinio, tiek srauto duomenų atžvilgiu. Tačiau paminėtinas vienas šio įstatymo trūkumas. Įstatyme vartojamos sąvokos buvo aktualios galiojant Lietuvos Respublikos telekomunikacijų įstatymui. Tuo tarpu 2004 m. balandžio 15 d. Lietuvos Respublikos elektroninių ryšių įstatyme Nr. IX–2135 (toliau – Elektroninių ryšių įstatymas) vartojamos šiek tiek kitokios sąvokos, pavyzdžiui, vietoj telekomunikacijos – elektroniniai ryšiai ir pan. Dėl šios priežasties minimas sąvokas patartina suvienodinti, atitinkamai pakeičiant Operatyvinės veiklos įstatymą.

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*“. Manytina, jog šios nuostatos užtikrina teisę surinkti duomenis baudžiamojo proceso metu.

Lietuvos Respublikos baudžiamojo kodekso 154 straipsnyje vartojama telekomunikacijų tinklais perduodamos informacijos kategorija, todėl iš pirmo žvilgsnio problemų dėl turinio ir srauto duomenų atskyrimo neturėtų kilti, nes minima kategorija apima tiek srauto, tiek turinio duomenis, kuriuos elekt-

---

prieinamomis elektroninių ryšių paslaugomis. Kitaip tariant, turinio duomenimis laikytinas pokalbio telefonu ar elektroninio pašto žinutės turinys.

roninėje erdvėje, kaip jau minėta, dažnai sunku atskirti. Tačiau kodekso 154 straipsnio 2 dalis numato telekomunikacijų tinklais perduodamos informacijos kontrolės ir fiksavimo galimybę tik srauto duomenų atžvilgiu. Todėl komunikacijų internetu atveju dėl šios normos įgyvendinimo gali kilti problemų.

Taip pat kritikuotinos kai kurios Lietuvos Respublikos baudžiamojo proceso kodekse vartojamos sąvokos (Operatyvinės veiklos įstatymo atvejis), todėl pageidautini atitinkami (nors ir formalūs) šio kodekso pakeitimai.

Išvados

1. Siekiant užtikrinti operatyvų saugomų kompiuterinių duomenų išsaugojimą, svarstytinas klausimas dėl naujos procesinės prievartos priemonės – įpareigojimo operatyviai išsaugoti laikomus kompiuterinius duomenis – įvedimo Lietuvos Respublikos baudžiamojo proceso kodekse, nustatant tokio įpareigojimo maksimalų terminą ir kitas pagrindines sąlygas.

2. Lietuvos Respublikos baudžiamojo proceso kodekso normos dėl kratos formaliai diskriminuoja informaciją elektronine forma. Galimos tokios diskriminacijos panaikinimo alternatyvos – minėto kodekso papildymas arba atitinkamų normų, skirtų elektroninės informacijos prilyginimui dokumentui, įvedimas Lietuvos Respublikos teisės aktuose.

3. Lietuvoje egzistuoja praktiniai būdai, kaip nesant kratos išplėtimo instituto, atlikti kratą kitoje kompiuterių sistemoje, sujungtoje su tiriamąja kompiuterių sistema. Todėl naujos teisės normos (teisės normų pakeitimai arba papildymai) nėra būtinos.

4. Internete sunku atskirti srauto duomenis nuo turinio duomenų, o tai gali apsunkinti teisės kontroliuoti ir fiksuoti telekomunikacijų tinklais perduodamus srauto duomenis įgyvendinimą, remiantis Lietuvos Respublikos baudžiamojo proceso kodekso 154 straipsnio 2 dalimi. Dėl šių kategorijų atskyrimo arba, atvirkščiai, teisinio reguliavimo suvienodinimo šių kategorijų atžvilgiu būtinos papildomos mokslinės diskusijos.

5. Išskyrus turinio ir srauto duomenų atskyrimo interneto aplinkoje problemą, Lietuvos Respublikoje užtikrinama galimybė įgaliotoms institucijoms rinkti kompiuterinius duomenis realiu laiku, tačiau aprašytose procedūrose vartojamos sąvokos keistinos aktualiomis.

♦ ♦ ♦

LITERATŪRA

1. **Explanatory** Report to the Convention on Cybercrime // http://conventions.coe.int (žiūrėta 2004 m. spalio 27 d.).
2. **Survey** on the Cybercrime Convention (CETS 185) and its Additional Protocol (CETS 189). European Committee on Crime Problems // http://eee.coe.int (žiūrėta 2004 m. lapkričio 2 d.).
3. **Convention** on Cybercrime // http://conventions.coe.int (žiūrėta 2004 m. spalio 27 d.).
4. **Volevodz A. G.** Protivodeistvije kompiuternim prestuplenijam. – Maskva: Jurlitinform, 2002.
5. **US Code** / Crimes/ Stored Wire and Electronic Communications and Transactional Records Access / Required Disclosure of Customer Communications and Records // http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002703----000-.html (žiūrėta 2004 m. spalio 27 d.).
6. **Lietuvos Respublikos** baudžiamojo proceso kodeksas // Žin. 2002. Nr. 46–1341.
7. **Lietuvos Respublikos** baudžiamojo proceso kodekso komentaras. – Vilnius: Teisinės informacijos centras, 2003.
8. **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 (žiūrėta 2004 m. lapkričio 2 d.).
9. **Maxwell W.** Electronic Communications: The New EU Framework. – Oceana Publications, Inc., Dobbs Ferry, New York, 2002.
10. **Banisar D.** A Commentary on he Council of Europe Cybercrime Convention // http://privacy.openflows.org/pdf/coe_analysis.pdf (žiūrėta 2004 m. spalio 27 d.).
11. **Akdeniz Y.** An Advocacy Handbook for the Non Governmental Organisations: The Council of Europe`s Cyber-Crime Convention 2001 and the Additional Protocol on the Criminalisation of Acts of a Rasist or Xenophobic Nature Committed through Computer Systems // http://www.cyber-rights.org/cybercrime/ (žiūrėta 2002 m. lapkričio 2 d.).
12. **CCIPS** International Aspects of Computer Crime // http://www.cybercrime.gov/intl.html (žiūrėta 2004 m. spalio 27 d.).
13. **Europos** Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje // http://www.lrs.lt (žiūrėta 2004 m. lapkričio 2 d.).

14. **Europos** Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo // http://www.lrs.lt (žiūrėta 2004 m. lapkričio 2 d.).
15. **Lietuvos Respublikos** asmens duomenų teisinės apsaugos įstatymas Nr. IX–1296 // Žin. 2003. Nr. 15–597.
16. **Lietuvos Respublikos** baudžiamojo proceso kodekso 154 straipsnio pakeitimo ir papildymo įstatymą Nr. IX–1993 // Žin. 2002. Nr. 37–1341.
17. **Lietuvos Respublikos** elektroninių ryšių įstatymas Nr. IX–2135 // Žin. 2004. Nr. 69–2382.
18. **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 (žiūrėta 2004 m. spalio 26 d.).
19. **Lietuvos Respublikos** operatyvinės veiklos įstatymas Nr. IX–965 // Žin. 2002. Nr. 65–2633.

♦ ♦ ♦

Some Aspects of the Implementation of the Procedural Law Section of the Convention on Cybercrime in Lithuania

Dr. Darius Štitilis
Dr. Rolandas Krikščiūnas
Prof. Dr. Rimantas Petrauskas
Mykolas Romeris University

Keywords: *cybercrimes, investigation of cybercrimes.*

SUMMARY

The main purpose of the article – to analyze legal problems related to the implementation of the Convention`s of Cybercrime Procedural Law Section in Lithuania. The developments of cyberspace have given rise to an unprecedent economic and social changes, but they also have the other side: the emergence of new forms of crimes. Besides legal problems, related to criminalisation of illegal acts in cyberspace, emerge procedural problems, such as extention of search. The present work deals with main procedural law problems, raleted to cybercrime in the light of implementation of Convention on cybercrime.

In the first part the provisions related to production order are studied. According to Article 18 of the Convention, Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. The implementation of this legal norms is discussed.

In the second part the procedural norms related to search and seizure of computer data are studied. The main question arise – the extension of search according the Code of Criminal Procedure of the Republic of Lithuania. According to the authors of the article, the norms regarding extention of the search should be implemented in the Code of Criminal Procedure of the Republic of Lithuania.

In the third part the real tim collection of computer data are studied. The line drawn between traffic data (who someone calls, when, for how long) and communications data (the content of the telephone call) is drawn from the telephone infrastructure. Adapting this to the Internet in particular is quite different, if at all possible. Is communications the content of packets? Is traffic data just the packet headers? Or is traffic data clickstreams, or http-requests? A possible step forward would be to define the notion of communication.

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